RECONSIDERING CONSENT: AN EVALUATION OF THE EFFECTIVENESS OF DATA PRINCIPAL RIGHTS UNDER INDIA'S DPDP ACT, 2023 IN RELATION TO THE EU GDPR

Vijay Shalini Prajapati**,** B.A.LL.B. (Hons.), Atal Bihari Vajpayee School of Legal Studies, Chhatrapati Shahu Ji Maharaj University, Kanpur.

ABSTRACT

The rapid growth of the digital economy has turned personal data into a precious economic asset, and the issue of privacy, personal autonomy, and information management has become highly important. *Consent* has in its turn become one of the focal points of legal processes in the contemporary data protection systems. In this paper, the role and efficacy of consent, as specified in the Digital Personal Data Protection Act, 2023 of India, are considered and put into a comparison with the European Union's General Data Protection Regulation.

The paper concludes that despite the structured consent-based framework, which the DPDP Act entails and the data principal rights it grants, the practicality of the DPDP Act is constrained by structural and institutional problems. These consist of a comparatively limited range of rights, generalized provisions that concern the reasonable use and exemptions of the states, and issues of enforcement and awareness to the user. Conversely, the GDPR is more robust and rights-focused, with the consent working together with other legitimate reasons and with more enforceable rights and more powerful regulatory frameworks.

It follows a doctrinal and comparative approach to the study, examining the legislative provisions, judicial rulings, and academic sources on the topic to assess the extent and legitimacy of consent as a legal foundation to process data. It also evaluates the character and the scope of data principal rights as per the DPDP Act and contrasts them with the data subject rights framework as per the GDPR. The main questions concerning informed consent, consent fatigue, information asymmetry, and the influence of dark patterns on user decision-making are also discussed.

Keywords: Data Protection, Consent, Data Principal Rights, GDPR, Consent Fatigue, Dark Patterns, State Exemptions.

INTRODUCTION

The rise of digital technology on a global scale has changed the way we produce, gather and use personal information within our society. Thus, personal information is no longer incidental in today's economy. It is treated as an economic commodity with a high potential value, creating the potential for governments, corporations or digital platforms to use it to foster innovation, create or improve the delivery of goods or services and to improve the decision-making processes for businesses or public officials. Nevertheless, the extensive collection of data has raised concerns regarding issues related to individual privacy, surveillance and the loss of autonomy, necessitating the need for governments to create a comprehensive legal and regulatory framework to protect individuals and regulate the collection and use of their personal information.

Traditionally, the concept of privacy is defined as the "right to be let alone".[1] However, in the digital era this has been supplemented by the concept of 'informational privacy'. *Informational privacy* focuses on the right of an individual to control and regulate the gathering, utilization and sharing of personal information of the person. This change was constitutionalized in *Justice K.S. Puttaswamy v. Union of India* in which the Supreme Court categorically declared that right to privacy was a fundamental right in Article 21 of the Constitution.[2] The ruling emphasizes that informational self-determination is inherent to personal liberty and human dignity and, thus, this forms the normative basis of the data protection law in India.

However, globally, the recognition of privacy as a basic right has resulted in the establishment of extensive regimes of data protection. Early data protection regulations were mainly concerned with preventing unauthorized access and access to data and confidentiality. Eventually, this focus changed to giving individuals more power and control over their own personal data. The European Union's General Data Protection Regulation which was enforced in May of 2018 is one of the best examples of this evolution in data protection law.[3] The EU GDPR is a fundamental change in data protection laws as it creates a new rights-based method of presenting data protection laws using core principles such as accountability, transparency and fairness. It imposes new and significant responsibilities on those who process data.

[1] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 195 (1890).
[2] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016 O.J. (L 119) 1 (GDPR).

In the case of *Google Spain SL V. Agencia Española de Protección de Datos,* the Court of Justice of the European Union recognised "the right to be forgotten" which allows individuals to ask for their information to be removed from search results.[4] Similarly, the Court in *Data Protection Commissioner v. Facebook Ireland Ltd,* emphasised the importance of protecting data through high standards in cross-border processing of data because of concerns regarding surveillance .[5]

On the other hand, the journey of India towards the development of an overall data protection system has been slow and very recent. Before any dedicated laws existed to protect data, protections have been subsections of the Information Technology Act, 2000[6] and rules regarding Sensitive Personal Data or Information (SPDI) rules, 2011[7]. Nevertheless, this law was weak in terms of scope as well as enforcement.

Moreover, the *Puttaswamy*[8] ruling was a turning point in the history of India in its legal system since it demonstrated that there was an urgent necessity to have a comprehensive law that would have addressed all issues related to the management of personal data. This resulted in the formation of the Justice B.N. Srikrishna Committee on data protection, the report of which in 2018 formed the basis of a legislative change.[9] Several draft bills later, the Digital Personal Data Protection Act, 2023[10] was adopted, and it is a major milestone in the organization of data management in India.

One of the key aspects of contemporary data protection systems is "*consent"* as a tool of data processing legitimization. Gaining consent is an essential part of promoting individual autonomy by giving individuals sufficient knowledge and understanding so they can make informed decisions regarding how their data is going to be processed. Moreover, both GDPR and DPDP Act recognize consent as a key legal basis for data processing. However, the practical effectiveness of consent has been widely in question. In a digital world, the user often accepts a long-winded and complicated privacy policy which is commonly known as 'consent

[4] *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, Case C-131/12, ECLI:EU:C:2014:317 (2014).
[5] *Data Prot. Comm'r v. Facebook Ireland Ltd.* (Schrems II), Case C-311/18, ECLI:EU:C:2020:559 (2020).
[6] Information Technology Act, No. 21 of 2000, India Code (2000).
[7] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) (India).
[8] *Puttaswamy*, *supra* note 2.
[9] Justice B.N. Srikrishna Comm., *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018).
[10] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

fatigue'. Due to this fact, consent is usually viewed as merely going through a process to consent as opposed to a genuine decision.

In addition, many digital platforms use interface design known as 'dark patterns' which influence users consent to use personal data. These practices will negatively impact the voluntary and informed nature of consent and raise questions about consent being an effective means of securing our privacy. These issues highlight a fundamental tension within data protection law, and consent is designed to provide consumer with control over their own personal data but it might in reality, not offer real control of personal data.

