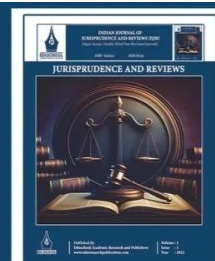




INDIAN JOURNAL OF JURISPRUDENCE AND REVIEWS (IJJR)

(Open Access, Double-Blind Peer Reviewed Journal)

ISSN Online: 3139-177X



Data Protection And The Right To Information: Section 44(3) In India

Sharmila

Indian Institute of Management, Rohtak, India

Article Information

Received: 6th July 2026

Received in revised form: 19th July 2026

Accepted: 24th August 2026

Available online: 2nd September 2026

Volume: 2

Issue: 3

DOI: <https://doi.org/10.63090/IJJR/3139.177X.0022>

Abstract

The Digital Personal Data Protection Act 2023 amended the Right to Information Act 2005 through a single sub-section of its miscellaneous chapter. The amendment substituted the exemption for personal information in the transparency statute, removing the qualification that had made disclosure turn on the presence of a larger public interest. This article examines the amendment as a question of statutory design rather than as a contest between privacy and transparency. It argues that the balancing structure removed by the amendment was not an accident of drafting but the mechanism through which the transparency statute reconciled two constitutional interests, and that its removal transfers a judgment previously made case by case into a categorical rule applied at the level of the information class. The article traces the judicial construction of the earlier provision, which had already narrowed disclosure considerably, and shows that the amendment displaces the very authority that produced that narrowing. It examines the constitutional position after the privacy judgment, the special problem of information about public servants acting in an official capacity, and the position of statutes elsewhere that address the same conflict through an exception rather than a prohibition. It proposes the restoration of the public interest override, a defined class of official capacity information excluded from the exemption, and a duty to record reasons.

Keywords: - Right To Information, Data Protection, Personal Information, Privacy, Transparency, India

1. INTRODUCTION

Amendments to one statute made in the miscellaneous chapter of another rarely attract the attention their effects deserve. Section 44(3) of the Digital Personal Data Protection Act 2023 is a case in point. It occupies a few lines, it appears among consequential provisions, and it substitutes clause (j) of sub-section (1) of Section 8 of the Right to Information Act 2005. The provision it replaced had governed every request in which the information sought concerned an identifiable person, which is to say a very large proportion of all requests made under the Indian transparency statute.

This article examines the amendment. The examination is deliberately narrow. It does not attempt a general assessment of the data protection statute, on which there is now a considerable literature, and it does not treat privacy and transparency as opposed values requiring a winner. Its question is structural: what did the replaced provision do, what does the substituted provision do, and what happens to the interests that the earlier structure reconciled.

The argument is that the earlier clause performed a specific and unusual function. It did not exempt personal information. It exempted personal information subject to a condition that returned the matter to the deciding officer whenever a larger public interest was shown. That condition is the reason the clause could accommodate both constitutional interests within a single provision. Removing it does not adjust the balance; it removes the instrument through which the balance was struck.

II. THE TWO STATUTES

The Right to Information Act 2005 gives every citizen a right of access to information held by a public authority, subject to exemptions in Section 8 and to a general public interest override in sub-section (2) of that section. Naib (2011) describes the design as one in which the exemptions are narrow, the override is general, and the burden of justifying refusal rests on the

public authority. That allocation of burden is the statute's distinguishing feature. It is what separates it from the earlier position in which official information was presumptively closed.

The Digital Personal Data Protection Act 2023 regulates the processing of digital personal data by data fiduciaries. It imposes obligations of notice and consent, creates rights for data principals, and constitutes a Data Protection Board. Parsheera (2025), reviewing the long process that produced the statute, characterises the outcome as a framework whose substantive content depends heavily on delegated legislation and on the exemptions available to the state. Srivastava (2019) anticipated the difficulty during the drafting period. Calibrating a data protection regime is unusually hard in a jurisdiction where the state is itself the largest processor of personal data.

