VOLUME 6 | ISSUE 2

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

DIGITAL PRIVACY AND CONSENT IN INDIA: A DOCTRINAL ANALYSIS OF LEGAL PROTECTION FOR INTERNET USERS IN LIGHT OF THE SECTION 6 DPDP ACT, 2023

- Sanjeev H[1]

ABSTRACT

The digital personal data has become part of daily life in India, as people continue to share information regularly to secure simple access to the most important digital services. Digital Personal Data Protection Act, 2023, intends to address this fact, and it attempts to do so with a consent-based framework, highlighting individual autonomy as the central point in the protection of data. The Act provides specific circumstances of valid consent under section 6 such that the consent must be free, specific, informed, unconditional and limited to a given purpose, although it does not refuse the right to revoke consent. Regardless of these precautions, there is concern as to whether consent in the online context can actually serve as a valid exercise of user autonomy.In this paper, a doctrinal analysis of Section 6 of the DPDP Act is done to understand whether the consent framework, as presented, can result in informed and voluntary consent in reality. Placing reliance on Section 6 of the DPDP Act and the case of Puttaswamy (Retd.). v Union of India, it is noted that consent cannot be comprehended as a mere formal or contractual exercise. Rather, it has to be considered against the background of structural power imbalances, information overload, and lack of options on the part of the user that defines modern digital interactions.

The paper relies on the Indian scholarship along with the comparison with the General Data Protection Regulation of the European Union in order to point out the fact that consent is frequently turned into deception without the assistance of a strong interpretation and enforcement. Although the key mechanisms in Section 6 include the limitation of purpose, annulment of invalid clauses of unlawful consent, and ease of withdrawal, the outcome of the

[1] Student at School of Law, CHRIST (Deemed to be University)
For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

https://www.ijalr.in/

mechanisms varies with the intentional interpretation and institutional ability. The paper concludes that Section 6 can provide substantial protection, although such protection is only possible in case the regulators and adjudicatory authorities perceive consent as an ongoing relationship and not a formality.

Keywords: *Privacy, Data protection, Informed Consent, Revoke, Autonomy*.

INTRODUCTION

Digital interactions today are no longer occasional or optional; they are part of ordinary life in India. Whether it is paying bills online, booking a doctor's appointment through a telemedicine app, attending classes on digital platforms, or simply scrolling through social media, individuals constantly share personal data to participate in modern society. Most of the time, this sharing happens through consent mechanisms that are presented on a take-it-or-leave-it basis. Users click "I agree" not because they have carefully weighed the terms, but because refusing often means losing access altogether. It is within this everyday reality that the Digital Personal Data Protection Act, 2023[2] must be located.

The DPDP Act adopts a consent-based framework and places individual autonomy at the centre of personal data protection. Section 6[3], in particular, attempts to define what valid consent should look like by insisting that it be free, specific, informed, and limited to a clear purpose, while also allowing withdrawal. On paper, this mechanism appears to be a strong safeguard. However, the persistence of click-wrap agreements[4]and increasingly opaque data practices raise a fundamental concern: whether these formal requirements genuinely empower individuals, or whether consent has become a procedural formality that masks deeper power imbalances between users and data-processing entities.

This paper begins from the position that consent, although necessary, is an inherently fragile tool in the digital environment. The real issue is not whether consent exists in a technical sense, but whether it can ever be truly informed and voluntary when users face information overload, limited choices, and unequal bargaining power. The central question this paper seeks to address, therefore, is how Section 6 of the DPDP[5]Act can be interpreted and

[2] No. 22 of 2023
[3] No. 22 of 2023, § 6 (India).
[4] Devesh Agarwal, *Analyzing the Landscape of Click-Wrap Agreements*, LiveLaw (Jan. 5, 2024), https://www.livelaw.in/articles/analyzing-the-landscape-of-click-wrap-agreements-245917.
[5]Id. § 6

enforced in a way that gives real meaning to consent, despite cognitive limitations, structural asymmetries, and gaps in institutional enforcement.

Adopting a doctrinal approach, the paper closely examines the language of Section 6, situates it within India's constitutional understanding of privacy, and assesses the safeguards built into the provision. Rather than rejecting consent as a regulatory mechanism altogether, the paper argues for a more realistic engagement with it, one that acknowledges its weaknesses while still exploring how it can be strengthened within India's emerging data protection framework.

LITERATURE REVIEW

The scholarly debate of digital privacy has been concerned long enough as to whether consent can indeed save people in data-driven sophisticated settings. One theme that emerges in this body of work is that consent, despite being the key element in the law of data protection, is not implemented as an actual manifestation of user discretion but rather as a formal.

