



Supreme Court Examines DPDP Act Changes to RTI Framework, Raising Fundamental Questions on Privacy, Transparency and Public Accountability

Published On: 11-08-2026

Recent Developments:

- **Supreme Court scrutiny:** The **Supreme Court of India** is examining petitions challenging **Section 44(3) of the Digital Personal Data Protection Act, 2023**, which amended **Section 8(1)(j) of the Right to Information Act, 2005**.
- **Larger Bench:** In February 2026, the Supreme Court referred challenges concerning the **Digital Personal Data Protection Act, 2023** and its rules to a **five-judge Bench**, while declining to stay the operation of the challenged framework.
- **Core constitutional issue:** The petitions raise concerns about whether the amended RTI exemption excessively restricts **transparency and the citizen's right to know**, particularly where information relating to public officials has a genuine public-interest dimension.
- **April 2026 development:** The Supreme Court also sought the Centre's response to a public-interest petition challenging provisions of the **Digital Personal Data Protection Act, 2023** on the ground that they could dilute transparency under the **Right to Information Act, 2005**.
- **Current legal position:** The amendment to **Section 8(1)(j)** came into force on **13 November 2025** through the commencement notification for **Section 44(3)** of the Digital Personal Data Protection Act.
- **Rules framework:** The **Digital Personal Data Protection Rules, 2025** were notified on **14 November 2025**, alongside the enforcement timeline and establishment-related notifications for the **Data Protection Board of India**.

Background to the RTI-DPDP Conflict:

Amendment to Section 8(1)(j):

- **Section 44(3) of the Digital Personal Data Protection Act, 2023** substituted the earlier **Section 8(1)(j) of the Right to Information Act, 2005**.
- The amended provision now exempts **"information which relates to personal information"** from disclosure under the relevant RTI exemption.
- The earlier provision specifically dealt with personal information and contained safeguards linked to **public activity and larger public interest**.
- The change has therefore raised concerns that information concerning public officials could be denied merely because it is characterised as **personal information**, even where disclosure may have significant public-interest implications.
- The controversy reflects a broader tension between two legitimate constitutional objectives, namely **the right to privacy under Article 21** and **the right to information linked to Article 19(1)(a)**.

Constitutional Question Before the Supreme Court:

- The Supreme Court is required to examine how the **RTI Act and DPDP Act**, both enacted by Parliament, can operate coherently without unnecessarily defeating the purpose of either law.
- The central interpretative question is whether the newer data-protection framework should be read as substantially restricting the transparency framework created by the RTI Act.
- The Court may therefore have to consider principles of **harmonious construction, proportionality and constitutional rights balancing** while interpreting the two statutes.
- The dispute is significant because the **right to information** enables citizens to scrutinise public institutions, while the **right to privacy** protects individuals against unjustified disclosure of personal data.

Digital Personal Data Protection Act, 2023:

Evolution of the Data Protection Framework:

- In 2017, the **Ministry of Electronics and Information Technology** constituted the **Justice B. N. Srikrishna Committee** to examine the framework for protection of personal data in India.
- The Committee's work contributed to the evolution of India's statutory data-protection framework.
- The **Digital Personal Data Protection Act, 2023** was enacted on **11 August 2023** and establishes a framework for processing digital personal data while recognising both privacy interests and lawful data processing requirements.

Scope of the Act:

- The Act applies to the **processing of digital personal data within India** where the data is collected digitally or collected offline and subsequently digitised.
- It can also apply to processing outside India where such processing is connected with offering **goods or services to individuals in India**.
- The framework therefore has both **territorial and extra-territorial dimensions**.

Consent and Lawful Processing:

- The Act establishes **consent** as an important basis for processing personal data.
- Consent must generally be **free, specific, informed and unambiguous**, and it must relate to a specified purpose.
- The Act also recognises specified **legitimate uses** where processing may occur without obtaining consent in circumstances provided by law.
- Such legitimate uses include specified forms of State processing and voluntary provision of personal data by individuals.

Obligations of Data Fiduciaries:

- **Data fiduciaries** are required to take reasonable measures to ensure the accuracy and security of personal data.
- They must implement appropriate **technical and organisational safeguards** to prevent personal-data breaches.
- Personal data should generally be erased when its retention is no longer necessary for the specified purpose, subject to legal requirements.
- Data fiduciaries must also provide mechanisms for handling **grievances and exercising data-related rights**.