The two statutes are not natural adversaries. One regulates the state's disclosure of information it holds; the other regulates the processing of personal data by those who hold it. The conflict arises only at the point where a citizen asks a public authority for a record that identifies another person. Indian law addressed that intersection, before 2023, in the clause that Section 44(3) has now replaced.

III. THE PROVISION BEFORE THE AMENDMENT

The clause as originally enacted exempted information relating to personal information the disclosure of which had no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual. It then added a proviso: unless the officer concerned was satisfied that the larger public interest justified the disclosure of such information.

Three elements of that drafting deserve notice. The exemption was conditional on the absence of a relationship to public activity, which meant that information about an official act was outside it from the start. It required the invasion of privacy to be unwarranted, which is a comparative judgment rather than a categorical one. It attached an override exercisable by the deciding officer.

Judicial construction narrowed the clause considerably. In *Girish Ramchandra Deshpande v. Central Information Commissioner*, (2013) 1 SCC 212, the Supreme Court held that the service record of a public servant, including details of assets, income tax returns and disciplinary proceedings, was personal information within the clause, disclosable only on a demonstration of larger public interest. That holding was applied in *Canara Bank v. C.S. Shyam*, decided on 31 August 2017, where information about transfers and postings of employees was likewise treated as personal.

The Constitution Bench in *Central Public Information Officer, Supreme Court of India v. Subhash Chandra Agarwal*, (2020) 5 SCC 481, revisited the position in the context of information about judges. It held that the office of the Chief Justice of India is a public authority under the statute, and set out a structured approach in which the nature of the information, the relationship it bears to public activity and the extent of the invasion of privacy are weighed against the public interest asserted. Two features of that judgment matter here. It treated the assessment as one of proportionality rather than category, and it insisted on the procedure for third party information, requiring that the person concerned be heard.

The state of the law before 2023 was therefore not one of open disclosure of personal information. It was one of restricted disclosure, restricted by judicial construction, with a residual route available where the applicant could show a public interest of sufficient weight.

IV. THE TEXT AFTER THE AMENDMENT

The substituted clause exempts information which relates to personal information. The qualifying conditions and the proviso are gone.

Two readings are available, and the difference between them is substantial. On the first, the clause now exempts every record that relates to an identifiable individual, whatever its connection to public activity, with no route to disclosure on public interest grounds within Section 8(1)(j). On the second, the general override in Section 8(2) survives and can be applied, since it operates in terms on the whole of Section 8.

The second reading is the better one as a matter of construction, because Section 8(2) was not amended and a court will be slow to treat it as impliedly repealed for one clause alone. It is not, however, an equivalent substitute. The override in Section 8(2) is framed as a discretion where the public interest in disclosure outweighs the harm to protected interests, and it has been applied sparingly. The proviso to clause (j) was addressed to the officer as part of the very test he was applying. Relocating the balancing exercise from the operative clause to a general discretion changes both its prominence and, in practice, its frequency of use.

There is also a drafting consequence that will be felt in adjudication, and it is easily overlooked. The judicial authority developed under the earlier clause was built on words that no longer appear in the statute: *Girish Ramchandra Deshpande* turned on whether information had a relationship to public activity, and *Subhash Chandra Agarwal* turned on the weighing that the proviso authorised. Neither test has a textual home in the substituted clause. An information commission that wishes to apply the reasoning of either judgment must now do so by analogy, against a provision whose language points the other way.

V. COMMENCEMENT AND THE ASYMMETRY IT CREATES

The amendment did not take effect when the statute received assent. The 2023 Act provided for commencement on dates to be appointed, and the appointment was made in November 2025, when the Digital Personal Data Protection Rules 2025 were notified and the constitution of the Data Protection Board was announced. The commencement was staggered.