The first complete effort made by India to cover these concerns is the Digital Personal Data Protection Act 2023[11]. The Act provides a framework that is consent-based to provide consent to the processing of digital personal data between data principals and data fiduciaries. Under this act, the consent should be free, specific, informed and unambiguous. Moreover, the introduction of "Consent Managers" reflects an effort to enhance user control by providing accessible mechanisms for managing consent.

Furthermore, the DPDP Act also adopts a flexible method of processing data without consent under 'legitimate uses' i,e., state functions or complying with the law and during emergency situations. While such provisions facilitate better management and efficiency in the Government and administration of services but on the other hand, also raises concerns over potential overreach of the act and the reduction of individual protection. Additionally, the rights of Data Principals such as right to access, correct, delete and have grievances addressed are comparatively limited than those provided under the GDPR. Conversely, the GDPR include the concept of consent in a wider rights-based framework, which is backed by strict duties and effective enforcement schemes.

In light of this, the goal of this current study is to critically compare the effectiveness of the DPDP Act's data subject rights to the GDPR. Moreover, it looks at the question of whether the consent clauses of both these regimes are real act of empowering people or merely a mere appearance of law.

This paper argues that although both the GDPR and the DPDP Act use consent as a framework mechanism, the former offers a more efficient and rights-focused system because it introduces

[11] *Id.*

consent into a comprehensive system of enforceable rights and institutional responsibility.

LITERATURE REVIEW

1. Evolution of Privacy as a Legal Concept

Privacy has not only changed its classical definition of privacy as a "right to be let alone" given by *Samuel D. Warren and Louis D. Brandeis*[12], but also has taken a more intricate meaning of informational privacy in the digital age. This development is an indication of the transformation of physical and spatial privacy to personal data and individual autonomy security. The emergence of new digital technologies has led to a more liberal view of the concept of privacy, placing more focus on the control over personal information and its sharing.

2. Theoretical Basis of Consent and Informational Self-Determination.

"The privacy as control over personal information" theory by *Alan F. Westin* made a significant impact on the current data protection models, especially the prominence of consent.[13] However, researchers such as *Daniel J. Solove* have critically criticized this model that is founded on consent because he claims that in most cases, people cannot make informed choices as a result of the complexity of data processing practices.[14] *Helen Nissenbaum* theory of "contextual integrity" also questions the sufficiency of consent because it focuses on the relevance of information flows instead of individual choice.[15] These theoretical views point to the weaknesses of using consent as one-dimensional tool of privacy protection.

3. Scholarly Analysis of the GDPR Framework

The GDPR[16] has been widely studied as a comprehensive and rights-based model of data protection. Researchers like *Paul Voigt and Axel von dem Bussche* highlight that it places a high value on accountability, transparency, and enforceable data subject rights.[17] *Lee A. Bygrave* stresses its influence on other countries in particular due to its extraterritorial

[12] Warren & Brandeis, *supra* note 1.
[13] Alan F. Westin, *Privacy and Freedom* 7 (1967).
[14] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880, 1883 (2013).
[15] Helen Nissenbaum, *Privacy in Context* 127 (2010).
[16] GDPR, *supra* note 3.
[17] Paul Voigt & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* 9 (2017).

application and severe enforcement means.[18] Whether or not the GDPR rights, including the right to erasion and data portability can be applied in the context of augmenting individual autonomy and control of personal data, is also a subject of academic discussion.

Although it is a highly detailed document, the GDPR has not escaped criticism. Researchers have cited obstacles like compliance costs, regulatory overload, and the continued existence of problems, e.g., consent fatigue and dark patterns vanishing.[19]

These objections imply that sophisticated regulatory systems have constraints in guaranteeing meaningful user control, and that more general issues of the suitability of consent-based approaches in digital space are at stake.

4. Evolution of Data Protection Law in India

In India, the constitutional developments have been largely associated with the development of data protection law, especially the introduction of privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India*.[20] The recommendations of the Justice B.N. Srikrishna Committee[21] that mirrored a structured data protection system that would not discriminate against the interests of individuals. This was a big stride towards the adoption of enactment of comprehensive legislation.

5. Scholarly Perspectives on the DPDP Act, 2023

The current state of the Digital Personal Data Protection Act, 2023[22] is mixed in terms of evaluation presented by the recent literature. Other researchers consider the Act as a practical and context-specific document that is adapted to the socio-economic situation in India. Other people however criticize its narrow construal of rights, wide exemption of states and consent as a major mode. Issues have also been brought up on the capability of enforcement and efficiency of institutional mechanisms under the Act.

6. Research Gap and Relevance of the Study

Although there is ample literature on the topic of data protection, there is still a lack of critically

[18] Lee A. Bygrave, *Data Privacy Law: An International Perspective* 165 (2014).
[19] Solove, *supra* note 14.
[20] *Puttaswamy*, *supra* note 2.
[21] Srikrishna Comm., *supra* note 9.
[22] Digital Personal Data Protection Act, 2023, *supra* note 10.

analysing the effectiveness of data principal rights under the DPDP Act in comparison with the GDPR. The extant research is inclined to either theoretical criticism of consent or descriptive analysis of specific frameworks but lacks an adequate discussion of their practical implication in comparative terms.

The present research aims at filling this gap by taking a doctrinal and comparative approach to the question of whether the consent-based framework of the DPDP Act provides significant protection of individual autonomy, and whether it can be compared to a more developed and rights-oriented framework of the GDPR.

RESEARCH OBJECTIVE

- To critically analyse the concept and role of consent under the DPDP Act, 2023.
- To examine the nature, scope and restrictions of Data Principal rights.
- To draw a comparison between the Indian regime and the Data Subject rights regime as provided by the GDPR.
- To assess the extent to which the DPDP Act provides substantive informational control or procedural compliance.
- To determine structural gaps, such as state exemptions, and enforcement issues.
- To propose suggestions improvements and strengthening India’s data protection act.

RESEARCH QUESTION

1. Whether consent, as a legal basis under the DPDP Act, 2023 and the GDPR, effectively ensures meaningful control over personal data?
2. What is the comparison between the data principal right under the DPDP Act, 2023 and the rights of the data subjects under the GDPR?
3. Whether "legitimate uses" under the DPDP Act change the importance and usefulness of consent as a way to protect people?

