
CONSENT IN THE DIGITAL AGE: IS THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 SUFFICIENT TO PROTECT INDIVIDUAL AUTONOMY?

Aaisha Abdul Samad Advani, KES' Shri. Jayantilal Patel Law College.

ABSTRACT

Personal data has become a regular part of everyday life. People share their information when using social media, making online payments, accessing healthcare services or downloading mobile applications. Although these activities make life easier, users do not always know how their information will be stored, shared or used in the future. In many cases, accepting a privacy policy becomes a routine step rather than a decision made after considering the consequences.

The Digital Personal Data Protection Act, 2023 (DPDP Act) seeks to address some of these concerns by setting out requirements for valid consent, recognising the withdrawal of consent and placing obligations on organisations that process personal data. However, the existence of these legal safeguards does not automatically mean that individuals have meaningful control over their information. Long privacy notices, limited alternatives and processing permitted without consent can make it difficult for people to exercise a genuine choice.

This article examines whether the consent framework under the DPDP Act provides adequate protection for individual autonomy. It also considers relevant judicial decisions, including *Justice K.S. Puttaswamy (Retd.) v. Union of India*, which recognised privacy as a fundamental right, and *Central Inland Water Transport Corporation Ltd. v. Brojo Nath Ganguly*, which discussed unequal bargaining power in contractual relationships. Although these cases do not directly interpret the DPDP Act, they offer useful principles for examining privacy and the freedom to make decisions. The article argues that the Act establishes an important framework for data protection, but its ability to protect individual autonomy will depend on how its safeguards operate in practice.

Keywords: Digital Personal Data Protection Act, 2023; consent; individual autonomy; informational privacy; data protection; fundamental right to privacy; digital rights.

1. Introduction

Digital technology has become part of almost every aspect of our lives. People use mobile applications to make payments, shop online, communicate with friends, attend classes and access healthcare services. Most of these activities involve sharing personal information, sometimes without giving much thought to how that information will be used later.

The problem is that sharing information for one purpose does not necessarily mean that a person understands or expects every possible use of it. For instance, someone may provide their contact details while creating an account on a shopping application without realising how those details might be stored, analysed or used for other purposes. Although privacy policies are usually available, they can be lengthy and difficult to understand. Many users simply accept the terms because they want to use the service.

This raises a question that is becoming increasingly important: when a person clicks “I agree”, are they really making an informed choice, or are they simply accepting the conditions placed before them?

The Digital Personal Data Protection Act, 2023 (DPDP Act) was introduced to establish a legal framework for the processing of digital personal data in India. It lays down requirements for consent, places obligations on organisations that process personal data and gives individuals certain rights in relation to their information. However, the Act also allows personal data to be processed in specified circumstances without consent. This means that the protection it provides cannot be assessed by looking at consent alone.

The real difficulty lies in how these provisions work in everyday situations. A person may technically have the right to refuse consent, but what happens when refusing means losing access to a service that is important for work, education or communication? Similarly, even when an individual agrees to data processing, does that agreement mean much if they do not understand the terms or have little control over how the service operates?

This article examines whether the DPDP Act provides sufficient protection for individual autonomy. It discusses the Act's consent requirements, the rights available to individuals, the circumstances in which processing may take place without consent and the practical difficulties that users may face. It also considers relevant judicial decisions, including *Justice K.S.*

Puttaswamy (Retd.) v. Union of India and Central Inland Water Transport Corporation Ltd. v. Brojo Nath Ganguly, to understand the relationship between privacy, freedom of choice and unequal bargaining power.

The argument developed in this article is that the DPDP Act provides an important legal starting point, but the existence of statutory rights does not automatically ensure that individuals can exercise meaningful control over their personal information. That depends on how clearly organisations explain their practices, how they respond when consent is withdrawn and how effectively the law is implemented.

2. Understanding Consent and Individual Autonomy

Individual autonomy is the ability to make decisions freely and exercise control over matters that affect one's life. In the context of data protection, it means having a meaningful say in what personal information is collected, why it is collected and how it may be used.

Consent is one way of protecting this freedom. However, consent should mean more than simply accepting a privacy policy or clicking a button on a screen. A person should have enough information to understand the decision being made and a genuine opportunity to decide whether to agree.

Consider a person who wants to use an online banking application. The person may be willing to share information necessary to open an account or complete a transaction. That does not necessarily mean they also wish to permit unrelated uses of their information. If the distinction between necessary and optional data collection is unclear, the person may agree to more than they intended.