The staggering produces an asymmetry that bears directly on the argument of this article. The provisions establishing the Board and a group of ancillary provisions, including the amendment to the transparency statute, were brought into force at once. The obligations of data fiduciaries and the rights of data principals, which are the substance of the protective scheme, were deferred, with the principal compliance obligations taking effect eighteen months after notification and the provisions on consent managers at twelve months.

A citizen therefore stands, for a period of some eighteen months, in a position where the restriction on access has taken effect and the corresponding protection has not. The record about a third party is exempt from disclosure by reason of a statute whose obligations of purpose limitation, security and erasure do not yet bind the authority holding it. The sequence is difficult to defend. The justification advanced for the amendment is that personal data requires stronger protection than the earlier clause afforded, and that justification presupposes the operation of the protective scheme. A commencement order that brings the restriction into force while deferring the protection removes the premise of its own defence.

The point is not merely one of timing. Commencement in this staggered form was a matter of executive choice, exercised under a power the legislature conferred without conditions. A restriction on a right that has constitutional standing under Article 19(1)(a) was therefore brought into operation by an administrative instrument, at a moment selected by the administration, and separately from the provisions that were said to justify it.

VI. THE CONSTITUTIONAL POSITION

The privacy judgment in *Justice K. S. Puttaswamy v. Union of India*, (2017) 10 SCC 1, established informational privacy as an aspect of the right under Article 21 and set out a test of legality, legitimate aim and proportionality for restrictions upon it. That judgment is frequently cited in support of the amendment, on the footing that the state was obliged to protect personal data more firmly.

The citation proves less than it appears to. The right to information has its own constitutional foundation. In *State of Uttar Pradesh v. Raj Narain*, (1975) 4 SCC 428, the Supreme Court recognised the right of the people to know the particulars of every public transaction, and in *S. P. Gupta v. Union of India*, 1981 Supp SCC 87, the Court located access to information about the functioning of government within Article 19(1)(a). Both interests are constitutionally protected, and the proportionality analysis in *Puttaswamy* applies to the restriction of either. A categorical exemption that operates without regard to the weight of the public interest asserted in the particular case is, on its face, harder to justify under a proportionality standard than a provision that requires the weighing to be done.

The *Aadhaar* judgment, *Justice K. S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1, is instructive on a related point. In upholding the identity scheme in part, the majority relied on the availability of safeguards and on the limitation of purposes, and struck down provisions that permitted use beyond the purpose for which the framework was justified. The reasoning turns on the fit between the restriction and its objective. An exemption drawn at the level of the class rather than the record has a poor fit where a substantial part of the class consists of information about the discharge of public functions.

VII. THE PUBLIC SERVANT PROBLEM

The sharpest practical consequence concerns information about public servants acting in an official capacity. Attendance records, tour claims, expenditure sanctioned by a named officer, the allotment of a public benefit to a named beneficiary, and disciplinary outcomes all relate to identifiable individuals. On the wider reading of the substituted clause, each is exempt.

The consequence extends to the verification of public expenditure. *Muralidharan, Niehaus and Sukhtankar* (2016), in an evaluation of biometric payment infrastructure in Andhra Pradesh, demonstrate that measurable reductions in leakage in welfare payments depend on the ability to compare a record of entitlement with a record of receipt at the level of the named beneficiary. Social audit practice in employment guarantee and food distribution programmes rests on the same comparison. Where beneficiary level records are exempt as personal information, the audit becomes an examination of aggregates, and aggregates conceal precisely the diversion that the audit is designed to detect.

John (2025), analysing consent, accountability and data sovereignty in India's digital public infrastructure, identifies a related difficulty in the attribution of responsibility across the layers of those systems. The observation applies with force here. Where the record that would identify the responsible official is exempt from disclosure by virtue of relating to a person, accountability for an administrative act becomes dependent on the willingness of the administration to disclose it.

VIII. HOW OTHER SYSTEMS DRAW THE LINE

Access to information statutes elsewhere address the same conflict, and the common technique is an exception rather than a prohibition. Personal information is exempt, and the exemption is displaced where disclosure is necessary in the public interest, or where the information concerns the person in a professional or official capacity, or where the individual concerned has consented after notice.