4. Is the GDPR more effective and enforceable in terms of data protection than the DPDP Act, 2023?

RESEARCH HYPOTHESIS

- *The consent-based model of the DPDP Act, 2023 is relatively weaker than the GDPR to provide effective protection of personal data, as it has wider exceptions, fewer data principal rights, and weaker enforcement tools.*

- *In the context of the broad rights framework, a more varied set of lawful bases, and more robust enforcement mechanisms that the GDPR presents in comparison with the DPDP Act, the GDPR offers a more effective data protection framework than the DPDP Act, leading to over-reliance on consent.*

RESEARCH METHODOLOGY

This paper follows the research methodology of a doctrinal and comparative research in order to explore the effectiveness of consent as a legal foundation of protection of data. The doctrinal approach entails a critical study of the primary legal sources such as statutory clauses, judicial rulings and regulatory frameworks of the law of data protection. Specific attention, in this case, is paid to the Digital Personal Data Protection Act, 2023 (DPDP Act) and the General Data Protection Regulation (GDPR) as the main legal tools that are being analysed.

Critical analysis of judicial pronouncements has been done to appreciate the development of privacy and consent in various legal systems. Some of the landmark cases, including Justice *K.S. Puttaswamy v. Union of India*[23], *Google Spain SL v. AEPD*[24], *Planet49 GmbH*[25], *and Data Protection Commissioner v. Facebook Ireland Ltd. (Schrems II)*[26] have been discussed to analyse how principles regarding the informational privacy, user autonomy and consent validity develop.

Besides the primary sources, the research is based on secondary sources such as scholarly articles, legal commentaries, policy reports and academic literature. The sources will help undertake a critical approach to both theoretical underpinnings and practical issues of consent-

[23] *Puttaswamy*, *supra* note 2.
[24] *Google Spain*, *supra* note 4.
[25] *Bundesverband der Verbraucherzentralen v. Planet49 GmbH, Case C-673/17, ECLI:EU:C:2019:801 (2019).*
[26] *Schrems II*, *supra* note 5.

based data protection systems.

The study also uses a comparative method to find out the similarities and differences between the GDPR and the DPDP Act especially concerning consent requirements, the extent of individual rights, lawful grounds to process and enforcement provisions. The comparative analysis allows evaluating the relative strength and weaknesses of the Indian data protection regime as compared to the existing international standard.

It is a qualitative study that does not entail the collection of empirical data. Rather, it is concerned with interpretative and analytical analysis of law texts and systems. The aim is to critically evaluate the issue of whether consent as it is formulated under these regimes provides a sufficient level of protection to individual autonomy in the changing digital environment.

CONCEPTUAL FRAMEWORK OF CONSENT IN DATA PROTECTION

Consent is the main component that forms the basis of the modern data protection rules and offers the users the right to control their personal data. Consent allows people to willingly authorize the handling of their personal information that companies will use to attain certain operational goals. These are the core tenets of modern privacy jurisdiction, and have been supported by constitutional and regulatory trends in different jurisdictions. This was determined by the case of *Justice K.S. Puttaswamy v. Union of India* in India where the Supreme Court stated that informational privacy is one of the imperative elements of the Article 21, that mandates human beings to possess the authority to manage their own data.[27] Consent is a critical aspect of data protection systems that is stipulated by the constitution.

In addition, both the General Data Protection Regulation and the Digital Personal Data Protection Act, 2023 are largely reliant on consent as a prerequisite to legal processing of personal data. Article 4(11) of the GDPR refers to the *consent* as "freely-given, specific, informed and unambiguous expression of the desires of the data subject".[28] While Article 7 further explains the conditions that establish its validity.[29] Similarly, the DPDP Act requires consent to be free, specific, informed and unambiguous which aligns with international standards for consent requirements. The elements combine to create an effective system which

[27] *Puttaswamy*, *supra* note 2.
[28] GDPR art. 4(11).
[29] *Id.* art. 7.

shows that consent functions as more than a necessary procedure but as a true demonstration of personal selection.

Furthermore, to have a valid consent legally, it should meet some requirements. Firstly, consent should be free meaning that it should be voluntary and without coercion, undue influence, and power imbalance. In *Bundesverband der Verbraucherzentralen v. Planet49 GmbH*, the court stated that pre-ticked checkboxes are not valid consent as they cannot be shown to be an active and deliberate decision.[30] *Secondly*, consent should be informed, which means that people should be given clear, accessible, and detailed information about the nature, scope, and purpose of data processing. The GDPR implements this requirement by the transparency requirements of Articles 12 to 14. *Thirdly*, consent should be specific, that is, it should pertain to the well-articulated purposes that will not be combined in various unrelated processing operations. This principle was cemented in *Google LLC v. CNIL* that underlined the relevance of purpose limitation.[31] Lastly, the consent should be unambiguous, i.e. it has to be a clear act of affirmation. As lack of action and inactivity, as well as the implication of consent should not be regarded as a relevant consent in the modern data protection regulations.

Even with this strong legal framework, consent in the digital world is still complicated. In contrast to the traditional contractual relationships, the digital consent is usually received with the help of standardized interfaces, including click-wrap contracts and privacy disclosures, which usually restrict substantive user interaction. This raises crucial questions on whether consent in such cases constitutes an act of free and informed choice or is simply a formality that makes data processing legal. This problem is aggravated by the imbalance of power between data fiduciaries and individuals. The concept of unequal bargaining power that was recognized in *Central Inland Water Transport Corporation v. Brojo Nath Ganguly* is relevant in this regard to consider the validity of consent obtained in the digital world.[32]

Current data protection laws recognize these boundaries, and do not only use consent. The GDPR is also a pluralistic document which provides a number of valid reasons to process. According to Article 6, includes contractual necessity, adherence to legal requirements, safeguarding vital interests, carrying out public duties, and legitimate interests.[33] Such a

[30] *Planet49*, *supra* note 25.
[31] *Google LLC v. CNIL, Case C-507/17, ECLI:EU:C:2019:772 (2019).*
[32] *Central Inland Water Transport Corp. Ltd. v. Brojo Nath Ganguly, (1986) 3 S.C.C. 156 (India).*
[33] GDPR art. 6.

strategy acknowledges that permission is not an appropriate and reliable foundation of processing in certain contexts, particularly in the case of unequal bargaining power, as in employer-employee associations. The DPDP Act is also granted such flexibility in the term of "legitimate use" under Section 7, that allows processing without consent in some instances such as emergencies, state activities, and legal requirements.[34] The extent of these exceptions has been criticized especially in light of the possibility of governmental overreach and the weakening of individual liberties.