The problem becomes more complicated when refusing consent is not a realistic option. Many digital services have become important for everyday activities. A user may depend on a platform for communication, education or work and may therefore accept its terms simply to gain access. In such circumstances, the person has technically made a choice, but the circumstances surrounding that choice deserve attention.

This is the difference between formal consent and meaningful consent. Formal consent records that a person has agreed. Meaningful consent requires us to look more closely at what the person was told, what options were available and whether the decision was made with an

adequate understanding of the consequences.

The DPDP Act recognises some of these concerns by requiring consent to be free, specific, informed, unconditional and unambiguous. It also limits consent to the specified purpose and the personal data necessary for that purpose. These requirements are important, but their effectiveness depends on how organisations put them into practice.

In my view, consent should not be treated as the only measure of privacy protection. Clear information, responsible data handling, adequate security and accessible remedies are also necessary. Without these safeguards, an individual may have a legal right to make a choice without having much practical control over the outcome.

3. Analysis of the Digital Personal Data Protection Act, 2023

3.1 Section 3: Application of the Act

Section 3 determines the circumstances in which the DPDP Act applies. Broadly, the Act covers the processing of digital personal data within India, including personal data collected in non-digital form and subsequently digitised. It also covers certain processing outside India where it is connected with offering goods or services to Data Principals within India, subject to the conditions in the provision.

This provision matters because digital services do not always operate within one country. A person living in India may use an application whose systems, service providers or data storage facilities are located elsewhere. The application of data protection law therefore becomes important when information moves across borders.

At the same time, the Act does not cover every possible use of personal information. Section 3 contains exclusions, including specified personal or domestic processing and certain publicly available personal data. Its scope must therefore be understood from the wording of the provision rather than by assuming that every activity involving personal information is covered.

From the perspective of individual autonomy, the application provision determines when the protections under the Act become relevant. If an activity falls outside its scope, an individual may not be able to rely on the Act for that particular processing. This makes the boundaries of the legislation important, especially in a digital environment where personal information is

collected and used in many ways.

3.2 Section 4: Grounds for Processing Personal Data

Section 4 provides that personal data may be processed only in accordance with the Act and for a lawful purpose, based on consent or a legitimate use recognised under Section 7.

This shows that the DPDP Act does not make consent the only possible basis for processing personal data. There are situations in which processing may take place without obtaining an individual's consent, provided the applicable legal conditions are satisfied.

There are understandable reasons for this approach. For example, personal data may need to be processed to comply with a legal obligation, respond to an emergency or carry out a specified public function. Requiring consent in every situation could make some necessary activities difficult or impossible.

However, this also raises an important question about individual control. If an organisation relies on a lawful ground other than consent, refusing consent may not prevent the processing from taking place. The individual must therefore depend on the legal limits governing that processing rather than on a personal decision to agree or refuse.

For this reason, the protection of autonomy requires more than a well-designed consent mechanism. It also requires clarity about the circumstances in which consent is unnecessary and whether the processing remains within the limits permitted by law.

3.3 Section 5: Notice and Transparency

Section 5 deals with the notice that a Data Fiduciary must provide before or in connection with seeking consent, including information about the personal data and the purpose for which it is to be processed. It also addresses information concerning the exercise of rights and the process for making complaints.

Notice is essential because a person cannot make an informed decision without knowing what they are agreeing to. If an organisation does not explain the purpose of collecting information, the individual has little basis on which to decide whether sharing it is appropriate.

However, providing information does not necessarily mean that the information has been

communicated effectively. A privacy notice may contain the required details and still be difficult for an ordinary user to understand. Technical language, lengthy explanations and important conditions buried in several pages can make it difficult to identify what matters.

For example, a user may want to know whether a mobile application needs access to their location to provide its main service. If that information is difficult to find, the user may simply accept the request without understanding whether location access is necessary.

In my view, transparency should be measured not only by whether information is disclosed but also by whether users can understand it. Short explanations, clear headings and separate explanations of essential and optional data collection could make notices more useful. These approaches would help give practical meaning to the requirement that consent be informed.

3.4 Section 6: Consent and Its Legal Requirements

Section 6 is central to this article because it sets out the requirements for valid consent. Under Section 6(1), consent must be free, specific, informed, unconditional and unambiguous, and it must be indicated through a clear affirmative action. It must also relate to the specified purpose and be limited to the personal data necessary for that purpose.

These requirements seek to prevent organisations from treating a user's agreement as unlimited permission to collect and process personal information.

The Act's illustration involving a telemedicine application helps explain this principle. If an application needs certain information to provide medical consultations but also asks for access to a user's contact list, the additional information cannot simply be justified by the user's general agreement to use the application if it is unnecessary for the specified purpose. The example highlights the importance of connecting the information requested with the service being provided.

