FROM DIRECTIVES TO REGULATIONS: 'THE PARADIGM SHIFT IN DATA PROTECTION'

Ansh Dhariwal & Pratham Chaudhury, OP Jindal Global University

ABSTRACT

The General Data Protection Regulation (GDPR)[1], which was approved by the European Union (EU) in 2018, sought to profoundly transform global data privacy by building on strong business practices and a comprehensive framework of personal rights. By emphasizing consent, accountability, and transparency, the GDPR has established a global standard for data protection frameworks and replaced the EU's Data Protection Directive from 1995[2]. One example of the GDPR's enforcement efforts and extraterritorial implications in influencing global privacy laws is India's Digital Personal Data Protection Act, 2023 (DPDP Act)[3]. Questions are being raised about whether the DPDP Act is positioned to sufficiently protect individual privacy in a time of unprecedented socioeconomic inequity, increased technology, and increased government use of citizens' data. This paper compares aspects of India's DPDP Act with the GDPR to determine whether India's new data protection regime is aligned with individual needs for privacy protection in digital spaces. Actionable recommendations for reform of the privacy regime are proposed, including issues related to using consent in low literacy segments, organizational compliance burden, surveillance by the state, and algorithmic profiling. The paper also reflects on efforts to improve the DPDP Act's effectiveness through recommendations for structural reform that align privacy protection with India's constitutional values and the realities of the digital environment.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1
[2] Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1
[3] Digital Personal Data Protection Act 2023 (India)

Introduction: Global Privacy Norms in a Data-Driven World

In a period governed by digitalization, the captioning and commodification of personal data has changed the form of interaction of individuals, the state, and businesses. In an age where states and private actors are becoming more reliant on data in matters ranging from targeted advertising to algorithms informing forms of welfare payments, tensions and panic surrounding surveillance, consent, and data abuse are heightened globally. The European Union's General Data Protection Regulation (GDPR) is leading the world in response to those tensions. Since it commenced enforcement in 2018, the GDPR has evolved into the standard for new data protection legislation. The GDPR created a rights-based, holistic, and extraterritorial scheme that inspired legislative trends in jurisdictions like Brazil (LGPD), Japan (APPI), and, notably for us, in India.

India's data protection odyssey started to forge ahead with the Puttaswamy v. Union of India (2017)[4] decision that privacy became a constitutional right under Article 21 of the Constitution[5]. Since the Puttaswamy case, India has given precedence to expert deliberations, including the draft Personal Data Protection Bill of the Srikrishna Committee (2018)[6], and subsequently culminated in the Digital Personal Data Protection Act, 2023 (DPDP Act). The DPDP Act was purportedly an important step forward in data governance, however creates a serious concern of whether the DPDP Act will be a meaningful step forward in such a complex digital sphere composed of factors like low levels of digital literacy, the existence of centralized surveillance hardware, and the pace of algorithmic changes in India. This paper tries to answer the most important question of whether the DPDP Act sufficiently protects individual privacy in India's increasingly unequal and digitally connected society.

GDPR as a Global Standard: The Blueprint for Modern Data Protection

The 2018 General Data Protection Regulation (GDPR) of the European Union is a significant shift in international consciousness of privacy and international data governance. It goes beyond the 1995 Data Protection Directive, a step in the right direction 30 years ago, but one that failed in conjunction with the show and scale of digital expansion. The Data Protection

[4] Justice K.S. Puttaswamy (Retd.) and Anr. v Union of India and Ors. (2017) 10 SCC 1
[5] Constitution of India 1950, art 21
[6] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (MeitY 2018)

Directive was merely a recommendation with suggested next steps (fair processing, access rights, etc.), but was ultimately vague and ineffective with a non-universal application and an ambiguous plan for internationally transferred data.[7]

This was all addressed by the GDPR to create a more standardized, applicable internationalization of the approach to data protection within Europe. The distinction of the GDPR is that it is much more far-reaching and focused on individual rights. Therefore, it allows for more personal control by establishing the rights to access your data, amend it, delete it (the "right to be forgotten"), and transfer it from one service to another.[8] This was a drastic change—data protection was no longer an administrative necessity, but a tool for human empowerment.