Practical usefulness of consent is also compromised by various structural issues of the digital ecosystem. Besides, one of the most significant issues is *Information asymmetry*, where data fiduciaries possess much more resources, expertise, and knowledge than individual users, is among the most significant ones. This inequality reduces the ability of people to make fully informed decisions and undermines the autonomy principle that the concept of consent is based on. The fact that people have few real alternatives also creates a take-it-or-leave-it situation through the existence of standardized, non-negotiable agreements.

The "illusion of choice" is another important issue. Technically, users have the right to revoke consent, yet, in practice, they must accept conditions of data processing to employ significant online services. This actually coerces them to consent which is not in line with the fact that they are expected to do so on their own. Moreover, the complexity and incomprehensibility of the modern methods of data processing, characterized by artificial decision-making and the broad dissemination of data, make it extremely difficult to make people say full consent to the impact of their actions.

These structural problems are intensified with behavioural and design issues. The phenomenon of "Consent fatigue" occurs when individuals receive multiple requests to grant consent and therefore, they tend to blindly accept terms without paying attention to the meaning of those terms. Due to this fact, consent has turned into a habitual, automatic act rather than a decision. This is directly connected to the concept of so-called "dark patterns" that are deceptive design elements employed by digital platforms to alter the behaviour of people. The practices include some confusing interfaces, options that cannot be seen, and default settings, which are easier to say 'yes'. The European Data Protection Board and other regulatory authorities in the European Union have clarified that consent that is obtained by means of deceit or manipulation

[34] Digital Personal Data Protection Act, 2023, § 7.

would be against the requirements of the GDPR. This clarifies the fact that there exists a distinction in formal compliance and substantive protection.[35]

The theoretical frameworks of privacy and autonomy provide better insights into how consent fails to deliver its promised benefits. The liberal theory of autonomy assumes that individuals are rational actors capable of making informed decisions, which are the basis of the trust to consent as a tool of regulation. The research from behavioural economics proves that people make poor decisions in digital environments because they lack proper attention and face cognitive limitations which prevent them from understanding complex situations. Informational self-determination, a term coined in German constitutional legal thought, focuses on the principle of personal control over personal data, but at the same time, structural protections beyond the consent of the individual are acknowledged.

Further, Helen Nissenbaum's *theory of privacy* as contextual integrity provides a critical view of privacy because it shows that privacy extends beyond personal control to include proper information distribution in particular social settings.[36] The new approach shifts its attention from individual consent to the comprehensive set of rules that regulates data usage practices. Through their studies, the academic community has found out that individuals encounter what researchers refer to as the "consent paradox", since they need to make decisions concerning things which they do not have an in-depth understanding.

It is obvious that consent is a significant element in the law of data protection, yet it cannot stand alone. Its practical and theoretical restrictions also require a wider regulatory framework that includes accountability, transparency and enforceable rights. This conceptual framework provides the analytical foundation for evaluating the effectiveness of consent and data principal rights under the DPDP Act, 2023 in comparison with the GDPR in the subsequent sections.

CONSENT MECHANISM AND DATA PRINCIPAL RIGHTS UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The first comprehensive legislation in the country concerning the processing of digital personal data is Digital Personal Data Protection Act, 2023[37]. The Act, which was brought about by

[35] Eur. Data Prot. Bd., *Guidelines 05/2020 on Consent* (2020).
[36] Nissenbaum, *supra* note 15.
[37] Digital Personal Data Protection Act, 2023, *supra* note 10.

constitutional acknowledgement of privacy[38] and affected by international regulatory factors, aims at bringing a structured equilibrium between the rights of individuals and the valid demands of both the State and the private organizations. The centre of this framework lies the concept of *consent* that serves as the main legal foundation of data processing and as a way of giving individuals, also known as *Data Principals*, control over their own personal data.

As Section 4[39] of the Act states that the personal data can only be processed under the conditions of the legislation i.e., based on the consent or on some specific mentioned "legitimate uses". Section 6[40] establishes the requirements of a *valid consent*, which must be free and specific, informed, unconditional, and unambiguous and must be manifested by a definite affirmative act. This statement indicates a deliberate compliance with international norms, especially those that are represented in the GDPR. Nevertheless, the addition of the word "unconditional" brings about a certain ambiguity, particularly when dealing with digital services in which accessibility frequently depends on user consent. Thus, this casts doubt on the actual voluntariness of consent.

The Act also provides additional support to the consent framework by tying the consent to the "notice" provisions of Section 5[41]. According to this sec the *Data Fiduciaries* must provide a clearly, accessible and understandable notice to the *Data Principal* and under which hey state the state the purpose of processing, nature of personal data collected, and rights that the individual is entitled to. This is a requirement aimed at operationalizing the requirement of informed consent through a provision of transparency. But practically, the length and technicality of such notices is likely to persist and this adds to informational overload and reduces their usefulness in facilitating meaningful understanding on the part of the user.

Further, the concept of "Consent Managers" is an important institutional innovation brought about by the DPDP Act. These bodies are to be used as a mediator that will allow Data Principals to provide, administer, review, and revoke consent using available platforms. Although this mechanism can potentially increase the level of user control and simplify the consent management, its efficacy will rely on the regulatory clarity, technological implementation, and the level of independence that such entities will have.

[38] *Puttaswamy*, *supra* note 2.
[39] Digital Personal Data Protection Act, 2023, § 4.
[40] *Id.* § 6.
[41] *Id.* § 5.

Further, the DPDP Act also establishes a framework of rights for Data Principals which includes-

- right to receive information on the personal data under processing (Section 11)[42]
- right to correction and erasure (Section 12)[43]
- right to redress grievances (Section 13)[44]
- right to nomination of another person to exercise rights in case of death or incapacity (Section 14)[45]

Although these rights are a significant move towards empowering the user, they remain comparatively limited when compared to international standards such as the GDPR, which give other rights, such as data portability and the right to object to processing.