The theory of privacy self-management, written by Daniel J. Solove[6], is also quite often referred to in the given situation. Solove claims that contemporary data practices put unrealistic expectations on people as they demand them to analyze large and technical data to consent. People can hardly make informed decisions since they have to deal with a large amount of data processing and the lack of transparency in privacy policy. Consent will consequently be turned into a procedure box instead of a substantive protection. This criticism applies especially in India, where digital disparities compound informed decision-making. Julie E. Cohen develops this point by finding the consent in a wider context of informational autonomy.[7] She warns that using consent as a full answer to the harms of privacy is damaging because it will put the burden on individuals, but not structural power imbalances. According to Cohen, legal regimes should not simply enable choice but have a role in helping to maintain the circumstances which allow meaningful autonomy. This point comes in handy when considering Section 6 of the DPDP Act[8] that focuses on voluntariness without explicitly considering the imbalance in the bargaining power between data principals and data fiduciaries.

[6] Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880 (2013).
[7] Julie E. Cohen, What Privacy Is For, 126 Harv. L. Rev. 1904 (2013).
[8] No. 22 of 2023, § 6 (India).

Scholarship on the Indian constitutional aspects of privacy has been predominantly based on the constitutional aspects of the concept of privacy in the ruling of Justice K.S. Puttaswamy v. Union of India.[9] Other experts like Shubha Ghosh have maintained that consent should be evaluated in a context keeping an eye on the limitation of purpose and reasonable expectations. [10]This is in line with Section 6(1) of the DPDP Act, which limits the consent to data that is required to meet a set purpose. Simultaneously, the disconnect between legislative intent and institutional capacity has been pointed out by those who are critically commentating such as Usha Ramanathan, who cautions that rights-based frameworks are likely to be ineffective unless heavily enforced. [11]Another issue that underpins this debate is comparative literature on the GDPR in the European Union. European Data Protection Board[12] regulatory advice and the case of Planet49[13] and Bundeskartellamt v. Meta Platforms[14]show readiness to question consent in cases where there is a power disparity or contractual obligation. Such experience as this implies that consent only acquires practical importance in a condition in which it is reinforced by an active process of interpretation and enforcement.

CONSENT AND PRIVACY IN INDIAN CONSTITUTIONAL JURISPRUDENCE

Any talk of consent under the DPDP Act has to be understood in the larger legal understanding of privacy in India, and this changed dramatically with a decision by the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India[15], which gave a new shape to privacy in India, as privacy is not seen as a limited concept embodied in physical privacy by the court, but within concepts of dignity, freedom, or privacy in decision-making related to one's personal affairs, that is, one's own privacy.

What is noteworthy about the plural voices in the decision in Puttaswamy[16] is the role of control. Informational privacy is characterised by an individual's ability to control the circumstances of information distribution. Consent, in the opinion, was not the ticking of a

[9](2017) 10 SCC 1 (India).
[10] Shubha Ghosh, Consent, Context and the Right to Privacy, 12 NUJS L. Rev. 1 (2019).
[11]Usha Ramanathan, A Word on the Draft Data Protection Bill, 54 Econ. & Pol. Wkly. 12 (2019).
[12] European Data Protection Board,
Guidelines 05/2020 on Consent under Regulation 2016/679 (May 4, 2020).
[13] Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände, Case C-673/17, ECLI:EU:C:2019:801 (C.J.E.U. Oct. 1, 2019).
[14]Bundeskartellamt v. Meta Platforms Ireland Ltd., Case C-252/21, ECLI:EU:C:2023:537 (C.J.E.U. July 4, 2023).
[15](2017) 10 SCC 1 (India).
[16]Id.

box but the practice of freedom. However, the court was also mindful of the tendency to idealize freedom of choice. It was realized that, in certain circumstances, consent can easily become inconsequential to people who are put in a position where they are unable to say no to what is being offered to them.

This notion has been further upheld in later judicial decisions. In the case of Anuradha Bhasin v. Union of India, the Court has recognised that rights on paper can be meaningless if the legal safeguard fails to take note of real-life circumstances. In the case of Internet and Mobile Association of India v. Reserve Bank of India[17], the Court has employed the doctrine of proportionality to make sure that legal provisions do not lose touch with reality in respect to their effect on the individual. This is important in the interpretation of Section 6 of the DPDP Act. This section will not be interpreted in a generic contractual manner, in respect of data transfers, for example. Indeed, it has been rightly observed: "Consent in law must be much more than a formal exercise, and must not be content to remain 'empty in substance'; in other words, it must meet certain expectations, similar to, and in conformity with the judges' articulation in Puttaswamy Although latter was a nine judge decision, it was followed in a constitutionally significant 10 judge bench in K.S. Puttaswamy (Retd.) vs. Union of India. [18]Therefore, Section 6 must be interpreted in accordance with judges' expectations laid out in Puttaswamy to meet appropriate parameters in respect of data fiduciary.