At the same time, the GDPR places a lot of responsibility on companies and organizations, with firm requirements to transparently process data, report breaches as they happen, and appoint data protection officers when necessary[9]. In addition, the law does not only apply to European companies; any company, any business, any organization that collects or processes the data of European Union citizens—even if the headquarters are in Delhi, Dubai, or New York—must comply with the GDPR. Thus, it is a norm for other countries looking to adopt or revise data protection laws to use GDPR as a standard.

India's Digital Personal Data Protection Act, 2023, echoes many of these international influences. Although the DPDP Act takes a page from the GDPR in structure and language, its enforcement and underlying ethos remain to be seen, particularly when it comes to balancing state surveillance and individual privacy, or dealing with issues such as digital literacy and informed consent in a highly diverse population[10]. In this way, the GDPR is not only a regulatory system but also a standard that challenges us to think about how legal systems can be both globally responsive and locally responsive.

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data. See also González Fuster, G. The Emergence of Personal Data Protection as a Fundamental Right of the EU (Springer, 2014).
[8] General Data Protection Regulation (EU) 2016/679, Articles 15–20. For broader discussion, see Kuner, C. The General Data Protection Regulation: A Commentary (OUP, 2020).
[9] Ibid, Articles 30, 33, 37–39. These provisions collectively reflect the GDPR's accountability framework.
[10] See Baijal, A. (2023). India’s DPDP Bill: Between Global Influence and Local Realities, Indian Journal of Law and Technology. Also see Puttaswamy v. Union of India (2017) 10 SCC 1, which recognized privacy as a fundamental right under the Indian Constitution.

India's Data Protection Journey: From Puttaswamy to the DPDP Act, 2023

India's data protection regime is developing not only in a legislative manner, but also in a jurisprudential journey towards the constitutional recognition of informational privacy as part of dignity and autonomy. This journey was initiated by Justice K.S. Puttaswamy (Retd.) v Union of India, where the Indian judiciary included privacy in the ethical-moral values that ground the Indian Constitution instead of in the statutory privilege of privacy that we understand it as today. As for Puttaswamy, it was entered in the context of increasing concerns over the growing digital architecture of the Aadhaar project, a biometric identity meant to collectively prescribe personal information under a state-controlled structure. Although the ostensible purpose was the provision of welfare, the constitutional issue was more profound: Does the Indian Constitution guarantee privacy as a fundamental right? In thunderous affirmation, the Supreme Court of India's nine-judge constitution bench determined that privacy inheres within the freedoms of Part III of the Constitution under Articles 14, 19, and 21[11]. In a significant step forward, the Court accepted informational privacy by stating that the ability to control the sharing and use of our personal information is an essential element of personal autonomy in the contemporary dominion of all-encompassing surveillance.

This recognition was not abstract. The judgment relied expressly on concerns about "profiling" individuals using big data, algorithmic opacity in governance, and the asymmetry of power for individuals (as compared to the state/corporations) in data transactions. The Court's conclusions in Puttaswamy have created a constitutional duty on the state to create a data protection regime that respects individual autonomy, the rule of law, and passes the requirement of proportionality if the state decides to intrude on individuals' data. After the ruling in Puttaswamy, the Government of India established the Committee of Experts led by Justice B.N. Srikrishna, who was tasked to consider a framework of data protection. The Committee's report, A Free and Fair Digital Economy, made significant contributions. Firstly, it referred to privacy as a 'horizontal' right that could be enforced against both the state and against any private actor too, and secondly, it highlighted data fiduciary obligations, signaling the need for technology accompanied by an ethical data processing architecture that depends on both trust and deals with responsibility.