Further, the important point about the Act is that consent cannot be the fundamental foundation of all data processing processes. Under Section 7 introduce the "legitimate uses" concept where processing without consent is permitted under particular circumstances, including state purposes, adherence to legal requirements and under emergencies.[46] Although this provision increases flexibility and makes governance easier, it also becomes an issue of whether it can be widely interpreted and abused especially in terms of state surveillance and administrative discretion.

Additionally, the Act allows the Central Government to give exemptions under the Section 17 on the basis of sovereignty, State security, and people order.[47] Such exemptions greatly restrict the relevance of Data Principal rights in some situations and represent a policy decision in Favor of state interests in addition to individual privacy. This balancing strategy creates a difference between the DPDP Act and more rights-focused frameworks such as GDPR and has been an area of significant scholarly and policy controversy.

[42] *Id.* § 11.
[43] *Id.* § 12.
[44] *Id.* § 13.
[45] *Id.* § 14.
[46] *Id.* § 7.
[47] *Id.* § 17.

Another important feature of the consent framework is the *right to withdraw consent.*[48] The Act states that Data Principals should have the capacity to revoke the consent in the same manner one gave it. Although this is consistent with the global standards but its application in real life is questionable, especially in sophisticated digital ecosystems where the data can already be shared or passed through various parties.

Overall, despite the fact that the DPDP Act creates an organized system of consent-based regime, it is limited in its effectiveness by both pragmatic and institutional factors. The dependency on consent within the settings of power asymmetry, informational asymmetry, and complexity of technology makes it questionable whether it can provide real user control. These issues are also reinforced by the fact that Data Principal rights are very limited and the State has a wide range of exemptions. Therefore, the interplay between consent, legitimate purposes, and state exemptions indicates a regulatory policy that favours flexibility and regulation, and individual autonomy, thus requiring a relative assessment with more rights-cantered policies, like the GDPR.

CONSENT AND DATA SUBJECT RIGHTS UNDER THE GENERAL DATA PROTECTION REGULATION (GDPR)

The General Data Protection Regulation (GDPR)[49], implemented in 2018 is commonly viewed as the most extensive and potentially impactful data protection model in the world. It is a paradigm shift of the fragmentation and compliance-based models to a holistic and rights-based regime where individual autonomy, transparency and accountability are at the centre stage. The Regulation is not just a procedural framework but a substantive legal framework which aims to re-equilibrium power between individuals and entities that handle personal data. Its application as stated under Article 3, it has extraterritorial jurisdiction as it not just applicable to the territories of the European Union but also to organizations that are not EU members but process the personal data of EU citizens, thus it significantly expanding its international regulatory effect.[50]

The GDPR is based on the principles established in the Article 5 which apply to all of the data processing. These includes lawfulness, fairness, and transparency, purpose limitation, data

[48] *Id.* § 6(4).
[49] GDPR, *supra* note 3.
[50] *Id.* art. 3.

minimization, accuracy, storage limitation, integrity and confidentiality and accountability. [51] These principles are no longer aspirational but impose a binding obligation upon data controllers and processors which requires them to show compliance. These principles were emphasized in case of *Rigas satiksme v. Datu valsts inspekcija*, when the Court made a point that processing should comply strictly with the principle of purpose limitation and necessity. [52]

Under Article 4(11) of the GDPR defines "consent" as it must be voluntary, specific, informed, and unambiguous expression of the wishes of the data subject, which is expressed by a clear affirmative action.[53] Further, Article 7 goes further to discuss the circumstances of valid consent which is that the consent must be demonstrable, presented, in an understandable form that is readily accessible and can be easily revoked at any time just as it was originally granted.[54] Also, the GDPR mandates explicit consent in situations where special categories of personal data are involved, as per Article 9 of the legislation, thus presenting an increased protection standard.[55] The Court in *Bundesverband der Verbraucherzentralen v. Planet49 GmbH*[56], held that pre-ticked checkboxes are not active and informed consent, since they are an attempt to express an active and informed choice. Equally, in *Orange România SA v. ANSPDCP*, the Court pointed out that consent should be free and cannot be implied by silence or on the basis of the currently existing contractual relations, especially when there is an imbalance in power.[57] Such cases confirm that consent should be real and it should not be acquired passively or under duress.

Nevertheless, the GDPR is not based on consent only. Article 6 gives several legal justifications of processing, such as necessity in a contract, legal duty, general interest of the community, essential interests, and legitimate interests.[58] This is a diversified structure that shows a subtle appreciation of the constraints of consent especially where one side has unequal bargaining power.

In addition to consent, another key strength of GDPR lies under Articles 12 to 22 which create a broad and enforceable list of data subject rights that should help to maintain and establish an

[51] *Id.* art. 5.
[52] *Rīgas Satiksme v. Datu valsts inspekcija, Case C-13/16, ECLI:EU:C:2017:336 (2017).*
[53] GDPR art. 4(11).
[54] *Id.* art. 7.
[55] *Id.* art. 9.
[56] *Planet49*, *supra* note 25.
[57] *Orange România SA v. ANSPDCP*, Case C-61/19, ECLI:EU:C:2020:901 (2020).
[58] GDPR art. 6.

unbroken control over the personal data throughout its lifecycle. Article 12[59] establishes the broad principles of effective communication of information, which presupposes that the information should be presented in a clear, informative and easy-to-read form. Article 15[60] provides the right of access. Article 16[61] provides right to rectification. Further the right to erasure under Article 17[62] is one of the most important rights, also referred to as "the right to be forgotten".

In case *Google Spain SL v. Agencia Española de Proteccion de Datos*[63], as the Court stated that people have a right to demand the removal of links to personal data which is insufficient, irrelevant or excessive in terms of purposes of processing. The principle was also enhanced in *Google LLC v. CNIL,* here the Court explained the territorial scope of duties of delisting, balancing privacy rights against the freedom of information.[64]

Other rights were the right to restriction of processing in Article 18[65], the right to data portability in Article 20[66]. Further, Article 21 allows individuals to object to processing under legitimate interests or to engage in direct marketing.[67]

Further under Article 25 of regulation a structural approach of data protection through the principle of "data protection by design and by default" is also adopted.[68] This approach is further reinforced by the fact that Data Protection Impact Assessment mandated by Article 35 must be performed before high-risk processing activity is assessed.[69] Such processes transform the individual consent to institutional responsibility.