Section 6(2) also provides that consent is invalid to the extent that it infringes the Act, its rules or any other applicable law. An organisation cannot therefore rely on consent to justify processing that is otherwise unlawful.

Despite these safeguards, questions remain about how freely consent is given in practice. A person may accept the terms of a platform because refusing would mean losing access to a

useful or necessary service. Although that does not automatically make the consent invalid, it raises questions about the circumstances in which the choice was made.

It is also important to distinguish between information genuinely needed to provide a service and information collected for optional purposes. A person who agrees to use a service should not necessarily be expected to agree to every additional request for personal information.

The requirements in Section 6 provide a legal basis for questioning excessive or poorly explained data collection. Their practical value, however, depends on whether organisations respect these requirements and whether individuals have an effective way to challenge non-compliance.

3.5 Withdrawal of Consent

Consent should not be understood as a decision that an individual can never change. Section 6(4) allows a Data Principal to withdraw consent at any time and requires the ease of withdrawal to be comparable to the ease with which consent was given.

Section 6(5) clarifies that withdrawing consent does not affect the legality of processing carried out based on consent before withdrawal. Section 6(6) requires the Data Fiduciary to cease the relevant processing within a reasonable time and ensure that its Data Processors do likewise, unless processing without consent is required or authorised by law.

These provisions recognise that people may change their minds. A person might initially agree to receive marketing communications but later decide that they no longer want their information used for that purpose. The law should allow the person to change that decision without facing unnecessary obstacles.

A difficulty arises when withdrawing consent is more complicated than giving it. If accepting a request takes one click but withdrawing consent requires several steps, repeated confirmations or a lengthy process, the right may be harder to exercise in practice.

Withdrawal also does not necessarily mean that every record must immediately be deleted. Other legal requirements or an independent lawful basis may affect whether processing or retention can continue. The consequences of withdrawal must therefore be considered in light of the Act and the circumstances of the particular processing.

The important point is that withdrawal should be a usable right, not merely an option mentioned in a privacy policy. Individuals should be able to understand how to withdraw consent, and organisations should comply with the legal consequences of that decision.

3.6 Consent Managers

The DPDP Act provides for Consent Managers as a mechanism through which individuals can manage their consent. Sections 2(g) and 6(7)–(9) establish the statutory framework for this arrangement.

The idea is useful because people may use numerous digital services, each with its own privacy settings and consent requests. Keeping track of all these permissions can become difficult. A system that allows individuals to review and manage consent more conveniently could make it easier to understand what they have agreed to and to change their decisions when necessary.

However, the usefulness of Consent Managers will depend on how the system operates in practice. Users must be able to access the service, understand its functions and trust that their instructions are accurately recorded and communicated. It must also work effectively with the relevant services.

There is another limitation to consider. A Consent Manager cannot solve every problem associated with digital consent. It cannot, by itself, remove unequal bargaining power or prevent processing that is lawfully permitted without consent.

Consent Managers should therefore be viewed as one part of the wider framework. They may make consent easier to manage, but meaningful autonomy also depends on clear information, appropriate limits on data collection and effective enforcement.

3.7 Sections 8 and 10: Accountability of Data Fiduciaries

Section 8 imposes general obligations on Data Fiduciaries, including responsibility for compliance with the Act, reasonable security safeguards, specified obligations concerning personal data breaches, erasure in applicable circumstances and grievance redressal. Section 10 provides additional obligations for Significant Data Fiduciaries.

These provisions matter because users rarely know exactly what happens to their information

once it enters an organisation's systems. They may know what information they have provided, but they cannot easily determine who has access to it, how securely it is stored or whether it has been shared with others.

It would be unrealistic to expect individuals to monitor these activities themselves. Organisations are generally better placed to understand their systems, identify risks and maintain records of how personal data is handled. The Act therefore places important responsibilities on the organisations processing the information.

Section 6(10) is also relevant because it places the burden on the Data Fiduciary to demonstrate, where the question arises in proceedings under the Act, that the required notice was given and valid consent was obtained.

This is significant because the organisation is normally in a better position to maintain evidence of the consent process than the individual who accepted the terms. Appropriate records can help establish whether the legal requirements were followed.

Nevertheless, obligations on paper are not enough. Organisations must actually follow the required procedures; protect the information they hold and respond appropriately when something goes wrong. Accountability is meaningful only when compliance can be assessed and failures can lead to appropriate consequences.

