Volume 34, August 2024 ISSN 2581-5504

"Data Privacy Regulations and Technological Advancement"

***Ajay Sahani**
Indian Law Society (ILS) College
Pune

****Utkarsha Rananaware**
Indian Law Society (ILS) College
Pune

Abstract

The blog contains an introduction to data protection and how it came into effect and a brief history. Further, it talks about the effects of technological advancement and how it is currently affecting data privacy negatively and possibly. Also, how technology is misused when it comes to data privacy and digitalization, and lastly it concludes how data privacy can be used effectively. Through the course of this paper, we will understand the problems arising due to this recently introduced act and its drawbacks by taking examples from recent cases.

Keywords: Data Privacy, Digitalization, Technological Advancement, misuse of technology.

Introduction

The right to privacy concerning data protection refers to the ability to prevent illegal access to and disclosure of personal information, ensuring that people have control over their data and use it as a fundamental human right. Since there is an increasing amount of personal data being collected and analyzed, privacy is more crucial than ever. Maintaining control over our information on our terms and preventing its use by third parties is a fundamental component of the right to privacy. Businesses and governments frequently use this kind of data for their own business and political ends, which allows them to obtain fresh insights and make better decisions. Using instances from current cases, we shall analyze the issues raised by this recently enacted act of Digital Personal Data Protection Act 2023, (hereinafter referred to as DPDP) and its shortcomings throughout this essay.

The Supreme Court in Justice K.S. Puttaswamy and Others v. Union of India and Others[1] said that the right to informational privacy is a component of the fundamental right to life in India, and is therefore guaranteed. Privacy encompasses more than simply our right to be free from intrusions; it also involves safeguarding our personal information in the digital age. Nevertheless, the ruling did not define the precise parameters of the right to informational privacy or provide certain safeguards for this privacy right. Therefore, after almost half a decade of deliberation and

[1] Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors (2017) 10 SCC 1, AIR 2017 SC 4161.

Volume 34, August 2024 ISSN 2581-5504

discussion and after the introduction of various draft bills DPDP was finally adopted. The Committee appointed for this act, stated that to process personal data, consent needs to be obtained first. Such assent ought to be meaningful or well-informed. Furthermore, a data protection law must adequately protect the interests of specific vulnerable groups, such as children and sensitive personal data, while taking into account their vulnerability and exposure to threats online. Furthermore, the person's express consent should be required before disclosing sensitive personal information. Sensitive information that people might not wish to disclose or that organizations may have utilized without permission is also included in the data. Sensitive information relates to personal topics (such as a person's caste, religion, or sexual orientation) where there is a greater expectation of privacy. Passwords, financial information, biometric information, genetic information, caste, political or religious views, and any other type of data designated by the Authority are all considered sensitive personal data. biometric information. Financial information, face photographs, dactyloscopy data, and other personal data resulting from particular technical processing related to a natural person's physical, physiological, or behavioral features that permit or validate that natural person's unique identification.

How are technological advancements creating problems for the protection of data?

The Bill's clause 3(c)(ii) specifies that it will not apply to personal information that a user makes publicly available. For instance, the Bill demonstrated that processing of personal data will not fall under the ambit of data protection laws if the person openly disclosed her personal information on social media while blogging about her opinions. This permits businesses to handle personally identifiable information that is readily available to the public without obtaining consent or following other Bill requirements. In cases where an influencer's information benefits a firm, but also causes loss or disadvantage for her, the onus of responsibility falls on her, rather than the other party. This may seem a bit like victim blaming. Now, in cases where knowledge benefits a business but also causes loss or disadvantages the influencer, it is his/her fault and not the other party's; this almost sounds like victim blaming, like when a celebrity is deepfake.

Another problem that data privacy-related technology improvements provide is employment loss and economic disruption. One possible consequence of AI technology's economic disruption is a rise in worker financial instability. This can therefore result in a scenario where people are compelled to give up their privacy to survive. It's as if folks can make some money in exchange for their privacy. Regarding the ratings we assign to different workers, such as the Uber auto-wala bhaiya or the Zomato/swiggy person, this is also a form of data input that dictates the kind of economic development that individual workers will experience in their careers. The problems that technological improvements present to maintaining economic privileges are not insignificant to a person.

Volume 34, August 2024 ISSN 2581-5504

The possibility of malicious actors abusing Artificial Intelligence (hereinafter referred to as AI) technology is yet another important concern. AI has the power to produce convincingly phony photos and movies that can be used to disseminate false information and even sway public opinion. AI can also be used to develop extremely complex phishing assaults, which deceive people into disclosing personal information or clicking on harmful links.

Another notable example of how technology affects data privacy is the Deep Fake case of Rasmika Mandana.

