GDPR and DPDP: A Comparative Analysis on User-Centrism

Neehra Sharma & Sanyam Mahajan

Ramjas College, University of Delhi

Introduction

The shape and the volume of ideas and conversations that flow through a medium are directly influenced by the rules and regulations governing said medium. To ensure a freer flow of ideas and conversations, one must have regulations that increase user capacity. One of the primary ways of doing that is through a decrease in state capacity. In this article, we discuss the formulation of General Data Protection Regulation (GDPR) and Digital Personal Data Protection Act (DPDP), and how they have and might influence user capacity in the digital domain through a comparative analysis of the two regulations.

The Ideas of Personal Data and User-Centrism

Both the ideas of privacy and user-centrism, especially in the digital domain, are quite inter-related; while privacy talks about the ownership of one's information (Alan, 2019), user-centrism talks about the ability to have said ownership over one's information. Following the Right to Privacy verdict (Justice K. S. Puttaswamy (Retd.) and Anr. vs. Union of India & Ors.), it was realised that privacy is "necessary", "reasonable", and "proportional". However, to use said fundamental right to privacy, one must have the user capacity to make optimal use of it. One's privacy, as an individual, primarily concerns their personal data, which is information that relates to an identified or identifiable individual. This information could range from easily accessible information, such as one's name, email address, or phone number, to extremely sensitive information such as medical records and passwords. In the digital arena, access to one's personal data is provided to avail different services, but such a transactional framework also harbours dangers to one's digital privacy and therefore needs to be regulated through legal means.

User-centrism is the idea of giving primacy to the rights and liberties of a user over company policy and state regulation. It is the idea of putting the user at the centre of both policy design and policy implementation. This concept is especially important in the digital domain, given the flow of extremely sensitive personal data. That said, the implementation of user-centric policy design often comes with a high implementation cost for companies, as seen in the implementation of rights in GDPR, according

to the International Association of Privacy Professionals (IAPP) Annual Privacy Governance Report 2016, data controllers consider three aspects of the regulation most challenging to implement in their organisation: the right to be forgotten, data portability, and gathering explicit consent. However, given the importance of the powers provided to rights holders, the benefits heavily outweigh the cost, especially in the long term.

In the following sections, in order to gain a better understanding of the two regulations, we will briefly discuss the formulation of GDPR and DPDP and the principles they were based on.

GDPR: History

The General Data Protection Regulation (GDPR) was adopted on April 14th, 2016, and enacted on May 25, 2018. Built as a regulation to unify the digital data privacy and protection laws of the members of the European Union (EU), it was the first of its kind cross-sectoral, economy-encompassing digital data protection law. Drawing its power from Article 8 of the Charter of the Fundamental Rights of the European Union (Charter), it puts prime focus on the rights of the individual over their personal data. Even before the signing of the Charter in 2000, GDPR can trace its roots to the Data Protection Directive, 1995 (European Data Protection Supervisor, 2018), which provided directives to its member states for the formulation of their own national digital personal data protection policy. The current regulation states seven principles that are to be followed in the processing: lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. (Elstgeest, 2018)

DPDP: History

The draft DPDP Bill, 2022, was introduced after the retraction of the Personal Data Protection Bill, 2019, this was done in order to form a comprehensive legal framework set to the global standard (Burman, 2020). DPDP can trace its origin back to Justice KS Puttaswamy case of 2017, where the fundamental right to privacy was reaffirmed. Other than that, the recent introduction of GDPR in Europe at that time helped accelerate the lawmaking process. The bill became an act in August 2023. It too is a cross-sectoral, economy-encompassing, digital data protection regulation. Until now, the protection of personal data was regulated under Section 43A of the Information Technology (IT) Act, 2000, however, given the growing usage of the digital medium, it was highly pertinent for the Government to bring in a comprehensive law regulating said medium. The act tries to bring in the digital protection law while bringing minimum disruptions ensuring the process is followed (Burman, 2022). It bases itself on the following seven principles (similar to those of GDPR) - consented, lawful and transparent use of personal data; purpose limitation; data minimisation; data accuracy; storage limitation; reasonable security safeguards; and accountability (PIB, 2023).

User-Centrism in GDPR and DPDP

Though both regulations lay emphasis on provisions that provide increased user-centric policies, there are a few key differences, especially seen in the rights to be forgotten and data portability. Data portability, according to GDPR, is defined as the process of movement of data from the data principal to the data fiduciary across different applications, programs, and cloud computing services. In the age of Big Data, swift movement of large and complex data in a standardised format becomes imperative (Milt; Elvy, 2017). In the realm of personal data, data portability works with Personal Identifiable Information, which means data that can be used to identify a specific person. From a consumer's perspective, the personal data they put on various social media sites like Twitter and Facebook remains consistent throughout these different applications which increases the accessibility of data. Article 20 of the General Data Protection Regulation provides for the Right to Data Portability: "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used, and machine-readable format, and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided." This provision gives a user-centric approach to data privacy which places the autonomy of a person's personal information with the "data subject". This right allows the individual to reuse their personal data for their own purposes across different platforms.