3.8 Section 9: Children's Personal Data

Section 9 provides additional protection for children's personal data. It generally requires verifiable consent from a parent or lawful guardian before a child's personal data is processed. It also restricts processing likely to have a detrimental effect on a child's well-being and addresses tracking, behavioural monitoring and targeted advertising directed at children, subject to the Act and applicable exemptions.

These safeguards are important because children may not fully understand the consequences of sharing personal information online. They may provide details, photographs or other information without considering how those details could be used later.

Parental consent is one way of addressing this difficulty, but it cannot resolve every concern. A parent may also be unaware of the technical practices used by an application or the possible

consequences of collecting information. The design of the service and the organisation's data-handling practices therefore remain important.

The provision also raises a broader point about the limits of consent. In some situations, obtaining agreement may not be enough to protect the person concerned. Additional restrictions may be necessary where forms of processing create risks to children's well-being.

The protection of children's personal data should consequently involve both consent requirements and responsible practices by the organisations providing digital services.

3.9 Sections 11–14: Rights of Data Principals

Sections 11–14 recognise rights that complement the consent framework. Section 11 concerns access to information about personal data; Section 12 deals with correction, completion, updating and erasure; Section 13 provides for grievance redressal; and Section 14 recognises the right to nominate another person to exercise specified rights in certain circumstances.

These rights are important because the relationship between an individual and their data does not end once consent has been given. A person may later want to understand what information is being processed, correct an error or request erasure where the law permits it.

The right to raise a grievance is also significant. If an individual believes that an organisation has failed to comply with its obligations, there should be a way to bring the concern to the appropriate authority or process.

However, the practical value of these rights depends on whether individuals know about them and can exercise them without unreasonable difficulty. A right may offer limited protection if the procedure for using it is confusing or if the response takes too long.

For these provisions to support individual autonomy, organisations must respond appropriately to valid requests, and the relevant procedures must be accessible. Individuals should not need extensive technical or legal knowledge merely to understand how to exercise their statutory rights.

3.10 Sections 7 and 17: Processing Without Consent and Exemptions

One of the most important questions raised by the DPDP Act is how it protects individuals

when consent is not required.

Section 7 identifies circumstances in which personal data may be processed for specified legitimate uses. These include certain situations involving the voluntary provision of personal data for a specified purpose, specified State functions, compliance with legal obligations or judgments, medical emergencies, public-health situations, disasters and employment-related purposes, subject to the statutory conditions.

Section 17 provides exemptions in specified circumstances. These include certain legal proceedings and law-enforcement activities, along with provisions concerning notified State instrumentalities and other situations identified in the Act.

There are valid reasons for allowing some processing to take place without consent. For instance, personal data may need to be processed to comply with a court order or respond to a medical emergency. In such situations, seeking consent may be impractical or may prevent necessary action.

The concern is not that every instance of processing without consent is improper. Rather, it is whether the applicable legal ground is clear and whether the organisation or authority stays within the limits permitted by law.

This issue is particularly important because an individual cannot rely on refusal of consent in the same way where processing is authorised on another legal basis. The safeguards governing that processing therefore become especially significant.

In my view, the adequacy of the DPDP Act must be assessed by considering both sides of the framework: the protections available when consent is required and the safeguards that apply when it is not.

4. Judicial Approach to Privacy, Consent and Autonomy

The DPDP Act forms part of India's wider legal framework for protecting privacy and individual freedom. Several Supreme Court decisions offer useful principles for examining the relationship between personal information, autonomy and the circumstances in which individuals make choices.

These judgments were decided before the commencement of the Act's principal consent provisions and do not directly interpret Section 6. Their relevance lies in the broader legal principles they discuss.

4.1 Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)

Citation: (2017) 10 SCC 1

Court: Supreme Court of India

In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, a nine-judge Bench of the Supreme Court unanimously recognised privacy as a fundamental right protected by the Constitution. The judgment connected privacy with dignity, liberty and individual autonomy and recognised informational privacy as an important part of that right.

The decision is relevant because personal information can reveal far more than individual details viewed separately. When information from different sources is combined, it may disclose a person's habits, relationships, interests and patterns of behaviour. The way personal data is collected and used can therefore affect an individual's ability to maintain privacy and make decisions without unjustified interference.

The judgment also highlighted the need for a strong data-protection framework. It recognised that privacy concerns arise in relation to both State and non-State actors, although the legal questions and applicable obligations may differ according to the circumstances.

Relevance to the DPDP Act: The judgment provides an important constitutional foundation for examining the protection of personal information. The Act's consent requirements, individual rights and obligations on Data Fiduciaries can be considered considering the values of privacy, dignity and autonomy recognised by the Court.