After years of waiting, the first independent and comprehensive data protection law in India

[11] Constitution of India 1950, art 21

was passed in 2023 with the passage of the Digital Personal Data Protection Act[12], after decades of political horse-trading and parliamentary stalling. The DPDP Act asserts that it regulates the processing of personal data in both public and private realms, with a focus on elements like consent, notification, lawful purpose, and data subject rights. Upon initial observation, it appears to duplicate key aspects of the GDPR, including rights to redress, erasure, and correction. Yet its philosophical anchoring has an altogether different foundation; unlike GDPR, which is anchored in the EU Charter of Fundamental Rights, the DPDP Act is not based on an explicit declaration of privacy as a fundamental right. It is more of a compliance handbook rather than a normative rights document. The gap between Puttaswamy's constitutional promise and the DPDP's legislative compliance handbook is indicative of a minimalist, administrative notion of privacy in contrast to the Court's transformative constitutionalism.

Additionally, Section 18[13] of the Act gives the Union Government broad authority to exempt state agencies from any or all of the following, which goes against the proportionality concept outlined in Puttaswamy. The lack of a clear safeguard against algorithmic decisionmaking, profiling, or widespread surveillance calls into question the Act's commitment to the original ruling. The path from Puttaswamy to the DPDP Act is a convergence point of constitutional desire and legislative prudence. India's course from the Puttaswamy decision to the DPDP Act, 2023, is a story with high expectations for the Constitution and low ambitions for the law. India finally has a specific law to protect individuals' data for the first time. But the law sounds more like a set of obligations for companies and government departments to meet. Hardly an earnest promise to protect individuals and their rights.

The Puttaswamy case had clearly articulated that privacy is a fundamental right on par with the right to life, freedom of speech, etc. The Act has not moved the spirit forward. It is about processes and approvals, but it does not adequately protect individuals from the potential state efforts at surveillance or the potential abuse of individuals' data by large tech companies. What matters today is not that we have a data protection law. What matters is whether the law affords individuals dignity, control of their data, and accountability of both government and business.

[12] Digital Personal Data Protection Act 2023 (No 22 of 2023)
[13] Digital Personal Data Protection Act 2023, s 18

Comparative Analysis: GDPR vs. DPDP Act

As nations around the world seek to govern personal data in the era of the internet, both the European Union's General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act, 2023 (DPDP Act) are attempts at establishing transparent guidelines on privacy, accountability, and the use of data. Although the GDPR has been held out as the gold standard for data protection, the DPDP Act is a localized effort shaped by it. Yet, differences in underlying constitutional principles, socio-political priorities, and institutional capacities unveil major divergences.

Philosophy and Constitutional Backing

The GDPR is based on a rights-based approach, with its roots firmly anchored in Article 8 of the EU Charter of Fundamental Rights, under which it enshrines the right to protection of personal data as an independent fundamental right[14]. This constitutional embedding informs how GDPR is interpreted and applied—it places the dignity and autonomy of the individual at the center stage in the online world. In contrast, the DPDP Act does not have a clear rights based approach. It does not establish a direct connection to the right to privacy acknowledged as a basic right in the Indian Constitution after the Puttaswamy judgment (2017)[15]. The Act's language is administrative and compliance-oriented rather than declaratory of personal rights. This is a source of concern regarding enforceability, particularly where the individual has to contest state or corporate encroachment without the strong backing of constitutional language within the Act itself.

Rights of Individuals

The GDPR gives data subjects an extensive list of rights, which range from access, rectification, erasure, restriction of processing, objection to automated profiling, and data portability[16]. The rights are actionable and come with recourse mechanisms. The DPDP Act, though recognizing some of these rights, such as access, rectification, and erasure, is more limited in scope. It does not include the right to data portability and the right to object to automated decision-making or profiling, both of which are considered essential in the current AI-driven digital environment.

[14] Charter of Fundamental Rights of the European Union, Article 8.
[15] Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1.
[16] GDPR Articles 15–22

Absence of these protections can restrict people's capacity to make effective decisions about the use of their data, especially in fields involving algorithmic discrimination like credit scoring, targeted advertising, or welfare provision.

