
THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A CRITICAL ASSESSMENT

Preksha Nagpal, Rajiv Gandhi National University of Law, Punjab

ABSTRACT

The Digital Personal Data Protection Act, 2023: A Critical Assessment examines and analyses the recent legislation passed by the Government of India on August 11, 2023. The act has been ordained after the Supreme Court laid guidelines for data protection in the landmark case of Justice K.S. Puttaswamy and Anr. v. Union of India & Ors. The act got passed after various discussions, public consultations, meetings held by Joint Parliamentary Committee and Standing Committee to incorporate the needs of citizens, companies and the government. This Legislative Comment deals with the provisions of the Act and analyses it by pointing the issues which can potentially harm the data security of data principal.

The Act's key element is consent, it encapsules the provisions of giving of consent and withdrawal of consent provided that the consent is of legitimate uses such as license, benefits, permits, security of the nation etc., the word 'legitimate uses' is very unclear and is seemed as coerced consent. The act provides arbitrary and wide exemptions to the government on the ground of "instrumentality of the State" which leads to abuse of power and lack of accountability. Another significant issue in the Act is sending data to foreign countries which violates the individual's fundamental right to privacy under Article 21 of the Constitution and could harm an individual's data which can potentially fall into the wrong hands especially in countries which do not have their own legislation to govern data protection. The act also excludes right to portability and right to be forgotten.

Conclusively, the Act marks India's dominance in taking lead towards protecting its citizen's personal and sensitive data.

I. INTRODUCTION

The Digital Personal Data Protection Bill was laid by the Minister of Electronics & Information Technology before the Lok Sabha on August 3, 2023 which was passed by the house on 7th August 2023. Subsequently, the Bill was also passed by Rajya Sabha on August 9, 2023 which later also got assent from President on August 11, 2023 and became Digital Personal Data Protection Act, 2023¹. It took five years of deliberations and discussions of Central Government, companies, various committees etc. in drafting and enacting this law. And the final outcome has its own hopeful prospects consisting of provisions for regulating personal and sensitive data as well as some serious issues such as wide exemptions provided to the government, overriding of consent etc.²

II. BACKGROUND AND CONTEXT

In the landmark 2017 case of *Justice K.S. Puttaswamy and Anr. v. Union of India & Ors*³, right to privacy was declared a fundamental right by the Supreme Court under Article 21 of the Constitution and directed the Government to make a legislation for data protection in the country. In accordance to that, a committee chaired by Justice B.N. Srikrishna was constituted in 2018 which was given the task to prepare the draft for data protection. A draft and report were prepared known as Data Protection Bill, 2018, after various rounds of discussions, the bill was approved by council of ministers and the Personal Data Protection Bill, 2019 was presented in the Lok Sabha. This bill was alluded to the Joint Parliamentary Committee and after its report, the Personal Data Protection Bill, 2019 was withdrawn on the grounds for blanket exemptions to government and less emphasis on protection of consumer's data. Later, incorporating all the deliberations, feedbacks and public consultation, the Digital Personal Data Protection Bill, 2023 was presented before the Lok Sabha and Rajya Sabha and also got assent from the President officiating it as an Act.

III. OVERVIEW

The Digital Personal Data Protection Act, 2023⁴ is applicable to manage personal data in India as well as outside India. Data from data principals will be processed with their due consent but

¹ Digital Personal Data Protection Act 2023.

² Donaldson MS, 'Confidentiality and Privacy of Personal Data' (1994) NLM 26.

³ K.S. Puttaswamy v. Union of India, (2018) 1 SCC 809.

⁴ *Supra* note 1.

no consent is required for legitimate purposes such as permits, licence, benefits, services, sovereignty and integrity of India, employment etc. Data fiduciaries as per the act are required to keep the data safe and secure and erase it when the ends have been met.⁵ Data principals can withdraw their consent and can ask for any grievances to be addressed. The Act exempts government agencies from some of the provisions of the act such as in the cases of security of the nation. A Data Protection Board of India has also been constituted under the Act. The Act also specifies penalties for certain offences.

IV. ANALYSIS

A. Unreasonable exemptions to government leading to violation of right to privacy

The act provides unreasonable and extensive exemptions to the government by foreshadowing and naming it as 'legitimate'. As mentioned in Section 18(1)(c)⁶ of the aforementioned act, "data can be processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law", the usage of the word 'any' and such broader collection of data without consent in the name of averting offences is solely arbitrary. The Act also mentions exemption to the government on the ground of "instrumentality of the State", such means does not adhere to the sole purpose of protecting the data of data principals.⁷ As mentioned in the Puttaswamy case⁸, violation of right to privacy should be in correspondence to the necessity whereas the exemptions granted to the state in the act such as in retention and processing of data is not proportionate and necessary, violating the Supreme Court judgement, such arbitrary exemptions may lead to harm and losses to the data principal. There is no mention of any provision in the Act which mandates the State to delete data of the data principal when the objective has been met, which breaches individual's right to privacy without any check on their data usage and falsifying the proportionality test. The law provides a wide range of exemptions to the Central Government and is not steady as could be seen in Section 7⁹ of the Digital Personal Data Protection Act, 2023, "consent shall not be required for legitimate uses such as subsidy, certificate, benefit, for security of state or in the interest of sovereignty and integrity, employment" etc., instead of protecting rights and data of individuals, the Act

⁵ Anghrija Chakraborty, *Data Protection Laws Demystified* (1st edn, Oak Bridge Publications 2021).