"Welfare functions" have also led to certain issues. If a business repeatedly violates Section 37, the government may, at its discretion, prohibit access to websites or content in the “interests of the general public” or in response to recommendations from the Data Protection Board. This expansive wording goes beyond the government's previously debatable ability to censor content under section 69A of the Information Technology Act of 2000. Furthermore, since the Data Protection Board is tasked with overseeing data protection matters and "content" falls under a larger purview already covered by other laws like the IT Act, the Board's authority to recommend blocking of "content" is problematic.

However, despite the DPDP's misuse of technology, some aspects of the bill's beneficial uses of technology—like the principles-based approach—cannot be disregarded. Owing to the tech industry's rapid growth and disruption, the Charge places more emphasis on principles and outcomes than on modes and forms. This will extend the charge's lifespan and provide firms more flexibility in achieving compliance.[2]

Light-touch approach: Businesses will advantage of the light-touch and facilitative approach of the Charge towards individual information assurance. This implies the belief rested by the government within the private division to act as mindful overseers of the individual information of their clients. [3]Driving force for startup biological system: The rationalized and negligibly meddlesome information security administration will pull in worldwide tech ventures. The Charge will be a boon for new companies as they are to be exempted from certain commitments, upon

[2] ForumIAS, ‘Digital Personal Data Protection Bill, 2023: Explained, Pointwise’ (*Community*, 28 August 2023) <https://forumias.com/blog/digital-personal-data-protection-bill-2023-explained-pointwise/#What_are_the_positive_aspects_of_the_Digital_Personal_Data_Protection_Bill_2023> accessed 16 February 2024.

[3] ForumIAS, ‘Digital Personal Data Protection Bill, 2023: Explained, Pointwise’ (*Community*, 28 August 2023) <https://forumias.com/blog/digital-personal-data-protection-bill-2023-explained-pointwise/#What_are_the_positive_aspects_of_the_Digital_Personal_Data_Protection_Bill_2023> accessed 16 February 2024.

Volume 34, August 2024 ISSN 2581-5504

notice. This will assist impulse to the startup biological system and boost its worldwide competitiveness.[4]

Instances where courts have dealt with Protecting Data -

The Delhi High Court directed Google LLC to immediately remove any videos that addressed the health and well-being of Abhishek and Aishwarya Bachchan's daughter, Aaradhya Bachchan. The films were removed, but not immediately, even after Google LLC received a complaint about them, erroneously claiming that Aaradhya was in critical condition. Citing the video publishers and uploaders as utterly demented people, the Court mandated that Google LLC immediately take down the videos. It also asked Google to take down any further videos that looked similar to what the petitioner had alerted it to.[5] Similar to other intermediaries, Google contended in court that it had no control over the films and that it does not actively remove anything unless it is classified as rape, obscenity, or another such category. After declaring that the petitioner's response was unacceptable, the Court gave the petitioner relief. The main arguments in the lawsuit focused on Rules 3 and 4 of the 2021 Intermediary Guidelines, which mandate that content removers, such as Google, remove information promptly upon receiving complaints about, among other things, harm to children, privacy, copyright infringement, and defamation. This event demonstrates the increased responsibility that high-tech intermediaries have when handling data.

Conclusion

The rising computerized scene has lastingly modified how individual information is collected, put away, and tackled for numerous known and obscure purposes. Within the nonappearance of organized and comprehensive information protection laws, the security of individual information is more deliberate than required. With the rise of Data Governance and its serious emphasis, India has taken a cautious approach in clearing its way on the worldwide outline as a 'nation centered on building a solid information security regime' and offering assistance to boost worldwide belief, making our nation an appealing venture center.[6] Information Administration is the hone of effectively and successfully overseeing information (both individual and non–personal

[4] ForumIAS, 'Digital Personal Data Protection Bill, 2023: Explained, Pointwise' (*Community,* 28 August 2023) <https://forumias.com/blog/digital-personal-data-protection-bill-2023-explained-pointwise/#What_are_the_positive_aspects_of_the_Digital_Personal_Data_Protection_Bill_2023> accessed 16 February 2024.

[5] https://www.ndtv.com/india-news/aaradhya-bachchan-google-told-to-remove-false-content-on-aaradhya-bachchan-from-youtube-3964166.

[6] India E, 'How Will the Data Protection Bill Help India Achieve Its Vision of a Digital Future?' (*How will the Data Protection Bill help India achieve its vision of a digital future?* 28 January 2022) <https://www.ey.com/en_in/cybersecurity/how-will-the-data-protection-bill-help-india-achieve-its-vision-of-a-digital-future> accessed 17 February 2024.

information) to maximize trade esteem as well as secure the information. Data Management comprises an organization's hones of overseeing individual and non– individual information in arrangement with the targets set for Information Data Privacy and Data Protection comprises an organization's hones of overseeing and securing information in arrangement with appropriate information security laws and controls. Presently, organizations ought to center their arranging on designing a cross-utilitarian protection program that will construct competitive advantage, develop belief, and back long-term maintainability.