Besides, there is a strong enforcement framework in the GDPR, which provides independent supervisory authorities under the power of Articles 51 to 59 to oversee compliance and to penalize it.[70] Article 83 gives the administrative fines that are significant and could reach to 20

[59] *Id.* art. 12.
[60] *Id.* art. 15.
[61] *Id.* art. 16.
[62] *Id.* art. 17.
[63] *Google Spain*, *supra* note 4.
[64] *CNIL*, *supra* note 31.
[65] GDPR art. 18.
[66] *Id.* art. 20.
[67] *Id.* art. 21.
[68] *Id.* art. 25.
[69] *Id.* art. 35.
[70] *Id.* arts. 51–59.

million or 4% of the global annual turnover of an undertaking, whichever is greater.[71]

As compared to the Digital Personal Data Protection Act, 2023, the GDPR is more rights-focused and organized, minimizing the reliance on consent and providing greater protection of the autonomy of a person. This renders it a fundamental parameter of measuring the efficacy of new data protection regimes.

COMPARATIVE ANALYSIS BETWEEN DPDP ACT AND EU GDPR

Digital Personal Data Protection Act, 2023 and the General Data Protection Regulation (GDPR) are two major and different methods of data protection legislation. Although both models acknowledge the role of consent and individual rights, the two frameworks differ in many ways, including their framework, scope, and the philosophy of regulation. A Comparative analysis of these regimes shows that there are critical dissimilarities in the standards of consent, the extent of individual rights, implementation strategies, and the role of the State.

1. Consent Framework

Both the GDPR and the DPDP Act identify *consent* as a primary basis of legal data processing that needs to be free, specific, informed and unambiguous. This is a manifestation of a mutual belief in individual autonomy. Nevertheless, the GDPR sets a more stringent and formalized system of consent. Article 7 is very rigid and obligatory in that it requires demonstrability, affirmative action and the consent can be withdrawn at any time with ease.[72]

In case **Planet49**[73] and **Orange Romania**[74] have also enhanced the norm of consent with judicial interpretations that disapprove of pre-ticked boxes and implied consent models and forceful reinforcement of active and informed user involvement.

Contrarily, though DPDP Act uses similar terms, its practical implementation is constrained by more lenient flexibility and lack of more detailed interpretative guidance. Use of the word unconditional consent is unclear, particularly in situations where the receipt of digital services

[71] *Id.* art. 83.
[72] *Id.* art. 7.
[73] *Planet49*, *supra* note 25.
[74] *Orange România*, *supra* note 57.

depends on consent and hence, the issue of voluntariness of consent arises.

2. Lawful Bases for Processing

One of the major areas of disagreement is the way of lawful processing. Under Article 6, the GDPR uses a diversified approach, which accepts several legitimate grounds, such as contractual necessity, legal obligation, vital interests, public task, and legitimate interests.[75] This multi-ground strategy will minimize excessive dependence on consent and recognize its practical shortcomings.

On the other hand, the DPDP Act largely uses consent as the main foundation in processing, and the idea of legitimate uses as the second concept is supported by the idea of legitimate uses in Section 7.[76] Nonetheless, such provisions are relatively wide and less detailed, as they do not include detailed safeguards and balancing tests as the GDPR does. This brings up the question of the possibility of misuse and excessive discretion on the part of the state or institution.

3. Scope and Nature of Individual Rights

The GDPR offers a broad and precise list of rights, such as the right to access, amendment, eradication, limitation of processing, information portability and the right to protest. These rights have procedural protections which support them and have been proactively read and applied upon through judicial and regulatory application.

Conversely, the DPDP Act provides a smaller number of rights, such as access, correction, erasure, grievance redressal, and nomination. The lack of such vital rights as data portability and the right to object dramatically limits the area of user control, especially in the situations involving automated processing and specific data use. This is a weakness to the general empowerment of data principals in the Indian context.

4. Mechanisms of Enforcement and Institutional Framework.

The GDPR creates independent supervisory bodies that have robust investigative, corrective and punitive capabilities including the imposition of administrative fines that may be massive.

[75] GDPR art. 6.
[76] Digital Personal Data Protection Act, 2023, § 7.

Its enforcement mechanism is decentralized but aligned throughout the European Union making it consistent and effective.

Comparatively, DPDP Act uses the Data Protection Board of India as its main enforcement authority. It has raised issues over its independence, institutional capacity and transparency of the procedure. Also, the penalties in the Act are not as severe as those in the GDPR, even though the general enforcement framework is not as robust and well-developed, which may influence compliance and deterrence.

5. Government Powers and State Exemptions.

The GDPR allows the restriction of some rights in Article 23 however the restrictions are subject to rigid needs and proportionality tests which guarantees that limitations on individual rights are strictly limited.[77]

Conversely, the DPDP Act gives the Central Government wider exemption authority in Section 17 based on sovereignty, security, and public order.[78] Although these reasons could be valid, their broadness and insufficient specifications of protection present the problem of potential overreach and the weakening of personal protection of privacy.

6. Regulatory Philosophy and Approach

The regulatory philosophies are also different in the difference between the two regimes. The GDPR is rights-oriented and gives great focus on personal autonomy, responsibility, and minimization of data. It gives stringent requirements to data controllers and protects personal data as a primary right.

The DPDP Act, in turn, is a more realistic and balanced strategy, which tries to balance data protection with governance requirements, economic development, and the ease of doing business. Although this flexibility can make the administrative system more efficient, the question still remains as to whether the framework offers adequate protection against the rights of individuals.

[77] GDPR art. 23.
[78] Digital Personal Data Protection Act, 2023, § 17.

7. Overall Effectiveness and Practical Impact.

Comparatively, GDPR has a more solid and detailed framework, which is based on powerful individual rights, multiple lawful grounds of processing and strict enforcement mechanisms. It has an elaborate regulatory framework that improves compliance and accountability.

The DPDP Act is a very important move towards the field of data protection in India, but the scope of the Act is relatively smaller. Its consent-based nature and a more liberal set of exemptions and an underdeveloped enforcement mechanism can restrict its usefulness in guaranteeing meaningful control over personal data.