Consent and Accessibility

The GDPR and the DPDP Act place consent as a primary legal basis for processing personal data. GDPR mandates that consent must be freely given, specific, informed, and unambiguous, with a clear affirmative action[17]. Likewise, the DPDP Act also requires clear and specific consent to be received before data processing. The Indian context, however, has its own set of challenges. With a vast digitally connected population but frequently low in digital and legal literacy, and with information normally available in English or legal terminology, the notion of informed consent is tenuous. Numerous users click "agree" without understanding. In addition, designs that deceive users into providing consent are under-regulated. This is problematic on ethical and practical grounds about whether or not consent, in the Indian case, serves as an actual protection or merely a procedural formality[18].

Obligations on Organizations

The GDPR presents strong obligations to data controllers and processors. Appointment of a Data Protection Officer (DPO) under specific conditions, Data Protection Impact Assessments (DPIAs) on high-risk processing, and enforcement of data breach notification within 72 hours are some of these obligations. Such obligations promote the culture of compliant behavior. Some of these obligations are present in the DPDP Act, but in a more elastic and less onerous manner. For instance, DPIAs and DPOs apply only to "Significant Data Fiduciaries," a term given by the government. There could be loopholes if there aren't universal timelines for breach notification and weak mechanisms for auditing. Besides, India's SMEs rarely have enough resources or ability to develop mature compliance systems, and the Act is not too supportive, with limited phased implementation opportunities[19].

[17] GDPR Article 6(1)(a); Recital 32.
[18] Baijal, A. (2023). India’s DPDP Bill: Between Global Influence and Local Realities, Indian Journal of Law and Technology.
[19] Ministry of Electronics and Information Technology, DPDP Act, 2023 – Overview & FAQs.

Cross-Border Data Transfers

GDPR permits only data transfers outside the EU in strict conditions, including when the destination country has an adequacy decision from the European Commission, or if Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) are available. This provides the same level of protection to personal data leaving the EU. The DPDP Act is more discretionary, enabling the Central Government to certify nations or regions to which data can be exported, based on criteria that are not made public. The model is not transparent and leaves one wondering if political interests may play a role in making decisions regarding data flow, as compared to the adequacy of data protection. Additionally, it might jeopardize India's vision to be regarded as a trustworthy data processing center globally[20].

DPDP in the Indian Context:

India's Digital Personal Data Protection Act, 2023 (the DPDP Act) is a long-overdue step towards digital privacy. Although the DPDP Act purposefully presents itself as a fundamental protection to individual rights against data-enabled governmentality, the Act has left open a myriad of gaps exposing three distinct fault lines: algorithmic obscurity, government excesses, and the digital divide, especially as a function of India's sociopolitical context and technological capacity.

- **Government Supervision and Lack of Checks**

The most significant and controversial aspects of the DPDP Act is in section 17(2)(a)[21] of the act, whereby the Central Government may exempt any of its agencies from the application of the DPDP Act "in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States" etc. The exemption is only conceptual, and together with section 4 of the act[22], which provides that processing can be undertaken only for lawful purposes. Thus, these vague and contradictory provisions envisaged in the act lack the impartial examination and responsibility that would set it apart from a legitimate system. In the case of Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court ruled that any infringement of the right to private life must pass the three-part test of proportionality,

[20] Bhandari, U. (2023). Data Sovereignty vs. Data Protection: A False Choice for India?, Centre for Internet and Society.
[21] Digital Personal Data Protection Act 2023, s 17(2)(a)
[22] Digital Personal Data Protection Act 2023 (India), s 4

necessity, and legality. In violation of the Puttaswamy doctrine, the exemption under section 17(2)(a) also lacks any prior legislative framework granting permission to surveil, does not establish an objective standard of necessity, and does not provide for judicial or parliamentary oversight from an impartial and independent party. Hence, although the DPDP Act confers powers on the private actors in the private sector of both rights and responsibilities, it dismisses bulk surveillance and adopts a relaxed attitude towards collecting state information, which jeopardizes individuals, particularly if we consider scenarios concerning Aadhaar, online policing, or welfare databases.

