Page 706 - 725 **DOI:** *https://doi.org/10.63108/IJLMH.13255*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 6

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: https://www.ijlmh.com/
Under the aegis of VidhiAagaz (https://www.vidhiaagaz.com/)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact **support@vidhiaagaz.com**.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to **submission@ijlmh.com.**

Digital Personal Data Protection Act, 2023: Balancing the Right to Privacy and Freedom of Speech in India – A Critical Legal Analysis

SHASHI AGNIHOTRI[*] AND ANIL KUMAR PANDEY[**]

ABSTRACT

The Digital Personal Data Protection Act, 2023 (DPDP Act) is India's principal legislative response to the growing importance of personal data in a digitally connected society. It establishes obligations for entities that determine the purpose and means of processing digital personal data and recognises rights for the individuals to whom such data relates. The Act is also part of a larger constitutional conversation about informational privacy, dignity, autonomy, free expression and democratic accountability. The central difficulty is not whether privacy or expression should prevail in every case, but how law can protect both without allowing one interest to become an automatic veto over the other. This paper critically examines the constitutional and statutory relationship between the right to privacy under Article 21 and freedom of speech and expression under Article 19(1)(a) of the Constitution of India. It focuses on the consequences of data protection regulation for journalism, public interest reporting, research, access to government-held information and the right to know. Particular attention is paid to the structure of the DPDP Act, its consent and legitimate-use framework, the exemptions in section 17, the amendment to section 8(1)(j) of the Right to Information Act, 2005 through section 44(3), and the phased commencement of the Act and the Digital Personal Data Protection Rules, 2025. The research adopts a doctrinal and analytical methodology. It studies constitutional text, legislation, delegated rules, leading judicial decisions and comparative materials, especially Article 85 of the European Union General Data Protection Regulation.

Keywords: *Digital Personal Data Protection Act, 2023, right to privacy, freedom of speech, investigative journalism, Right to Information Act, 2005, proportionality, informational privacy.*

I. INTRODUCTION

Digital technology has changed the scale, speed and character of information exchange. Individuals communicate, work, purchase goods, obtain public services, use financial products and participate in political debate through digital systems. Each activity may generate

[*] Author is an LL.B. Student at TRC Law College, Barabanki, Uttar Pradesh, India.
[**] Author is an Independent Legal Researcher.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

information capable of identifying a person directly or indirectly. Such information may include contact details, location records, transaction histories, photographs, identity particulars, online identifiers, preferences and records of interactions. When combined, apparently ordinary data points may reveal intimate patterns about a person's health, finances, relationships, movements, beliefs or habits.

The collection and use of personal data can produce substantial benefits. It can make services more accessible, improve fraud detection, support research, facilitate public administration and enable innovation. At the same time, data processing can expose individuals to identity theft, discrimination, manipulation, profiling, surveillance, reputational injury and loss of control over personal information. The challenge for law is to permit socially valuable processing while preventing unfair, excessive or insecure use. This challenge is especially significant in a country with a large and diverse population, uneven digital literacy, substantial digitisation of public services and a rapidly expanding digital economy.

The DPDP Act, 2023 must be understood against this background. It is not merely a compliance statute for businesses. It gives legislative form to a set of concerns associated with informational privacy and places duties on persons and organisations processing digital personal data. It also recognises that data processing may be necessary for legitimate purposes, including certain uses specified by law.

II. Statement of the problem and scope of the study

The problem addressed is the uncertainty that may arise when data protection duties intersect with speech-related activity. A journalist who receives a leaked document, a non-profit organisation analysing public procurement, a researcher studying discrimination, or a citizen seeking information from a public authority may encounter personal data in the course of otherwise legitimate work. The legal consequences may depend on the identity of the actor, the purpose of processing, the source of information, the applicable statutory provision, the existence of an exemption and the manner in which the information is used or disclosed.

The issue is not limited to publication. It may arise at earlier stages: collection, verification, storage, analysis, sharing with editors or lawyers, contacting persons for comment, and retention of source material. A data protection framework can influence each stage. Uncertainty may lead to cautious self-censorship, particularly for smaller newsrooms, independent journalists, local-language media, civil society organisations and individual researchers who may lack specialist legal support.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

The scope of the paper is confined principally to the constitutional relationship between privacy and expression under Indian law, with a focus on the DPDP Act and the RTI amendment. The paper asks whether the DPDP Act, 2023, read with the DPDP Rules, 2025 and the wider constitutional framework, provides a sufficiently clear and proportionate balance between the right to privacy and freedom of speech and expression in India.