Concisely, the DPDP Act and the GDPR share the same objective of safeguarding personal data however, in a very different manner. The GDPR places an exceptionally high standard of data protection in the global arena whereas the DPDP Act places a more realistic and pragmatic standard. This kind of comparison makes it obvious that the data protection regime in India should be regularly enhanced to make the consent more efficient and the right of data principals stronger.

FINDINGS AND OBSERVATIONS: CHALLENGES IN THE EFFECTIVENESS OF DATA PRINCIPAL RIGHTS

The Digital Personal Data Protection Act, 2023, acknowledges the formal data principal rights, yet the Act contains significant structural, institutional, and socio-economic issues that complicate the implementation of these rights. Although the Act provides the framework of personal control of personal data, the possible scope of the implementation of these rights in the real-world digital context can be subjected to critical scrutiny.

1. Information Asymmetry and the Erosion of Informed Consent

The imbalance of information between Data Principals and Data Fiduciaries is one of the most fundamental issues in the successful implementation of the data principal rights by the DPDP Act. Digital platforms have much more technical skills, technical infrastructures, and influence on data processing processes, which puts people in a structural disadvantage. Even though the Act requires an informed consent and notification, in reality, the privacy policy is usually too long, too legal, and too hard to be understood by an average user. This imbalance is a destabilizer of the very idea of informed consent and does not allow the effective exercise of

such rights as access, correction, and erasure.

2. Consent Fatigue and the Manipulative Use of Dark Patterns

The consent fatigue phenomenon also undermines the usefulness of consent as a legal protection. Mechanical, but not deliberate, decision-making is encouraged in digital spaces as users are continuously encouraged to give their consent. This is augmented by the growing application of dark patterns interface designs that indirectly influence user behaviour by pushing them to an acceptance. The voluntariness of a consent is undermined by such techniques as pre-selected options, the use of confusing language, and the design of interfaces. In its turn, consent tends to become procedural and unimportant, as well as a simple facade instead of an act of autonomy exercised by the user.

Such theoretical issues are also supported by the real-life digital practices which prove how consent works in the daily online interactions. Practically, users are often confronted with standardized consent forms, including cookie banners, privacy pop-ups and click-wrap agreements that are more convenient than easy to understand.

For example - the “cookie” consent interfaces usually feature the Accept All buttons prominently in contrast to the rejection or customization settings that are less accessible or involve several steps. This design leads users towards acceptance hence compromising with making informed decisions.

Dark patterns like preselected choices, deceptive language, and concealed opt-out mechanisms further control user behaviour and cast serious doubts on whether such consent can be described as being free and informed at all.

3. Limitations in the Scope and Breadth of Data Principal Rights

Although the DPDP Act defines some of the fundamental rights, including access, correction, erasure, and grievance redress, the structure is relatively small in comparison with other international regulations, including the GDPR. It is important to note that the lack of such rights as data portability or the right to object to processing limits the autonomy of an individual to a significant extent. These exclusions are especially applicable to the situations where the automated decision-making, profiling, and targeted advertising are concerned since in that scenario, people need to have more control over how their data is utilized. Consequently, the

rights framework provided by the DPDP Act might be considered as less comprehensive in its scope, which restricts its ability to serve in the modern day data protection issues.

4. Institutional Limitations and Enforcement Challenges

The success of any legal system depends on the power of its enforcement. In the DPDP Act, it has been argued that the Data Protection Board of India lacks the autonomy and the capability of the institution. The questions connected to its procedural transparency, technical proficiency and operational autonomy can affect its capacity to successfully resolve conflicts and implement compliance. Devoid of strong institutional backing, even clearly defined rights are likely to go unexploited or not well implemented, which undermines the entire regulatory regime.

5. Broad Scope and Implications of State Exemptions

Another major challenge is the clauses that deal with state exemptions in the DPDP Act under Section 17.[79] Even though exemptions based on sovereignty, national security, and public order can be reasonable within the context of some situations, the wide and even wide-reaching interpretation of such exemptions creates a problem of their abuse. These can restrict the scope of the protection of data rights in the cases when they are the most required, which is an imbalance between personal privacy and the interests of the state. This organizational issue has significant implications on the credibility of the data protection regime as a whole and its strength.

6. Lack of Awareness and Digital Literacy as Structural Barriers

Data principal rights are also not fully realised practically due to the lack of awareness and digital literacy of the population. Some large percentage of people do not even know their legal rights or do not possess the required skills to make good use of them. Such rights as access, correction and grievance redressal demand some amount of procedural awareness and digital interaction, which not all socio-economic groups may have in an even manner. Such digital divide reduces the inclusivity and effectiveness of the legal framework especially in a diverse and populous country such as India.

[79] *Id.*

7. Corporate Compliance Burdens and Their Impact on Rights Realization

Adherence to data protection requirements as per the DPDP Act can be costly and difficult to implement especially to the small and medium enterprises. These issues may cause unequal enforcement of the law, hence, influence the equal implementation of data protection standards. This, in its turn, affects the capacity of people to exercise their rights effectively as the level of protection might be different depending on the capacity of the data fiduciary in question.

8. Cross-Border Data Flow and Jurisdictional Complexities

In a more globalized digital world, personal data is often transited over national borders, with its complex jurisdictional concerns that become more complicated. The provision of uniform protection and effective redress in the case is a big challenge. Though the DPDP Act offers a guideline on how to transfer data across the border, the mechanisms of the same are yet to be developed and might encounter the challenge of aligning with other internationally accepted standards like those established by the GDPR. This poses a dilemma in the application of rights and protection in cross-jurisdictional situations.

Together, these issues indicate a great gap between the legal recognition and the practice of the rights of data principals. Despite the DPDP Act representing a significant step in the law-making arena, its success will greatly depend on the quality of its implementation, the quality of institutional procedures, and the level of enlightenment of the population. Comparatively, the GDPR alleviates much of these issues with a larger rights framework, stricter enforcement measures and increased clarity of regulation. Nevertheless, the GDPR is not free of such problems as consent fatigue and complexity of compliance, meaning that these challenges are inherent to the contemporary data protection regimes.

RECOMMENDATIONS AND REFORMS

In the light of structural and practical difficulties in the implementation of data principal rights within the Digital Personal Data Protection Act, 2023, it is evident that specific reforms are necessary to make it more effective. The Act despite being a significant step towards codification of data protection in India, long-term success of the Act will be pegged on the enhancement of its normative framework and institutional mechanisms.