STRUCTURE AND SCOPE OF THE DPDP ACT 2023

Section 6 of the DPDP Act lays down the conditions under which consent by a Data Principal[19]is considered valid. Sub-section (1) sets out the substantive requirements: consent must be free, specific, informed, unconditional, and unambiguous, accompanied by a clear affirmative action. It further incorporates the principle of purpose limitation by requiring that consent be limited to personal data that is necessary for the specified purpose.

The statutory illustration accompanying sub-section (1)[20], involving a telemedicine application requesting access to a user's contact list, is particularly instructive. By explicitly invalidating consent for data that is unnecessary for the core service, the legislature signals an intention to curb overbroad data collection practices. This reflects an implicit recognition of

[17](2020) 10 SCC 274 (India).
[18] (2017) 10 SCC 1
[19]Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 2(j) (India).
[20] DPDP Act § 6(1)

the imbalance between users, who may consent indiscriminately, and platforms, which are incentivised to maximise data extraction.

Sub-section (2)[21] addresses the problem of unlawful or coercive consent clauses by rendering invalid any part of consent that infringes the Act or other applicable laws. The illustration concerning the waiver of the right to complain to the Data Protection Board of India reinforces the non-waivable nature of statutory rights. This provision is significant because it departs from traditional contract law, where parties are generally free to waive rights, and instead prioritises regulatory objectives over private ordering.

Sub-section (3)[22]introduces procedural safeguards by mandating that consent requests be presented in clear and plain language, with accessibility in English or any language listed in the Eighth Schedule to the Constitution. This language need is especially applicable within the Indian context, where digital inclusion has helped to increase the internet penetration among non-English-speaking elites. Responsibility is also enhanced by the requirement to disclose the contact information of a Data Protection Officer or any other authorised representative.

Sub-sections (4)[23]and (5)[24]deal with withdrawal of consent. The requirement that withdrawal be as easy as giving consent is an important corrective to practices that allow frictionless opt-in but impose barriers on opt-out. Concurrently, sub-section (5) makes it clear that the effects of withdrawal are bound to be suffered by the Data Principal and that the previous lawful processing would not be affected. This is a realistic compromise between personal discretion and predictability on the job of data fiduciaries. Combined, Section 6 is a wholesome effort to control consent other than formal. Nevertheless, it is its effectiveness is based upon the interpretation, enforcement, and operationalisation of these requirements. The provision is worded in such a way that it is open to interpretation, especially in situations where informed or free consent can be identified in complicated digital spaces.

THE ILLUSION OF INFORMED AND VOLUNTARY CONSENT UNDER SECTION 6

Despite the detailed safeguards embedded in Section 6, the practical operation of consent in digital environments often falls short of the statute's normative aspirations. The central

[21]DPDP Act § 6(2)
[22] DPDP Act § 6(3)
[23] DPDP Act § 6(4)
[24] DPDP Act § 6(5)

difficulty lies in translating formal legal requirements into meaningful user autonomy. While Section 6 insists that consent be "free" and "informed," these concepts are inherently contextual and vulnerable to erosion in standardised digital transactions.

Informed consent presupposes that the Data Principal understands the nature, scope, and consequences of data processing. However, consent requests are typically embedded within dense privacy notices that are lengthy, technical, and drafted unilaterally by data fiduciaries. Even when such notices are written in "clear and plain language," as mandated by Section 6(3), their sheer volume and complexity may overwhelm users. The law does not currently specify benchmarks for adequacy of disclosure, leaving room for compliance that is technically correct but substantively thin.

Voluntariness presents an even deeper challenge. Section 6(1) requires that consent be "free" and "unconditional," yet most digital services operate on a take-it-or-leave-it basis. Access to essential services, such as digital payments, educational platforms, or health-related applications, is often conditioned on acceptance of broad data processing terms. In such circumstances, the formal presence of a choice obscures the absence of realistic alternatives. Consent obtained under these conditions may satisfy statutory language while failing to meet the constitutional ideal of autonomous decision-making articulated in *Puttaswamy*.[25]

The DPDP Act attempts to mitigate this concern through the necessity limitation embedded in Section 6(1)[26]. By restricting consent to data that is necessary for a specified purpose, the provision implicitly curbs coercive bundling of unrelated processing activities. However, the determination of what is "necessary" remains largely within the discretion of the data fiduciary, subject to ex post review by the Data Protection Board. Without clear interpretive guidance, necessity risks being defined expansively, thereby diluting the protection intended by the statute.