III. CONSTITUTIONAL EVOLUTION OF THE RIGHT TO PRIVACY IN INDIA

The constitutional status of privacy in India developed through judicial interpretation. The text of the Constitution does not contain a separate article expressly titled the right to privacy. Nevertheless, the Supreme Court gradually recognised privacy-related interests through the guarantees of life and personal liberty, equality and freedoms. The development reflects the understanding that constitutional rights must respond to changing social and technological conditions while remaining anchored in constitutional text and structure.[1]

Early decisions did not speak with one voice on whether privacy was independently protected. In *M.P. Sharma v. Satish Chandra*, the Court considered search and seizure in the context of constitutional protections and expressed reservations about importing a general right to privacy. In *Kharak Singh v. State of Uttar Pradesh*, the Court examined police surveillance. The majority rejected some privacy claims while recognising that unauthorised intrusion into a person's home could violate personal liberty; Justice Subba Rao's dissent offered a broader understanding of privacy. These cases form part of the historical background, but their reasoning must be read in light of the later nine-judge decision in *Puttaswamy*.[2]

In *Gobind v. State of Madhya Pradesh*, the Court accepted that privacy interests could be constitutionally protected, while recognising that the right was not absolute. The decision indicated that privacy claims require a careful assessment of the nature of the intrusion and the State interest relied upon. Later cases involving telephone tapping, bodily integrity, reproductive choice and personal autonomy further developed the constitutional vocabulary of privacy.[3]

The question was settled in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, where a Bench of nine judges held that privacy is a constitutionally protected right emerging primarily from the guarantee of life and personal liberty in Article 21 and from the other freedoms in Part III,

[1] INDIA CONST. arts. 14, 19, 21; *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, ¶¶ 323–28 (India).
[2] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300, 306 (India); *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295, 1299–1300 (India).
[3] *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148, 155 (India); *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301, 312 (India).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

that informational privacy is a facet of that right, and that an invasion of privacy must satisfy the requirements of legality, a legitimate State aim and proportionality.[4]

IV. Freedom of speech, press freedom and the right to know

Article 19(1)(a) guarantees citizens freedom of speech and expression. The guarantee protects more than the act of speaking. It includes the communication of ideas, opinions and information through different media and forms. The press is not separately named in the Constitution, but the Supreme Court has repeatedly treated press freedom as part of Article 19(1)(a). The freedom is central to democratic government because citizens must be able to debate public policy, criticise authorities and receive information about matters affecting collective life.[5]

Freedom of expression is not absolute. Article 19(2) permits reasonable restrictions on specified grounds, including the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, contempt of court, defamation and incitement to an offence. A restriction must fall within the constitutional text and satisfy the applicable standards of reasonableness. A general concern that information is inconvenient or embarrassing to an institution is not, by itself, a free-standing ground under Article 19(2).[6]

The right to know is closely related to meaningful political participation. Citizens cannot effectively evaluate public decisions if information about the exercise of public power is routinely withheld. The right is not an unrestricted entitlement to every record, but it supports a strong presumption in favour of transparency where disclosure concerns public functions, public expenditure or institutional accountability.[7]

The press also acts as an intermediary between records and public understanding. It selects, verifies, contextualises and communicates information that may otherwise remain inaccessible to the wider public. Press freedom therefore protects not only the publisher but also the public's interest in receiving information and participating in informed debate.[8]

V. The DPDP Act, 2023: structure and key concepts

The DPDP Act establishes a statutory framework for processing digital personal data in India. Its application depends on the definitions and conditions contained in the Act, including the

[4] *Puttaswamy*, *supra* note 1, ¶¶ 320, 325, 328 (plurality opinion of Chandrachud, J.).
[5] INDIA CONST. art. 19(1)(a); *Bennett Coleman & Co. v. Union of India*, (1972) 2 SCC 788, 797 (India); *Indian Express Newspapers (Bombay) Pvt. Ltd. v. Union of India*, (1985) 1 SCC 641, 664 (India).
[6] INDIA CONST. art. 19(2); *Shreya Singhal v. Union of India*, (2015) 5 SCC 1, 45 (India).
[7] *State of Uttar Pradesh v. Raj Narain*, (1975) 4 SCC 428, 453 (India); *S.P. Gupta v. Union of India*, 1981 Supp SCC 87, 232 (India).
[8] *Bennett Coleman*, *supra* note 5, at 797; *Indian Express Newspapers*, *supra* note 5, at 664.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

concepts of personal data, digital personal data, Data Principal, Data Fiduciary and processing. The Act applies to the processing of digital personal data within India where the data is collected in digital form, or collected in non-digital form and digitised subsequently. It also applies to certain processing outside India in connection with offering goods or services to Data Principals within India, subject to the statutory terms.[9]

The Act uses the concept of a Data Principal for the individual to whom personal data relates. A Data Fiduciary is the person who, alone or in conjunction with others, determines the purpose and means of processing. The distinction is important because obligations generally attach to the entity that controls the processing, while rights are conferred on the individual concerned. The Act also recognises a Data Processor, which processes personal data on behalf of a Data Fiduciary.[10]

