Naveen Shodh Sansar (An International Refereed / Peer Review Multidisciplinary Research Journal)
RNI No.- MPHIN/2013/60638, ISSN 2320-8767, E- ISSN 2394-3793, Scientific Journal Impact Factor (SJIF)- 8.054,
January to March 2025 E-Journal, Volume I, Issue XLIX, ISO 9001:2015 - E2024049304 (QMS)

Legal Rights of Individuals Under India's Data Protection Laws

Dr. Surendra Singh Baghel*

***Director, Law Academy, Bhopal (M.P.) INDIA**

Abstract: India's digital economy is rapidly expanding, leading to the generation and processing of massive volumes of personal data. The right to privacy, affirmed as a fundamental right by the Supreme Court of India in 2017, necessitated the establishment of a legal framework for data protection. The Digital Personal Data Protection Act, 2023 (DPDP Act) was introduced to address this need. This paper explores the legal rights conferred on individuals under the DPDP Act, examining the provisions for consent, data access, correction, erasure, grievance redressal, and remedies. It also assesses the effectiveness of these rights in safeguarding individual privacy in a digital society.
Keywords: Data Protection, Digital Rights, India, Privacy, Personal Data, Consent, DPDP Act, 2023.

Introduction - India's digital economy is witnessing unprecedented growth, leading to the large-scale generation, processing, and dissemination of personal data. With the increasing dependence on digital platforms, safeguarding the privacy and security of personal data has become a pressing concern. The Supreme Court of India, in its historic judgment in Justice K.S. Puttaswamy v. Union of India (2017), recognized the right to privacy as a fundamental right under Article 21 of the Constitution. This pivotal ruling underscored the necessity for a comprehensive data protection framework in India. Responding to this legal and social imperative, the Indian Parliament enacted the Digital Personal Data Protection Act, 2023 (DPDP Act), marking a significant milestone in the country's digital governance landscape.

The DPDP Act aims to protect digital personal data and lays down the rights of individuals, referred to as Data Principals, while imposing obligations on entities that collect and process data, known as Data Fiduciaries. The Act is designed to ensure the responsible use of personal data while upholding the privacy rights of individuals. In a society increasingly reliant on technology, these legal rights empower individuals to exercise greater control over their personal data and enhance their ability to seek redress in cases of misuse or negligence.

At the core of the DPDP Act is the recognition of several key rights of individuals. The right to access information is one of the most fundamental entitlements, allowing individuals to know whether their data is being processed, the nature of such data, the purpose of processing, and the entities with whom the data has been shared. This provision promotes transparency and accountability among data fiduciaries and enables individuals to make informed decisions about the sharing and usage of their personal data.

Another crucial right enshrined in the Act is the right to correction and erasure. Individuals can request the correction of inaccurate or outdated data, the completion of incomplete data, and the erasure of data that is no longer necessary or for which consent has been withdrawn. This right ensures that the data maintained about individuals is accurate, up-to-date, and limited to what is necessary, thereby aligning with the principles of data accuracy and minimization.

Consent is central to the data protection regime under the DPDP Act. The law mandates that consent must be free, informed, specific, and unambiguous. Individuals must be provided with clear information about the purpose and scope of data processing. Importantly, the Act grants individuals the right to withdraw consent at any time, which must be as easy to perform as giving it. This reinforces the autonomy of individuals over their personal data and places a significant responsibility on data fiduciaries to ensure transparent and ethical data practices.

In recognition of the possibility of grievances arising from data processing activities, the Act provides individuals with the right to grievance redressal. Data Principals can lodge complaints with the data fiduciary and, if not satisfactorily resolved, escalate the matter to the Data Protection Board of India (DPBI). This two-tier redressal mechanism provides a structured pathway for individuals to assert their rights and seek remedies in cases of violation.

The DPBI, established as an independent regulatory authority under the Act, is empowered to investigate complaints, enforce compliance, and impose penalties for contraventions.

The DPDP Act also introduces the right to nominate. This allows individuals to designate a nominee who can exercise their rights under the Act in the event of death or incapacity. This right ensures that the digital legacy and privacy preferences of individuals are respected even after their death, offering a humane and forward-looking dimension to data protection.

In scenarios involving data breaches, the Act mandates that individuals must be informed promptly when such breaches are likely to have a significant impact on their rights. Timely notification empowers individuals to take preventive or corrective actions, such as changing passwords, monitoring accounts, or seeking assistance, thereby mitigating potential harms. This right to be informed reflects the principle of accountability and enhances trust in digital ecosystems.

In addition to these rights, the DPDP Act imposes certain duties on individuals, thereby fostering a balanced framework of rights and responsibilities. Data Principals are required not to impersonate others, not to suppress any material information while exercising their rights, and to comply with lawful orders or directions. This provision ensures that the data protection framework is not misused and that individuals exercise their rights responsibly and ethically.