A primary area of reform lies in *strengthening the consent framework.* The consent has to

become not a formal legal necessity but the real tool of user empowerment. This necessitates the simplification of privacy notices in standardized and user friendly formats and layered disclosures that is more accessible and understandable. Further, regulatory intervention may also require to curb the use of dark patterns which ensures that the consent is received based on fair and clear interface design. This would greatly help in enhancing the quality of consent.

Additionally, there is a need to *broaden the data principal rights*. One should also align the DPDP Act with international best practices and enhance the right to control users should be extended to include other rights like the right to data portability and the right to object to processing. These rights particularly apply when addressing the emerging challenges that are of concern in the area of algorithmic decision-making, targeted advertising and platform dominance. With the increased rights framework, the subjects would guarantee them the ongoing control of their personal data after the first consent.

Further it is also important to *enhance institutional and enforcement mechanisms.* The success of any data protection regime is determined by the robustness, autonomy and ability of its regulatory bodies. Enhancing the functional autonomy of the Data Protection Board of India, the transparency of the procedures, and offering it adequate technical expertise and resources would do wonders in enhancing the outcome of the enforcement. Furthermore, it would be more practical to make rights more available by setting clear rules on grievance redressal and prompt redressal of complaints.

Additionally, the other area of reform is related to the *extent of the state exemptions.* Despite the need to have some exemptions on legitimate state activity, they should be narrowly restricted and be accompanied by the circumscription of the need, proportionality, and independent check. Moreover, to curb any abuse, as well as in ensuring that exemptions are not abused at the cost of the desired objective of protecting the privacy of individuals, it would be prudent to establish more explicit statutory limitations and accountability mechanisms.

Additionally, there is an urgent need *to improve the public awareness and digital literacy.* Legal rights will only be effective when people are conscious of these rights and can exercise them. Awareness campaigns led by the government, introduction of digital literacy programs in learning programs and creation of available grievance systems can play a crucial role in bridging this gap.

Furthermore, from regulatory perspective, promoting *privacy by design and accountability-based frameworks* can reduce over-reliance on individual consent. Promoting the idea of organizations integrating data protection into technological infrastructure and business operations early in life would re-orient the compliance mode towards protection. it would be prudent to establish more explicit statutory limitations and accountability mechanisms.

Additionally, India can benefit from *learning from global best practices*, particularly the GDPR. Although direct transplantation is not always possible because of different socio-economic backgrounds, the selective application of the main principles, such as stronger enforcement mechanisms, clearer consent standards, and expanded rights can promote the efficiency of the DPDP framework. International collaboration in areas such as cross-border data flows and regulatory standards would further strengthen India's position in the global data governance landscape. Lastly, there is a need for *continuous review and adaptive regulation*. While considering the dynamic nature of digital technologies the data protection laws should be adaptable and responsive. Periodic legislative review, stakeholder consultations, and regulatory changes will be necessary to respond to the emerging challenges of artificial intelligence, big data analytics and surveillance technologies.

To sum up, despite the fact that the DPDP Act, 2023 offers the overall framework on data protection in India, the success will be reviewed in the long-term processes of strengthening and refining the provisions. This can be improved by an improvement in the consent procedure, increasing rights, enhancing enforcement and more of a focus on accountability to help this change this to a more robust and future-oriented data protection regime.

CONCLUSION

The growing prominence of consent within the contemporary data protection systems evokes the issue of its ability to serve as a functional tool to protect the privacy of information in the era of digitalism. Although the Digital Personal Data Protection Act, 2023 aims to institutionalize user autonomy in the form of a consent-based model, the real question is whether this model can produce meaningful control over personal data or is just a formal legal provision on a complicated digital ecosystem.

This paper concludes that despite its well-organized structure of the data protection law and the formal status of the main data principal rights, including access, correction, and erasure,

the DPDP Act has a limited functional capacity due to structural, institutional, and socio-economic limitations. The lack of information asymmetry between the data fiduciaries and individuals and the more advanced data processing practices are going to hinder the truly informed choices of the user. The issue of consent fatigue and the tactical deployment of dark patterns make the issue of voluntariness of consent even more watered down to a routine and frequently inattentive act. Also, low digital literacy and awareness of users limit the effective exercise of rights as the lack of some important rights, including the right to portability of data and the right to object, limit the area of individual control. The enforceability and widespread application of these protections is also undermined by institutional issues associated with the independence and the ability of the Data Protection Board and the wide scope of state exemptions under the Act.

The comparative study against the General Data Protection Regulation shows that there is a vast difference not only in the legal framework but also the philosophy of the regulation. The GDPR is an expanded and rights-based framework, which is backed by numerous legitimate grounds of processing, a wider and stronger system of data subject rights, and a highly developed institutional structure that enforces accountability and transparency. Its focus on the principles of data minimization, purpose restriction, and design protection enhances the excessive consent-based elements and reinforces substantive privacy protection. Against this, the DPDP Act is more pragmatic and sensitive to the state and aimed at balancing the individual rights and the goals in governance and economy. Nevertheless, such a balance, when not backed up by sufficiently strong safeguards, is prone to undermine the privacy protection.

On an analytic level, the results demonstrate a bigger conflict between formal law adherence and substantive safeguarding of individual autonomy. Although the DPDP Act and the GDPR consider consent as a pillar of data protection, the success of both regulations is ultimately determined by the legal, institutional, and technological ecosystem. Indian system, despite its progressive intention, is still at the developmental stage when the rights and protections operationalization has not yet come to full. Consequently, consent under the DPDP Act might not be yet a real enabling process of individuals, but a procedural entry point of data processing.

To sum up, the DPDP Act is a major step in India data protection path, and it is the shift to a more organized and rights-based regulatory framework. Nevertheless, its contemporary design and implementation issues restrict its capabilities to guarantee significant and beneficial

protection of data principal rights. Going forward, the ongoing legal and institutional clarification, such as the enhancement of enforcement systems, extension of individual rights, and the improvement in data practices transparency and the introduction of a clear and reasonable boundaries on the exercise of state exemptions, is required. It will be necessary to fill the gap between legal and practical realisation of data protection, by taking the approach towards more holism and user-centric, which seeks to bring the concept of privacy not only as a statutory protection, but as a lived and enforced reality in the digital age.