- **Algorithm Profiling**

India is becoming more reliant on automated systems and computer processes that make decisions without human involvement for doing services such as credit scoring, employee sorting, and even deciding who will get government benefits like food rations, pensions, or health subsidies. This is usually termed algorithmic profiling, which involves using information about people to assign them to categories based on patterns or predictions. The Digital Personal Data Protection Act, 2023 does not say much at all about how such systems are to be governed or whether people are to have any kind of right to challenge or opt out of decisions made solely by algorithms which is concerning owing to India's idea and aim of integrating and including technology in the lives of every Indian citizens.

The definition of "processing" in section 2(x)[23] of the act includes automated activity, but it again excludes protections and transparency. For example, if an algorithm in a government app that determines a pregnant woman's eligibility for maternity benefits decides that she is not entitled to maternity benefits and makes a mistake or discriminates against her, then these people along with those whose lives and claims depend on these systems do not appear to have the legal right to demand a manual decision or to ask why, which is a very big flaw in the provision. In contrast, Article 22 of the GDPR[24] in the EU grants individuals an explicit right not to be subjected to automated decisions that materially affect them. There is no such right in India's law, even though automated systems are being deployed to help in critical areas like

[23] Digital Personal Data Protection Act 2023, s 2(x), s 7
[24] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, art 22 [25] Digital Personal Data Protection Act 2023, s 6

welfare, where flawed systems or bias could prevent the most disadvantaged from receiving required assistance.

- **The Gap between Literacy and The Digital Divide**

Section 6 of the DPDP act[25] clearly emphasizes free, explicit, informed, and unambiguous consent to collect and use data; it also assumes that everyone has an equivalent capacity to understand what they are committing to. As a result of India's significant digital divide and incredibly low levels of technical and legal literacy, many people, particularly those living in rural areas, elderly individuals, non-native English speakers, and even those who are illiterate, may not even be able to provide informed consent. To do this, the Act established a useful provision, section 5(3)[25] stating that notice of consent must be given in both plain English and any language listed in the Constitution's Eighth Schedule. However, despite this safeguard, the issue still exists: the majority of consumers will never be able to read a privacy notice or even comprehend the technical terms of "processing" or "data sharing." People run the risk of technically "consenting" without really understanding what they are consenting to because of this disconnect between social reality and legal form. The Indian context requires the use of alternative methods to make consent effective. Public service announcements in the local language educating individuals about digital rights, interactive videos explaining data consumption, or audio-visual consent messages could all be examples, but would require huge public expenditure to be incurred by the government. In the absence of such efforts, the right to privacy could end up being a privilege that only those who are proficient in digital technology can enjoy.

Reforming the DPDP Act: A Rights-Based, Context-Sensitive Approach

First, let’s take a look at a case study. In 2017-2018, several reported instances of distress originated in Jharkhand, where citizens were being deprived of access to the Public Distribution System (PDS) due to Aadhaar-based biometric failures. The most widely publicized case was that of 11-year-old Santoshi Kumari, who starved to death, allegedly, after she was denied her family's food rations due to repeated biometric failures[26]. Although she and her family were eligible beneficiaries, they were unable to get rations since fingerprint authentication failed,

[25] Digital Personal Data Protection Act 2023, s 5(3)
[26] Scroll Staff, “11-year-old girl dies of starvation in Jharkhand after Aadhaar-linked ration card is cancelled,” Scroll.in (17 October 2017).

and no backup plan was activated. The same occurred across the state, and studies found a pattern of exclusion of the most vulnerable—rural, elderly, and poor citizens. These cases revealed the risks involved in the employment of large-scale digital systems in the absence of proper accountability, transparency, or personal protections, especially where stakes are concerned for access to necessities like food and welfare.[27]

Incidents like these underscore the urgent need for a data protection framework that is not only technologically sound but also ethically grounded and legally enforceable. India's DPDP Act represents a much-anticipated move toward regulating personal data usage in the digital era. Nevertheless, despite the law appropriating heavily from international templates like the GDPR, its efficacy is undercut by structural silences and contextual misalignments. To deliver on its commitment to safeguard citizens in a data-driven world, the DPDP Act needs reform that is at once rights-focused and attuned to India's distinct digital ecosystem.