⁶ Digital Personal Data Protection Act 2023, s 18(1)(c).

⁷ Viswanath Namisha, 'The Digital Personal Data Protection Act 2023 The End of The Beginning' (2023) IL 5-6.

⁸ *Supra* note 1

⁹ Digital Personal Data Protection Act 2023, s 7.

established provisions for data principals mentioning what to do and what not to. It also leads to abuse of power and lack of accountability from the government's side. The exemptions are also applicable on supervisory and regulatory bodies which covers almost the whole ambit of government which in turn is quite unreasonable.

B. Transfer of data outside India

The Digital Personal Data Protection Act authorizes and allows to send individual's data to most of the countries outside India, which increases the risk of data security.¹⁰ It also does not ensure the protection of data in those countries which do not have a legislation or proper standards to protect personal data and therefore the data sent there is unguarded and at risk which neglectly could fall in unsafe hands such as entities involved in illegal means which clearly jeopardizes and hampers individual's privacy. When data leaves its jurisdiction, it becomes difficult for the government to access it and prevent it from getting breached. When the data gets transferred outside the country, there is also lack of explicit consent over how the data is being processed and if the data is being exploited and put to wrong use, it is difficult to seek legal help because of difference in rule of law and legal right and its enforcement.¹¹ It also leads to external control by the foreign country over our country because of financial dependence on them. Ironically foreign countries do not send their data to India which shows how much unsafe data is in India.

C. Overrides consent of individuals

The Act mentions a lot of provisions where an individual's consent is said to be deemed such as for the provisions of license, certificate, sovereignty, employment etc. It destroys purpose limitation which is important to protect privacy. Purpose limitation means a person's data should only be collected when it is important whilst specifying its purpose or use. The legislation tends to mandate consent from data principals in the name of legitimate uses, it is seen that the consent is being forced and is not given voluntarily.¹² In furtherance to that, withdrawing consent should be as easy as giving consent and should not be difficult and complicated. A balance of power is required between data principals and data fiduciary. The Act is ambiguous on how an individual's data would be collected and processed which makes

¹⁰ Roy Raktima, 'The Personal Digital Data Protection Act of India' (2023) FPF 18.

¹¹ Gillis Alexander, 'Consumer Privacy' (2012) DM 34.

¹² Faisal Kamrul, 'European Data Protection Law' (2023) TFO 67-97.

it difficult for the data principals to give their consent without any uncertainty. These exemptions made to the government are not appropriate in nature and such data collected can cause financial and mental harm.

Additionally, the Act does not have any provision mentioning data portability and right to be forgotten. Right to data portability allows transferring of data from data fiduciary to data principals for retaining their personal data for their own use and having their own authority on it. The right to be forgotten limits sensitive and personal data to be released digitally.

The Act does not constitute any provision to prevent any harm, if caused to data principals. Harms such as impersonation, monetary losses, arbitrary checks are quite common. Only digital data is being covered under Digital Personal Data Protection Act¹³ whereas if someone uses paper or physical data, there is no regulation on that, it doesn't matter how much data is with them. The Act does not provide any provision to compensate data principals if their sensitive data is being used negligently as mentioned in Section 43A of IT Act, 2000¹⁴.

V. CONCLUSION

Without any doubt, Digital Personal Data Protection Act, 2023 is a great advancement towards protection of personal data, addressing the issues of consent and data transferred abroad, processing and retaining of sensitive and personal data considering the increase of internet users every single day. As a whole, legislators played a good role in making of the Act after thorough discussions, deliberations and feedback through public consultations marking country's viewpoint in data protection.

However, the Act also has some issues mainly being blanket and wide exemptions provided to Central Government, deemed consent in the namesake of legislative uses and security, sovereignty of India, violation of fundamental right to privacy, transferring personal data in foreign countries which increases the risk of data security etc. But, as a country where privacy of data is not recognised as such in its true sense, the Digital Personal Data Protection Act, 2023¹⁵ is a great start before coming to the conclusion on what is best for the nation.

¹³ *Id*

¹⁴ Information Technology Act 2000, s 43A.

¹⁵ *Supra* note 1.