Rights of Data Principals:

- Individuals, described as **data principals**, receive rights relating to their personal data.
- These include rights to obtain information about processing, seek **correction and erasure**, and obtain **grievance redressal**.

- The framework therefore shifts Indian data governance from a predominantly sectoral approach towards a more comprehensive statutory architecture.

Government Exemptions:

- The Act permits specified exemptions from its provisions for certain State agencies and circumstances involving **national security, sovereignty and integrity, public order, prevention of offences and other specified grounds**.
- Such exemptions are significant because they determine the balance between **State interests, individual privacy and accountability**.
- The breadth and safeguards surrounding these exemptions are therefore relevant to constitutional scrutiny.

Data Protection Board of India:

- The Act establishes the **Data Protection Board of India** as the principal statutory body for adjudicating specified matters relating to non-compliance.
- The Board can deal with matters involving **personal-data breaches and statutory contraventions**.
- The statutory framework provides the Board with specified powers and procedures for adjudication.
- The **2025 notification framework** formally established the Board and provided for its operationalisation.

Right to Information Act, 2005:

Objectives:

- The **Right to Information Act, 2005** seeks to promote **transparency, accountability and participatory democracy** by providing citizens access to information held by public authorities.
- The Act strengthens the ability of citizens to scrutinise governmental decisions, expenditure and administrative functioning.
- The RTI framework is therefore an important instrument of **democratic accountability and good governance**.

Scope:

- The Act applies to **public authorities**, including constitutional and statutory bodies, government departments, ministries and bodies substantially financed by the government, subject to statutory conditions.
- Under **Section 3**, Indian citizens possess the right to information subject to the exemptions and limitations contained in the Act.
- Information under the Act broadly includes **records, documents, memoranda, e-mails, opinions, advice, circulars, orders, logbooks, contracts, reports and electronically stored data** held by or under the control of a public authority.

Time Limit for Providing Information:

- A **Central Public Information Officer or State Public Information Officer** is generally required to provide or reject an RTI request within **30 days**.
- Where the information concerns the **life or liberty of a person**, it must ordinarily be provided within **48 hours**.
- Appeals are subject to separate statutory timelines, with the relevant Information Commission generally required to dispose of an appeal within **30 days**, extendable to **45 days** for recorded reasons.

Exemptions:

- The RTI Act does not create an unrestricted right to every category of information held by public authorities.

- **Section 8** provides exemptions covering interests such as national security, sovereignty, commercial confidence, fiduciary relationships, investigation-related information and personal information, among others.
- The exemption framework attempts to balance **maximum disclosure** with protection of legitimate competing interests.
- The Supreme Court has recognised that **Section 8(1)** operates as a set of statutory exceptions to the general citizen's right to access information.

Accountability Mechanism:

- The Act establishes the **Central Information Commission and State Information Commissions** for adjudicating appeals and complaints under the statutory framework.
- The Information Commissions can direct public authorities to provide information and can impose penalties on responsible officers in specified circumstances.
- The RTI framework therefore combines **citizen access, administrative obligations and appellate oversight**.

How the DPDP Amendment Changes the RTI Framework:

Earlier Position:

- Earlier **Section 8(1)(j)** permitted exemption of certain personal information where disclosure had an impermissible relationship with public activity or where disclosure would cause unwarranted invasion of privacy.
- The provision also contained a **larger public-interest balancing mechanism**.
- This structure enabled authorities and Information Commissions to weigh the individual's privacy interest against the public interest in disclosure.

Present Position:

- Section 44(3) of the DPDP Act replaced the earlier wording with the broader formulation concerning **information which relates to personal information**.
- The statutory amendment has removed the earlier express **larger public-interest proviso** from Section 8(1)(j).
- Critics therefore argue that the amendment may make it easier for public authorities to deny information by classifying it as personal information.
- Supporters of stronger privacy protection can argue that personal data should not become routinely accessible merely because it is held by a public authority.