The illustrations appended to Section 6 are notable in this respect. They demonstrate legislative awareness of the risk that consent may be overbroad or exploitative. Yet illustrations, while persuasive, do not carry binding force. Their effectiveness depends on whether adjudicatory and regulatory bodies are willing to draw normative conclusions from

[25] (2017) 10 SCC 1
[26] DPDP Act § 6(1)

them. Absent such willingness, the gap between statutory promise and practical reality persists.

COMPARATIVE DOCTRINAL INSIGHTS: CONSENT UNDER THE GDPR

It is imperative to look at the equivalent in the European Union of our Act on consent and how it has evolved. For instance, in comparing the General Data Protection Regulation (GDPR)[27] of the European Union and our Section 6 on consent, it can be observed that both require consent to be freely given, specific, informed, and unambiguous. The difference lies in the level of detail in the EU's definition of consent.

The European Data Protection Board (EDPB)[28] has repeatedly underlined that consent cannot be considered as "freely given" when a clear imbalance exists between the party seeking consent and the data subject. This applies with heightened emphasis to public authority controllers and major private online actors. The GDPR further specifically provides the situation in which consent becomes void when the performance of a contractual obligation depends on processing which is not required for the obligation. This applies with heightened emphasis to the necessity limitation in Section 6(1) of the old Act.

The Court of Justice of the European Union has made the position even clearer through a number of judgments. In the Planet49[29] decision, the Court simply reaffirmed the need for affirmative action in the Planet49 decision by confirming that pre-ticked boxes are not a valid form of consent. In the Bundeskartellamt v. Meta Platforms[30] decision, the relationship between dominance in the market and the matter of consent was also considered.

However, the unique aspect about the EU experience is that it encompasses the text of the law as well as the interpretive regime that pervades the particular piece of legislation. There are guidelines provided, as well as audit action, which carries substantial fines for violation. Consent, as a result, is neither static nor a one-time occurrence, as it is subject to review. At

[27]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 (General Data Protection Regulation), 2016 O.J. (L 119) 1.
[28] European Data Protection Board, Guidelines 05/2020 on Consent under Regulation 2016/679 (May 4, 2020).
[29] Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände, Case C-673/17, ECLI:EU:C:2019:801 (C.J.E.U. Oct. 1, 2019).
[30]Bundeskartellamt v. Meta Platforms Ireland Ltd., Case C-252/21, ECLI:EU:C:2023:537 (C.J.E.U. July 4, 2023).

this stage, the DPDP Act is backend, meaning that the Data Protection Board has not developed much interpretive capacity.

However, this analogy does not mean that Indian jurists should fall back on the EU model simplistically. There are also different market structures, regulatory capabilities, and digital inclusion considerations in both contexts. However, the Indian experience in this regard can show that consent can be given teeth if it is paired with proper enforcement and constructive interpretation. This can be achieved with the help of the relevant doctrine in Section 6 of the DPDP Act.

Enforcement and Institutional Constraints in the Indian Framework

Ultimately, the success of Section 6 rests on its implementation. The DPDP Act designates the Data Protection Board of India as the central adjudicatory authority for enforcement. Although the establishment of a specialised body is welcome news, a number of concerns pertaining to its ability to meaningfully govern consent practices do arise. First, the Board's role is largely passive. While it may investigate complaints and issue fines, it does not have direct rulemaking or guideline-setting powers like the EU data protection authorities. Without extensive subordinate legislation, the meaning of important terms, like "informed," "free," and "necessary"-may remain incompletely developed.

Second, scale further complicates enforcement. India's digital ecosystem involves millions of data fiduciaries and hundreds of millions of users. The onus of having individual data principals police consent violations through complaints places an undue burden on the users, most of whom lack either awareness or resources. These dynamic risksreproduce the very power asymmetries that Section 6 seeks to address.

Third, penalties alone may not suffice to correct structural consent failures. While the DPDP Act provides for significant monetary sanctions, enforcement actions are likely to focus on egregious violations rather than routine design practices that subtly undermine informed consent. Without proactive audits or sector-specific standards, consent may continue to function as a formal compliance ritual rather than a substantive safeguard. These institutional constraints put into sharp relief the limitations of a consent-driven model. Section 6 cannot work in isolation but rather requires interpretive clarity, administrative capacity, and complementary regulatory interventions. Otherwise, the promise of user empowerment risks being overshadowed by the realities of digital power.