The third of these devices is already present in Indian law. The procedure for third party information in Section 11 of the 2005 Act requires notice to the person concerned and consideration of any objection, and *Subhash Chandra Agarwal* emphasised its importance. That procedure is a proportionate mechanism: it protects the individual by giving a hearing rather than by closing the class. It survives the amendment, but its utility is reduced, since a categorical exemption removes the occasion for the procedure to operate at all.

IX. WHAT SHOULD BE RESTORED

Three changes would repair the position without weakening the protection of personal data.

The public interest override should be restored to the operative clause. Its location matters. An override that appears in the same provision as the exemption is applied by the officer as part of the same decision, and it generates a record of reasons that can be tested in appeal.

Information concerning a person in an official or professional capacity should be expressly excluded from the exemption, with a defined list covering the discharge of public functions, the receipt of public money and the exercise of

statutory power. This is the class in which the transparency interest is strongest and the privacy interest weakest, and drawing it in the statute removes the need for case by case litigation over the boundary.

A duty to record reasons should attach to every refusal under the clause. The 2005 Act already requires reasons for rejection, but a specific requirement that the officer state why the record relates to a person otherwise than in an official capacity would preserve, in a modest form, the analytical discipline that the deleted proviso imposed.

X. CONCLUSION

Section 44(3) is a short provision with a long reach. It replaced a clause that had been the principal site at which Indian law reconciled the constitutional interest in privacy with the constitutional interest in access to information, and it replaced it with a categorical exemption. The reconciliation has not been relocated; it has been removed from the operative provision and left to a general discretion that is exercised infrequently.

The case for restoring the override does not rest on a preference for transparency over privacy. It rests on the observation that the interests conflict at the level of the individual record and not at the level of the class, and that a rule drawn at the level of the class will therefore be over inclusive in a predictable and substantial way. The clause as it stood was capable of protecting a citizen's medical record and disclosing a district officer's sanction of a contract. The clause as substituted treats the two alike.

REFERENCES

- Canara Bank v. C. S. Shyam (Supreme Court of India, 31 August 2017).
Central Public Information Officer, Supreme Court of India v. Subhash Chandra Agarwal, (2020) 5 SCC 481 (India).
Digital Personal Data Protection Act, 2023 (India).
Digital Personal Data Protection Rules, 2025 (India).
Girish Ramchandra Deshpande v. Central Information Commissioner, (2013) 1 SCC 212 (India).
John, S. (2025). The legal architecture of digital public infrastructures: Consent, accountability, and data sovereignty in India's Aadhaar and UPI systems. *International Journal of Judicial Science Research Studies*, 2(4), 85. <https://doi.org/10.63090/ijjsrs/3049.0618.0028>
Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
Justice K. S. Puttaswamy (Retd.) v. Union of India, (2019) 1 SCC 1 (India).
Muralidharan, K., Niehaus, P., & Sukhtankar, S. (2016). Building state capacity: Evidence from biometric smartcards in India. *American Economic Review*, 106(10), 2895–2929. <https://doi.org/10.1257/aer.20141346>
Naib, S. (2011). Right to information in India. In *The right to information act 2005: A handbook* (pp. 21–39). Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780198067474.003.0002>
Parsheera, S. (2025). Awaiting the dawn of data protection regulation in India. In *Personal data architectures in the BRICS countries* (pp. 97–124). Oxford University Press. <https://doi.org/10.1093/9780198974468.003.0004>
Right to Information Act, 2005 (India).
S. P. Gupta v. Union of India, 1981 Supp SCC 87 (India).
Srivastava, A. K. (2019). Data protection law in India: The search for Goldilocks effect. *European Data Protection Law Review*, 5(3), 408–415. <https://doi.org/10.21552/edpl/2019/3/16>
State of Uttar Pradesh v. Raj Narain, (1975) 4 SCC 428 (India).