Analysis: The judgment does not mean that all processing of personal data requires consent or that privacy can never be limited. Rather, it establishes the importance of privacy as a constitutional right. Whether the DPDP Act provides adequate protection is a separate question that requires examination of its provisions, safeguards and practical operation.¹

4.2 *K.S. Puttaswamy (Retd.) v. Union of India* — Aadhaar Judgment (2018)

Citation: (2019) 1 SCC 1

Court: Supreme Court of India

The Aadhaar judgment examined the constitutional validity of the Aadhaar framework, including the collection and use of demographic and biometric information. The Supreme Court considered the relationship between the objectives of the framework and the privacy interests of individuals.

The decision is relevant because it shows why questions about data collection cannot always be answered simply by asking whether information has been provided. The purpose of collecting the information, the legal basis for doing so, the extent of the interference and the safeguards against misuse also matter.

The Court upheld important aspects of the Aadhaar framework while invalidating or limiting other aspects. The judgment therefore demonstrates the need to examine the particular legal provisions and circumstances involved rather than treating all forms of data collection in the same way.

Relevance to the DPDP Act: The decision supports a broader approach to data protection in which consent is important but is not the only consideration. The law must also address whether processing is legally justified and whether appropriate limits and safeguards exist.

Analysis: Where individuals have little practical choice about providing information, consent alone may not resolve every concern about autonomy. The Aadhaar judgment illustrates the importance of examining the surrounding legal framework. However, it should not be treated as a direct ruling on the DPDP Act or its consent provisions.²

4.3 *Central Inland Water Transport Corporation Ltd. v. Brojo Nath Ganguly* (1986)

Citation: (1986) 3 SCC 156

Court: Supreme Court of India

In *Central Inland Water Transport Corporation Ltd. v. Brojo Nath Ganguly*, the Supreme Court considered an unconscionable contractual term in the context of unequal bargaining

power. The judgment examined situations in which a stronger party imposes standard-form contractual terms on a weaker party who has little meaningful opportunity to negotiate.

The case did not concern digital privacy. Nevertheless, its discussion of unequal bargaining power provides a useful comparison when examining how consent works in the digital environment.

Digital platforms generally prepare their own terms and conditions. Users often cannot negotiate the privacy provisions individually and may have to accept the terms before using the service. Where alternatives are limited, a user's acceptance may reflect a practical need to access the service rather than a considered preference for every condition imposed.

Relevance to the DPDP Act: The judgment helps explain why the requirement of free consent should be examined in its practical setting. It encourages us to look beyond the fact that an agreement was accepted and consider the circumstances in which the choice was presented.

Analysis: The principles in *Brojo Nath Ganguly* do not automatically make digital consent invalid. The case concerned a different legal context, and the validity of a particular arrangement must be assessed under the applicable law. Its relevance here is analytical: it highlights that formal agreement and genuine freedom of choice may not always be the same.³

4.4 *Anuradha Bhasin v. Union of India* (2020)

Citation: (2020) 3 SCC 637

Court: Supreme Court of India

In *Anuradha Bhasin v. Union of India*, the Supreme Court considered restrictions on internet access and communications in Jammu and Kashmir. The case examined the effect of State restrictions on fundamental rights and the need for legal safeguards when those rights are affected.

The judgment discussed proportionality and the need for restrictions affecting fundamental rights to have a legal basis, pursue a legitimate aim and be appropriately tailored to that aim.

Relevance to the DPDP Act: The decision provides a useful constitutional perspective when considering State action that affects privacy or personal information. Where an individual

cannot decide whether their information will be processed, the legal basis and safeguards governing that processing become particularly important.

Analysis: The case did not concern the DPDP Act or consent obtained by private digital platforms. Its relevance lies in the broader principle that restrictions affecting fundamental rights must be justified within the applicable legal framework. It does not, by itself, establish that any particular exemption under the DPDP Act is unconstitutional.⁴

4.5 What These Decisions Tell Us

Taken together, these judgments help explain why privacy protection cannot depend entirely on consent. *Puttaswamy* establishes the constitutional importance of privacy and autonomy. The Aadhaar judgment illustrates the importance of examining the legal basis and safeguards for data-related measures. *Brojo Nath Ganguly* draws attention to the effect of unequal bargaining power on contractual choice, while *Anuradha Bhasin* provides a broader perspective on legal safeguards where fundamental rights are restricted.

None of these decisions directly interprets the DPDP Act's consent provisions. Their value lies in the principles they offer for evaluating whether the legal framework gives individuals adequate protection. They also highlight the need to examine the circumstances in which personal information is processed, rather than assuming that consent alone resolves every privacy concern.