STRENGTHENING SECTION 6: INTERPRETIVE AND REGULATORY PATHWAYS

While Section 6 of the DPDP Act[31] contains several substantive safeguards; its effectiveness depends on how these safeguards are interpreted and operationalised by regulators and adjudicatory bodies. Rather than requiring legislative amendment, many of the shortcomings identified can be addressed through purposive interpretation and regulatory clarification.

The courts tend to go for the purpose-driven approach when Indian courts and regulatory bodies need to interpret laws that involve fundamental rights. Coming to Section 6, the demand that consent is "free" isn't just about the absence of physical pressure. It's about ensuring that the user is in a position to make a choice, and that's not the case when they're given access to digital services in exchange for consent to data processing that isn't necessary for the service. The ruling in Puttaswamy v. Union of India in 2017[32]makes clear that autonomy is not about empty formalities, and is similar to what is being sought in Section 6 with this interpretation. "Informed" consent should be interpreted to mean more than just clear language, and more along the lines of transparency. Think layered notices, standardised summaries and purpose-specific explanations that would let users really get what's going on. Even though Section 6 does say that the language must be clear and plain, regulatory bodies can breathe life into this requirement by setting out the bare minimum that companies must tell their users.

The necessity rule in Section 6(1)[33] is a key yet underutilised aspect of the law. To stop wide reading by data controllers, the Data Protection Board should test necessity using a proportionality standard. This would ask if the data use is logically linked to the goal, if less intrusive ways could be used, and if the data collected is proportionate to the benefit the service provides. This rule would utilise existing legal principles regarding proportionality, thereby keeping data protection within familiar legal territory. Over time, Board decisions based on this test could create a kind of precedent that would be easier to predict and hold accountable.Section 6(4)[34]acknowledges that there is the right to withdraw the consent as easily as the consent is given. This is included in response to a typical asymmetry of digital design, with the ease of opt-in processes being contrasted with a complex opt-out process.

[31] DPDP Act § 6
[32](2017) 10 SCC 1
[33] DPDP Act § 6(1)
[34] DPDP Act § 6(4)

Regulators may implement this requirement by ensuring that the withdrawal mechanisms are visible and easily accessible by the same interface as used to consent.

Meanwhile, Section 6(5)[35]makes it clear that withdrawal repercussions are to be incurred by the Data Principal. Although this is a pragmatic acceptance of the realities of operation, one should not understand this to be an endorsement of punitive or disproportional outcomes. Regulatory advice can draw a line between the outcomes that are inseparable from the provision of the service and those outcomes which merely punish the exercise of a statutory right. DPDP Act presents the notion of consent managers that may become intermediaries and consent on behalf of Data Principals. Despite the fact that this mechanism is not described in Section 6 itself, it can potentially alleviate cognitive overload and equalise power relationships. Effectively controlled consent managers would provide users with a standardised way of giving, checking and revoking consent across platforms. Nevertheless, this model can only be effective when it is strictly supervised to make sure that the consent managers will act on behalf of the users and not become agents of the data fiduciaries. Fiduciary accounts, transparency and accountability measures are necessary in case consent managers are supposed to improve instead of undermine autonomy.

CONCLUSION

In India, the Digital Personal Data Protection Act, 2023, is an important milestone in the changing Indian digital governance system. Section 6, especially, represents the bold effort to base the protection of data on personal consent, relying on the best practices and constitutional principles of autonomy and dignity worldwide. Its elaborate statement of consent conditions, such as the voluntary nature, restriction of purpose, accessibility, and withdrawal are a breakthrough to the previous and piecemeal approaches to data regulation in India. However, this paper has suggested that the concept of consent as operationalised in the modern digital spaces is a very weak protection. The restrictions imposed by cognition, structural power inequalities and institutional constraints threaten to turn consent into a legal fiction, valid in form but empty of substance.

When section 6 is interpreted in a narrow or mechanical sense, it will not contribute to safeguarding the very autonomy that it is intended to facilitate.Its provisions can be used to enhance protection to the users through the application of purposive interpretation, strong

[35] DPDP Act § 6(5)

enforcement and judicious regulatory guidance. The necessity restriction, the nullification of illegal consent provisions, linguistic comprehensibility, and the right to revoke consent all offer doctrinal devices that can correct the imbalances of the real world. Finally, the institutional will of the DPDP Act consent framework will not rely on statutory text but rather on institutional will. In case regulating and adjudicating bodies view consent not as a transaction but as a relationship, as it existed before, then Section 6 will become a substantial protection of digital privacy in India. That way, it will be able to neutralise the divide between formal legal design and lived digital reality, so that consent is not used as an illusion of control, but as an exercise of individual autonomy.