Why the Change Matters:

- The amendment can affect access to information concerning **public servants, beneficiaries, government appointments, public expenditure and administrative decisions** where personal information is embedded within official records.
- Excessively broad interpretation could reduce the effectiveness of RTI as a mechanism for detecting **corruption, conflicts of interest and misuse of public resources**.
- Excessively narrow privacy protection, however, could expose individuals to unjustified disclosure of sensitive personal information.
- The central challenge is therefore to prevent both **opacity in public administration** and **unjustified intrusion into individual privacy**.

Constitutional Dimensions:

Right to Information and Article 19:

Kamaraj IAS Academy

Plot A P.127, AF block, 6 th street, 11th Main Rd, Shanthi Colony, Anna Nagar, Chennai, Tamil Nadu 600040

Phone: **044 4353 9988 / 98403 94477** / Whatsapp : **09710729833**

- The **right to information** has been judicially recognised as having a constitutional connection with **freedom of speech and expression under Article 19(1)(a)**.
- Access to information enables citizens to form opinions, participate meaningfully in public affairs and hold authorities accountable.
- Restricting access to information can therefore have consequences beyond ordinary statutory rights.

Right to Privacy and Article 21:

- The Supreme Court recognised **privacy as a fundamental right under Article 21** in the **Justice K. S. Puttaswamy v. Union of India** judgment of 2017.
- Privacy protects individuals against unjustified intrusion into their personal sphere.
- Digitalisation has increased the importance of privacy because personal information can be collected, aggregated, processed and disseminated at unprecedented scale.

Proportionality:

- Any restriction affecting a fundamental right must satisfy constitutional requirements, including the principle of **proportionality**.
- A restriction should pursue a legitimate objective, have a rational connection with that objective, be necessary and maintain a reasonable balance between competing rights and interests.
- The DPDP–RTI controversy therefore provides an important setting for examining how **privacy and transparency can coexist within constitutional limits**.

Harmonious Construction:

- Since the **RTI Act and DPDP Act are both Parliamentary enactments**, courts can attempt to interpret them so that both retain meaningful operation wherever possible.
- **Harmonious construction** seeks to avoid an interpretation under which one statute unnecessarily nullifies the purpose of another.
- This approach is particularly relevant where **privacy protection and transparency** are not inherently contradictory but require context-sensitive balancing.

Significance of the RTI Act:

Empowering Citizens:

- RTI converts citizens from passive recipients of government decisions into **active participants in democratic governance**.
- Access to official records enables citizens to question administrative decisions and demand explanations from public authorities.

Strengthening Accountability:

- RTI facilitates scrutiny of **government expenditure, procurement, implementation of welfare programmes and administrative decisions**.
- It can expose irregularities and create documentary evidence for further administrative, legal or social action.

Combating Corruption:

- Access to public records can help identify **financial irregularities, manipulation of records, conflict of interest and misuse of public resources**.
- RTI has therefore become an important instrument for transparency-driven anti-corruption efforts.

Supporting Social Audits:

Kamaraj IAS Academy

Plot A P.127, AF block, 6 th street, 11th Main Rd, Shanthi Colony, Anna Nagar, Chennai, Tamil Nadu 600040

Phone: **044 4353 9988 / 98403 94477 / Whatsapp : 09710729833**

- Citizens, civil-society organisations and community groups can use RTI to verify the implementation of welfare programmes.
- RTI-based verification can complement **social audits** by allowing communities to compare official records with ground-level outcomes.

Strengthening Democratic Participation:

- Transparency improves citizens' ability to understand government policies and evaluate institutional performance.
- The RTI framework therefore strengthens **participatory democracy, informed citizenship and public trust**.

Major Concerns Associated with the DPDP–RTI Interface:

Risk of Overbroad Privacy Claims:

- A broad interpretation of **personal information** could allow authorities to deny information even where disclosure has a substantial connection with public accountability.
- Such an approach could weaken the principle of **maximum disclosure with minimum exemptions** underlying transparency legislation.

Impact on Investigative Journalism:

- Journalists frequently use public records to investigate **corruption, regulatory failures and conflicts of interest**.
- Broad restrictions on access to personal information could make it more difficult to establish relationships between individuals and public decisions.
- Petitioners have therefore raised concerns regarding the potential impact of the framework on **investigative journalism and public-interest reporting**.

Public Officials and Public Accountability:

- The distinction between a person's **private capacity and public function** becomes important when personal information is connected with official decision-making.
- A blanket approach could fail to distinguish between genuinely private information and information whose disclosure is necessary to examine the exercise of public power.