5. Practical Challenges of Digital Consent

5.1 Consent Fatigue

Most people have encountered repeated requests to accept privacy policies, enable permissions or agree to updated terms. When these requests appear frequently, users may begin accepting them automatically rather than reading each notice carefully.

This problem is commonly described as consent fatigue. It can weaken the purpose of informed consent because the user may be agreeing without fully considering what the request involves.

Sections 5 and 6 of the DPDP Act seek to establish requirements for notice and consent. However, compliance should not become a matter of simply displaying a notice and recording

an acceptance. The information must help the user understand the decision.

For example, a short explanation of why an application needs access to a particular category of information may be more useful than a lengthy technical description. Clear and relevant notices can make it easier for users to identify what is necessary and what is optional.

The challenge is to make consent meaningful without expecting users to spend excessive time understanding every digital service they use.

5.2 Limited Alternatives and Unequal Bargaining Power

Another difficulty arises when individuals cannot realistically avoid a digital service. Online platforms may be important for employment, education, banking and communication. If access depends on accepting broad terms, the user's ability to refuse may be limited.

This does not mean that every requirement to accept a platform's terms is unlawful. Some information is genuinely necessary to provide a service. The concern arises when users are asked to provide additional information that is not clearly connected to the service they want to use.

The requirement of free consent under Section 6 is relevant here, as is the requirement that consent be limited to the specified purpose and necessary personal data. These requirements provide a basis for examining whether the information requested is appropriate.

In practice, the issue is whether users have a reasonable opportunity to refuse unnecessary processing without being forced to give up access to the main service. This is one area where the difference between formal consent and meaningful choice becomes particularly clear.

5.3 Reuse of Data and Purpose Limitation

People generally provide information for a particular reason. A customer may give a telephone number to receive updates about an online order, for example, without expecting it to be used for unrelated marketing or profiling.

Section 6 requires consent to relate to a specified purpose and limits it to the personal data necessary for that purpose. This helps prevent an organisation from treating one act of consent as permission for every future use of the information.

The difficulty lies in ensuring that actual processing remains consistent with the stated purpose and the applicable legal basis. Users may find it difficult to know whether their information is being used in ways they did not expect.

Organisations should therefore explain their purposes clearly and review whether the information they collect is genuinely required. The purpose of consent is weakened if individuals agree to one use but have little understanding of other processing that may follow.

5.4 Data Breaches and Loss of Control

Even when an individual has given valid consent, their personal information may still be exposed through inadequate security or a data breach. Agreeing to the processing of personal data should not mean accepting careless handling of that information.

Section 8 imposes obligations relating to reasonable security safeguards and personal data breaches. These obligations are important because individuals cannot protect their information entirely by making careful choices at the point of consent.

Once data is held by an organisation, users generally have limited control over the security systems used to protect it. They may not know whether appropriate safeguards are in place or whether access to their information is properly restricted.

This shows why consent cannot be the whole answer to data protection. Organisations must also handle information responsibly, maintain appropriate security and comply with their statutory obligations. Without these measures, an individual's initial choice to share information may not provide much protection against later misuse or exposure.

6. Are the Act's Exemptions Consistent with Individual Autonomy?

The DPDP Act allows processing without consent in specified circumstances and provides exemptions under Section 17. These provisions deserve particular attention because they affect the extent to which individuals can control what happens to their personal information.

There are situations in which obtaining consent may not be practical or appropriate. Personal data may need to be processed to comply with legal obligations, respond to an emergency or carry out certain public functions. The law must be able to accommodate such situations,

provided the relevant statutory conditions are met.

At the same time, when processing takes place without consent, individuals cannot exercise the same direct control over the initial decision. The legal basis for processing and the safeguards governing it therefore become more important.

The principles recognised in *Puttaswamy* provide a starting point for examining the relationship between privacy and State action. The Aadhaar judgment and *Anuradha Bhasin* also offer relevant guidance on legal justification and safeguards where fundamental rights are affected.

However, it would be incorrect to assume that every instance of processing without consent is unlawful or that every exemption under the DPDP Act is automatically unconstitutional. Each provision must be examined according to its wording, the circumstances in which it applies and the relevant legal requirements.

The more important question is whether the overall framework provides adequate protection against arbitrary or excessive processing. Where consent is not required, individuals need to be able to rely on the applicable legal limits and safeguards. This is particularly important where processing may have significant consequences for their privacy.

In my view, the exemptions do not necessarily undermine individual autonomy simply because they permit processing without consent. Their effect depends on how broadly they operate, what safeguards apply and whether the relevant authorities remain within the limits set by law.