One of the gravest concerns in the DPDP Act is the wide reach of state exemptions under Section 18, enabling the Central Government to exempt any state instrumentality from major provisions of the Act. The phrasing is comprehensive and does not specifically mandate observance of the principles of legality, necessity, or proportionality, as enunciated by the Supreme Court in Justice K.S. Puttaswamy v. Union of India (2017)[28].

A reformed framework needs to bring in statutory protections to curb executive discretion. State surveillance or data collection must be allowed only when it is authorized by law, required for a legitimate purpose, and proportionate to the purpose, standards based on both constitutional jurisprudence and international human rights law. Otherwise, the DPDP Act will end up facilitating untrammelled surveillance instead of safeguarding against it. India's Data Protection Board, conceived as the major enforcement agency under the Act, does not have institutional assurances that would make it independent of executive control. Its appointments, financing, and monitoring are under central government control, which puts in question its capacity to objectively regulate private and state actors alike[29]

[27] Jean Drèze and Anmol Somanchi, "Aadhaar and Food Security in Jharkhand," The Hindu (27 September 2018); Reetika Khera, "The UID Project and Welfare Delivery in India," Indian Journal of Human Development, 2017.
[28] Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1.
[29] Internet Freedom Foundation (2023), Analysis of the DPDP Bill, 2023, available at internetfreedom.in. [31] Baijal, A. (2023). India's DPDP Bill: Between Global Influence and Local Realities, Indian Journal of Law and Technology.

For the Board to acquire public trust and function effectively, its structure should demonstrate the autonomy of constitutional or quasi-judicial bodies. This entails transparent appointment processes, security of tenure, and administrative independence. Without this autonomy, enforcement risks becoming selective or politically motivated, particularly where influential government departments or large technology firms are concerned. While the DPDP Act recognizes significant rights like access, correction, and erasure, it excludes two significant safeguards inherent in meaningful data autonomy: the right of data portability and the right of objection to automatic profiling.

In a more platform economy, data portability is essential to consumer choice, competition, and digital empowerment. It facilitates the transfer of data from one service to another, preventing vendor lock-in. Similarly, protection against profiling and automated decisionmaking is essential in sectors like healthcare, education, and credit, where algorithmic discrimination can have significant real-world effects.[31] Implementing these rights would not only bring the DPDP Act in line with international norms but also bring India's constitutional promise of equality and procedural justice closer to reality. Above all, any revamp of the DPDP Act has to be grounded in constitutional values—dignity, equality, and due process. Privacy, by the way, is not a luxury in a world of bytes and bits—it is the foundation of personal freedom and democratic citizenship.

That is, it is about reimagining data protection not merely as a regulatory issue, but as part of the greater constitutional project of protecting individual liberty from the more powerful technology. The law must protect us from state intrusiveness as much as corporate excess, particularly in a society where power imbalances—digital, economic, and linguistic—are profound. A rights approach would emphasize the individual not just as a data subject, but as a rights-bearer, and entitled to have open, accountable, and fair treatment in all data transactions.

Conclusion

According to the GDPR, organizations that process personal data must specify the types of personal data they want to process as well as the reason for doing so. Processing personal information is subject to legal requirements, and organizations handling data must adhere to compliance requirements. Thus, Data protection has undergone a paradigm shift thanks to the General Data Protection Regulation (GDPR), both inside and outside of the European Union. In an increasingly digital environment, its broad reach, which includes data subject rights,

compliance requirements, and worldwide enforcement, makes it an effective instrument for safeguarding personal information. While full effects are still in the frame, GDPR has undoubtedly made a difference and changed the way companies approach sensitive data, persuading similar regimes around the world. Against this backdrop, legal professionals need to understand and navigate the nuances of GDPR to ensure privacy and foster trust in digital transactions in a data-driven legal world.