GDPR also provides the Right to be Forgotten in articles 17 and 19. There are certain grounds on which the data subject can have their data erased. There are certain restrictions to this right to be forgotten under Section 60 which relate to the use of personal data for public interest, and in Section 43 which aims to align the right of erasure with the right of freedom of expression and information.

Unlike GDPR, DPDP does not grant the Right to Data Portability or the Right to be Forgotten. Both the Srikrishna Committee (2018) and the Joint Parliamentary Committee formed to review the Personal Data Protection Bill (2019), had recommended the inclusion of both these provisions. While the Right to Data Portability provides the individual with the autonomy of migrating their data from one platform to another, the Right to be Forgotten refers to the right of a data subject to get their data erased. The Srikrishna Committee, in its report released in 2018, recommended that the right to be forgotten will compete with other rights, and the implementation of this provision may be decided based on factors like the sensitivity of the personal data to be restricted, the relevance of the personal data to the public, and the role of the data subject in public life. That said, DPDP did receive a downgraded version of the Right to be Forgotten, namely the Right to Erasure, which, because of its vaguely worded nature, opens several doors to exemptions from said erasure by stating ambiguous reasons. This opens the door to exploitation of the user and compromises user-centric ideas.

Other than that, there still are several problems within DPDP that include provisions that can lead to a compromise in user capacity. These include the shrinkage of the clauses from 90 to 30 from the proposed 2019 bill to the current act, this is due to the conversion of the language of the act into basic

English. The usage of SARAL language (Simple, Accessible, Rational & Actionable Law), according to Apar Gupta (2022), which could lead to compromised judicial takings because of the levied vagueness and brevity. There has also been a marked shift of power from the legislative to the executive, as out of the 30 provided clauses, there have been mentions of the phrase 'as may be prescribed' a total of 18 times. Another problem with the phrase is that of vagueness. With such a high amount of ambiguity in the text, the assumption of power from the state can lead to severe compromises to not only the user-centric needs but also to the checks and balances of India's institutions.

Conclusion

Though both the regulations put a heavy focus on the promotion of user-centric regulations, the rights provided and the wording of the DPDP regulation seem lacking. One must ensure policies are liberal for the individual, especially in the case of multicultural, pluralistic societies where personal data and information gain heightened importance because of the uniqueness found in such societies.

To ensure a free and liberal flow of ideas and a reinforced belief in one's institutional system, policies have to provide as many rights to the individual as possible without compromising state capacity. However, this has not been the case, as can be seen with the recent introduction of bills for the electronic medium, such as the amendment to the IT Rules, 2021, and the Telecommunications Bill, 2023. This, coupled with the ambiguous and vague wording of such bills, has led to a reduction in user capacity and a decrease in transparency and accountability. This is a case for DPDP, as noted by Professor Subhasis Banerjee (Professor, Computer Science and Engineering, IIT Delhi), who says the regulation "facilitates data collection and processing by the government and private entities rather than data protection (Gupta, 2023). Thus, it becomes the duty of civil society and informed citizens to ensure the increase in user capacity, because it is through the empowerment of said capacity that one can actualise their goals and aspirations.

References

Allen, A. L. (2019, October 31). *Philosophy of privacy and digital life* [Presidential Address]. American Philosophical Association One Hundred Fifteenth Annual Eastern Division Meeting, New York. https://papers.ssrn.com/abstract=4022657

Burman, A. (2020, March 9). *Will India's proposed data protection law protect privacy and promote growth?* Carnegie India. https://carnegieindia.org/2020/03/09/will-india-s-proposed-data-protection-law-protect-privacy-and-promote-growth-pub-81217

Burman, A. (2022, August 22). *The withdrawal of the proposed data protection law is a pragmatic move*. Carnegie India. https://carnegieindia.org/2022/08/22/withdrawal-of-proposed-data-protection-law-is-pragmatic-move-pub-87710

Directorate-General for Internal Policies of the Union (European Parliament), & Marzocchi, O. (2019). *Personal data protection achievements during the legislative term 2014-2019 : the role of the European Parliament*. https://doi.org/10.2861/666189

Elvy, S.-A. (2017). Paying for privacy and the personal data economy. *Columbia Law Review, 117*(6), 1369–1459. JSTOR. https://www.jstor.org/stable/44392955