7. Enforcement and Access to Remedies

The value of a legal right depends partly on whether a person can exercise it when necessary. The DPDP Act establishes the Data Protection Board of India and provides a framework for dealing with specified contraventions.

Sections 13 and 27 concern grievance redressal and the functions of the Board, while Section 33 and the Schedule address monetary penalties for specified contraventions. These provisions form part of the framework intended to encourage compliance with the Act.

Enforcement is especially important in data protection because individuals often lack access to

the information needed to understand how their personal data has been handled. An organisation may hold the relevant records and technical details, while the individual may know only what they were asked to provide.

The Act's obligations on Data Fiduciaries can help address this imbalance by placing responsibility on the organisations handling the data. However, individuals must also be able to understand where they can raise a concern and what procedure they need to follow.

A complaint mechanism may offer limited protection if it is difficult to access or if individuals do not know when they can use it. Similarly, the existence of penalties does not automatically guarantee that organisations will comply with their obligations.

The practical value of the enforcement framework will depend on how the Board operates, how complaints are handled and whether organisations respond appropriately to their legal responsibilities. Effective enforcement is necessary to ensure that the rights recognised by the Act have consequences in practice.

8. Critical Evaluation: Is the DPDP Act Sufficient?

The DPDP Act, 2023, establishes an important framework for protecting digital personal data in India. It addresses several concerns through its provisions on consent, notice, withdrawal, individual rights, security and organisational accountability. However, the question of whether it sufficiently protects individual autonomy requires a closer look at how these safeguards work together.

The first concern is the quality of consent. The Act requires consent to meet specific legal standards, but individuals may still find it difficult to understand privacy notices or assess the consequences of sharing their information. A person may formally agree without fully appreciating the request. This raises questions about how effectively the law can protect autonomy when the decision-making process itself is difficult to navigate.

The second concern is the limited practical choice available to some users. Where an important service is accessible only after accepting its terms, refusing consent may not be a realistic option. The requirements under Section 6 provide a basis for examining whether consent is free and whether the information requested is necessary, but the practical effect of those requirements depends on their application.

A third concern is that consent is not required for every form of processing. Sections 7 and 17 permit processing in specified circumstances without consent or provide exemptions. These provisions may serve legitimate purposes, but they also mean that individuals cannot always control processing simply by refusing permission. The legal safeguards governing these situations are therefore central to the protection of autonomy.

The rights available to individuals also require attention. The ability to withdraw consent, seek correction or erasure were permitted and raise grievances can help people retain control over their information. Yet these rights have limited value if the relevant procedures are difficult to understand or if organisations do not comply with their obligations.

Finally, the Act places responsibilities on Data Fiduciaries, but those responsibilities must be implemented and enforced. Individuals should not be expected to carry the entire burden of protecting their data when organisations have greater access to the systems, records and technical knowledge involved in processing it.

The judicial decisions discussed in this article provide a broader perspective on these issues. *Puttaswamy* establishes the constitutional importance of privacy, while the Aadhaar judgment and *Anuradha Bhasin* offer relevant principles concerning legal justification and safeguards. *Brojo Nath Ganguly* also provides a useful analogy for considering how unequal bargaining power may affect the significance of apparent agreement.

These cases do not establish that the DPDP Act is legally insufficient. Rather, they help identify the questions that should be asked when evaluating the Act's operation. The key issue is not simply whether a consent mechanism exists, but whether individuals can understand and exercise their choices and whether the law protects them when consent is not the basis for processing.

For these reasons, the Act should be viewed as an important starting point rather than a complete answer to every concern about digital autonomy. Its effectiveness will depend on the quality of consent practices, the limits placed on data collection, the safeguards applicable to non-consensual processing and the availability of effective remedies.

9. Suggestions for Strengthening Individual Autonomy

The DPDP Act provides several protections, but certain practical measures could help

individuals make better-informed decisions and exercise their rights more easily.

First, privacy notices should be easier to understand. Organisations should explain what information they need, why they need it and how it will be used. Important conditions should not be hidden in lengthy documents or technical language. A user should be able to identify the main consequences of a decision without having to interpret a complicated legal document.

Second, necessary and optional data collection should be distinguished clearly. A person who wants to use a service should not automatically be expected to agree to unrelated data collection. This would help give practical effect to Section 6's requirement that consent be limited to the specified purpose and the personal data necessary for it.

Third, withdrawing consent should be straightforward. Where processing is based on consent, individuals should be able to withdraw it without unnecessary steps. The withdrawal process should be as accessible as the process used to give consent in the first place.