Risk of Excessive Data Disclosure:

- The opposite extreme can also undermine individual privacy by allowing personal information to be disclosed merely because it is held by a public authority.
- Sensitive information relating to **health, family, identity, finances or other private matters** may cause serious harm if disclosed without adequate justification.
- Effective governance therefore requires a principled distinction between **information necessary for public accountability and information that is genuinely private**.

Institutional Capacity:

- Effective RTI depends not only on statutory provisions but also on **adequately staffed Information Commissions, timely disposal of appeals and effective enforcement**.
- Vacancies and delays in the information-commission system can weaken the practical value of the right even when the statutory framework remains intact.

- The Central Information Commission continues to exercise jurisdiction over **Central Public Authorities**, highlighting its institutional importance in the RTI architecture.

Way Forward:

Develop a Rights-Balancing Framework:

- The Government and courts should ensure that **privacy and transparency are treated as complementary constitutional values rather than mutually exclusive rights**.
- Disclosure should depend on the nature, sensitivity and public-interest relevance of the information rather than an excessively broad classification of all personal information.

Protect Genuine Public Interest:

- Information directly connected with **public functions, public expenditure, official decision-making or allegations of wrongdoing** should receive stronger transparency safeguards where legally permissible.
- Genuine personal information unrelated to public functions should receive robust privacy protection.

Strengthen Institutional Safeguards:

- **Information Commissions** should have adequate personnel and technological capacity to dispose of appeals efficiently.
- Clear administrative guidance can reduce inconsistent decisions by Public Information Officers.
- Data-protection authorities and transparency institutions should develop mechanisms for dealing with situations where the two regulatory objectives intersect.

Ensure Proportionality:

- Restrictions on information access should satisfy **legality, legitimate objective, necessity and proportionality**.
- The regulatory framework should avoid both indiscriminate disclosure and indiscriminate secrecy.

Promote Data Minimisation:

- Public authorities should collect and retain only the personal data necessary for legitimate administrative purposes.
- Better **data governance, anonymisation and redaction** can sometimes permit disclosure of public-interest information without exposing unnecessary personal details.

Preserve Democratic Accountability:

- Data protection should not become an instrument for creating unnecessary **administrative opacity**.
- At the same time, transparency should not become a justification for indiscriminate exposure of private citizens' personal data.
- India needs a framework in which **privacy protects citizens from unnecessary intrusion while transparency protects citizens from unaccountable exercise of public power**.

Conclusion:

- The RTI–DPDP controversy represents a fundamental challenge of **digital-era constitutional governance**, where the State simultaneously holds enormous quantities of personal data and exercises public power that requires democratic scrutiny.
- The objective should not be to choose between **privacy and transparency**, but to develop a legally coherent framework that protects genuine personal privacy while preserving legitimate public-interest access to

information.

- A balanced approach based on **proportionality, harmonious construction, data minimisation, institutional independence and public accountability** can strengthen both the privacy regime and India's transparency architecture.

Value Addition for UPSC:

Constitutional and Legal Keywords:

- **Article 19(1)(a):** Freedom of speech and expression, which has a constitutional relationship with the **right to know**.
- **Article 21:** Protection of life and personal liberty, encompassing the **right to privacy**.
- **Section 8(1)(j), RTI Act:** Statutory exemption relating to **personal information**, substantially modified through Section 44(3) of the DPDP Act.
- **Section 44(3), DPDP Act:** Provision that amended the RTI Act's Section 8(1)(j).
- **Proportionality:** Constitutional standard for assessing whether restrictions on fundamental rights are justified.
- **Harmonious construction:** Interpretative principle that seeks to allow two statutes to operate coherently without unnecessarily defeating either law.
- **Puttaswamy judgment, 2017:** Landmark Supreme Court judgment recognising **privacy as a fundamental right**.

UPSC Mains Linkages:

- **Essay:** "Privacy and transparency are not competing absolutes but complementary pillars of democratic governance."
- **Ethics, Integrity and Aptitude:** Accountability, transparency, confidentiality, privacy, public interest and ethical use of official information.

One-Line Mains Conclusion:

- "A mature democracy must ensure that privacy protects the individual from unnecessary exposure, while transparency protects society from unaccountable power."