The enforcement of the rights under the DPDP Act is entrusted to the Data Protection Board of India. The DPBI functions as a quasi-judicial authority with powers to adjudicate disputes, issue directives, and impose monetary penalties. The penalties for non-compliance range from INR 10,000 to INR 250 crore, depending on the severity and nature of the violation. This strong enforcement mechanism acts as a deterrent against negligent or willful misuse of personal data and reinforces the seriousness of compliance with the law.

In terms of alignment with international standards, the DPDP Act shares common features with the European Union's General Data Protection Regulation (GDPR), such as the emphasis on consent, rights to access and erasure, and accountability of data processors. However, the DPDP Act also differs in certain respects. For instance, the centralized regulatory structure and the exemption clauses for government agencies under certain conditions have raised concerns among privacy advocates regarding potential overreach and dilution of individual rights.

Despite its promising framework, the implementation of the DPDP Act faces several challenges. One major issue is the low level of public awareness and digital literacy in India. Many individuals remain unaware of their data rights and the means to exercise them. This lack of awareness undermines the effectiveness of the rights granted under the Act and highlights the need for widespread public education campaigns.

Another concern pertains to the institutional capacity of the Data Protection Board. Given the complexity and volume of digital transactions in India, the Board must be equipped with adequate resources, technological expertise, and independence to function effectively. The success of the data protection regime hinges on the credibility and operational strength of this regulatory body.

Moreover, the balance between privacy rights and national security remains a contentious issue. The Act permits the government to exempt certain data processing activities from the application of the Act for reasons of national interest, sovereignty, or public order. While such provisions may be necessary in exceptional circumstances, they must be clearly defined and subjected to judicial or parliamentary oversight to prevent abuse and ensure that they do not erode the fundamental right to privacy.

The Act's approach to cross-border data flow is also an area of ongoing debate. It allows for the transfer of personal data to countries or territories notified by the central government. However, the criteria for such notification and the safeguards required for international data transfers are not comprehensively detailed. This creates uncertainty for businesses and may raise concerns about data sovereignty and the adequacy of protection in foreign jurisdictions.

To strengthen the data protection regime in India, several measures can be recommended. Firstly, awareness and literacy programs must be rolled out nationwide to educate citizens about their rights under the DPDP Act and the steps to take in case of violations. This can be done through schools, community centers, digital campaigns, and partnerships with civil society organizations.

Secondly, the regulatory oversight of the Data Protection Board must be fortified. The Board should operate independently and transparently, free from undue influence. Its decisions should be subject to judicial review to uphold the principles of natural justice and accountability.

Thirdly, the DPDP Act should be periodically reviewed and updated to address new challenges emerging from technological advancements such as artificial intelligence, big data analytics, and the Internet of Things (IoT). These technologies raise complex data protection issues that require nuanced and adaptive legal responses.

Fourth, promoting privacy-by-design in technological development can enhance compliance and trust. Companies and developers should be encouraged to incorporate data protection principles at the design stage of digital products and services, ensuring that privacy safeguards are built into the architecture of digital systems. Finally, collaboration between the public and private sectors is essential to create a robust data governance ecosystem. Businesses, especially startups and small enterprises, should be provided with guidance and resources to comply with the law. Industry associations and regulatory bodies

can work together to develop sector-specific codes of practice and certification mechanisms.

In conclusion, the Digital Personal Data Protection Act, 2023 marks a critical step forward in India's journey toward safeguarding digital privacy. By conferring comprehensive rights to individuals and establishing a robust enforcement mechanism, the Act lays the foundation for a privacy-respecting digital economy. However, the realization of its objectives requires proactive implementation, widespread public engagement, and continuous legal evolution. A participatory, rights-based approach that places the individual at the center of data governance will be key to building trust and resilience in India's digital future.

India's success in this endeavor will serve not only its own citizens but also position it as a leader in shaping global norms for data protection and digital rights. As the world grapples with the challenges of data misuse, surveillance, and algorithmic bias, India's data protection journey offers a unique opportunity to blend constitutional values with technological innovation, ensuring that the digital revolution is inclusive, ethical, and just.

References:-

1. The Digital Personal Data Protection Act, 2023 (India).
2. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
3. Ministry of Electronics and Information Technology (MeitY). (2023). Explanatory Note on DPDP Act.
4. Bhandari, V. (2023). Data Privacy in India: A Legal Analysis. Indian Journal of Law and Technology.
5. European Union. (2016). General Data Protection Regulation (GDPR).
6. Internet Freedom Foundation. (2023). Critique of India's DPDP Act.
7. Ramanathan, U. (2022). Privacy and the Indian State. Economic and Political Weekly.
8. Dvara Research. (2023). Personal Data Protection in India: Opportunities and Challenges.
9. Narayan, S. (2023). Digital Rights and Data Protection. LexisNexis India.
10. World Economic Forum. (2022). Principles of Digital Trust.

****