Fourth, organisations should take accountability seriously. Data Fiduciaries should maintain appropriate records, review their data collection practices and ensure that their Data Processors comply with applicable obligations. Data protection should form part of the way a service is designed and operated, rather than being treated as a formality.

Fifth, individuals should be made more aware of their rights. Clear public guidance can help users understand how to access information about their personal data, request correction or erasure where permitted, withdraw consent and raise grievances. This is particularly important for people who are unfamiliar with legal or technical terminology.

Sixth, processing without consent should remain within the limits permitted by law. Where the Act authorises processing without consent, the relevant conditions and safeguards should be observed. Where State action affects fundamental rights, the applicable constitutional requirements must also be considered.

Finally, enforcement mechanisms should be accessible and effective. Individuals should be able to raise concerns without facing unnecessary procedural difficulties, and complaints should receive appropriate consideration. Organisations must also understand that their obligations involve more than obtaining consent; they must comply with the other applicable requirements of the law.

These measures would not remove every difficulty associated with digital privacy. They could, however, help ensure that consent provides a genuine opportunity to make a choice rather than merely recording that a user has accepted a set of terms.

10. Commencement and Implementation of the Act

An important point to consider when evaluating the DPDP Act is the difference between the enactment of legislation and the commencement of its provisions. A law may have been passed, but its provisions do not necessarily become operative on the same date.

The Central Government issued notification G.S.R. 843(E) on 13 November 2025, providing for different provisions of the DPDP Act to commence in phases. Under the notification, Section 6(9), concerning Consent Managers, is scheduled to commence one year after publication. Sections 3–5, Sections 6(1)–(8) and 6(10), Sections 7–17 and several related provisions are scheduled to commence eighteen months after publication. On that timeline, the principal consent provisions are scheduled to commence on 13 May 2027.⁵

The Digital Personal Data Protection Rules, 2025, also provide for phased commencement. The applicable dates should be checked against any subsequent official notification before the article is submitted or published.⁶

This distinction is important to the argument of this article. The DPDP Act establishes the legal framework being examined, but the practical effectiveness of its provisions depends on when they become operative and how they are implemented. It would be inaccurate to describe provisions that have not yet commenced as though they are already fully operational.

The implementation period also provides an opportunity to consider whether individuals will be able to understand and exercise their rights in practice. Clear guidance, accessible procedures and compliance by Data Fiduciaries will be important to making the statutory framework effective.

11. Conclusion

The Digital Personal Data Protection Act, 2023, marks an important development in India's approach to digital personal data protection. Its provisions on consent, notice, withdrawal, individual rights and organisational accountability provide a legal framework for addressing

several concerns associated with the collection and use of personal information.

However, the existence of a legal framework does not automatically mean that individuals have meaningful control over their data. Consent may be affected by complicated privacy notices, limited alternatives and differences in bargaining power between users and digital platforms. In addition, the Act permits processing without consent in specified circumstances, making the safeguards governing that processing particularly important.

The Supreme Court's decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India* establishes the constitutional importance of privacy, dignity and individual autonomy. The Aadhaar judgment and *Anuradha Bhasin* provide relevant principles for examining legal justification and safeguards, while *Central Inland Water Transport Corporation Ltd. v. Brojo Nath Ganguly* offers a useful perspective on the effect of unequal bargaining power. Although these cases do not directly interpret the DPDP Act, they help frame the legal and practical questions surrounding individual choice.

In my view, the Act provides an important foundation, but consent alone cannot guarantee autonomy. Individuals must be able to understand what they are agreeing to, refuse unnecessary data collection and exercise their rights without unreasonable difficulty. Where consent is not required, the applicable legal limits and safeguards must provide meaningful protection.

Ultimately, the question is not simply whether a user has clicked “I agree”. It is whether the person had a reasonable opportunity to understand the decision, whether the organisation respects the limits of that agreement and whether the law provides protection when things go wrong.

The DPDP Act has the potential to strengthen the protection of personal information in India. Whether it is sufficient to protect individual autonomy will depend on how its provisions are implemented, how effectively organisations are held accountable and whether individuals can exercise the rights the law recognises. The real test will be whether the framework gives people more than a formal right to consent and allows them to exercise meaningful control over their personal information.

References

1. The Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).
2. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
3. *K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1 (India).
4. *Central Inland Water Transport Corporation Ltd. v. Brojo Nath Ganguly*, (1986) 3 SCC 156 (India).
5. *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637 (India).
6. Notification No. G.S.R. 843(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Nov. 13, 2025) (India) (providing for the phased commencement of the Digital Personal Data Protection Act, 2023).
7. Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Nov. 13, 2025) (India).