The commencement position is especially important. By notification G.S.R. 843(E), dated 13 November 2025, the Central Government brought specified institutional and procedural provisions into force immediately, together with sub-sections (1) and (3) of section 44, the latter of which substitutes section 8(1)(j) of the RTI Act. Section 6(9) and section 27(1)(d) came into force one year later, on 13 November 2026, while the principal processing obligations and rights in sections 3 to 17 (other than section 6(9)), section 27 (other than clause (d) of sub-section (1)) and the other listed provisions are scheduled to commence eighteen months after publication, on 13 May 2027. The Digital Personal Data Protection Rules, 2025 follow a corresponding phased schedule: rules 1, 2 and 17 to 21 commenced on publication; rule 4 came into force one year later, on 13 November 2026; and rules 3, 5 to 16, 22 and 23 commence after eighteen months. Accordingly, the Act should not be described as fully operational on the date of this paper. Any analysis of enforceable duties must distinguish provisions already in force from provisions awaiting commencement.[11]

The statutory framework is built around lawful processing. Consent is a central basis, but it is not the only basis. Section 7 recognises certain legitimate uses for which personal data may be processed without consent, subject to its conditions. This matters for public administration and other specified activities, but it should not be assumed that every activity that an organisation

[9] Digital Personal Data Protection Act, No. 22 of 2023, §§ 2–3, INDIA CODE (2023).
[10] *Id.* § 2(i)–(k), (x) (defining 'Data Fiduciary,' 'Data Principal,' 'Data Processor' and 'processing').
[11] MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY, Notification G.S.R. 843(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Nov. 13, 2025); Digital Personal Data Protection Rules, 2025, r. 1(2)–(4), Notification G.S.R. 846(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Nov. 13, 2025).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

considers useful automatically qualifies as a legitimate use. The relevant statutory conditions must be met.[12]

VI. Consent, legitimate use and the practicality of journalistic processing

Consent is an important safeguard because it places the individual in a position to make an informed choice about processing. Section 6(1) requires consent to be free, specific, informed, unconditional and unambiguous, with a clear affirmative action. Notice should explain the relevant processing in accessible language. These requirements can reduce hidden or unexpected uses of personal data and improve accountability.[13]

However, consent is not always a workable foundation for journalism. A journalist investigating alleged corruption cannot ordinarily be expected to obtain consent from the subject before collecting and verifying documents. Advance notice may alert the subject, enable destruction of evidence or frustrate the investigation. Consent from a source may also be insufficient where the data concerns third parties. In other cases, the information may be held in public records or may have been disclosed by an institution without the consent of the person concerned.[14]

This does not mean that journalism should be exempt from all data protection principles. Journalists should still consider accuracy, relevance, data minimisation, secure storage, protection of sources and the consequences of disclosure.[15]

VII. Exemptions under section 17 and their limits

Section 17 of the DPDP Act contains exemptions from specified provisions in defined circumstances. Exemptions are important because a data protection statute must account for activities where ordinary compliance may be impracticable, disproportionate or inconsistent with another legal obligation. At the same time, exemptions should be interpreted carefully. An exemption that is too narrow may burden legitimate activity; an exemption that is too broad may remove meaningful protection for individuals.[16]

[12] Digital Personal Data Protection Act, No. 22 of 2023, §§ 4–7, India Code (2023).
[13] *Id.* §§ 5–6; Digital Personal Data Protection Rules, 2025, r. 3. Rule 3 is scheduled to commence on May 13, 2027, under the phased commencement provision in G.S.R. 846(E) (Nov. 13, 2025).
[14] Digital Personal Data Protection Act, No. 22 of 2023, §§ 3, 7, 17, India Code (2023). The Act does not create a general, express exemption framed specifically for journalism; the application of its scope, lawful-use provisions and exemptions must therefore be assessed on the statutory text.
[15] *Id.* § 8(1). The substantive obligations in § 8 are among the provisions scheduled to commence on May 13, 2027, under Notification G.S.R. 843(E) (Nov. 13, 2025).
[16] Digital Personal Data Protection Act, No. 22 of 2023, § 17, India Code (2023).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

The Act includes exemptions relating to specified State instrumentalities, legal claims and judicial or regulatory functions, certain offences and enforcement activities, research, archiving or statistical purposes subject to conditions, and other circumstances identified in the statutory text. It is particularly important not to describe the research exemption as an unrestricted licence to process personal data: statutory conditions and standards remain relevant.[17]

The absence of an express provision may create uncertainty about the treatment of editorial research, verification, publication, archiving and source management. It may also create different levels of risk for different actors.[18]

VIII. Section 44(3) and the Right to Information Act, 2005

Section 44(3) of the DPDP Act amends section 8(1)(j) of the RTI Act, which concerns personal information. The earlier text included a set of conditions and a public-interest balancing formulation. The substituted clause is shorter: it exempts 'information which relates to personal information'. This change has generated debate because the RTI Act is a major statutory instrument for transparency and accountability.[19]

The RTI Act was enacted to promote transparency in the working of public authorities. It recognises that access to information can expose maladministration, corruption, arbitrary decision-making and misuse of public resources. It also recognises that some information must remain protected. The Act therefore contains exemptions and mechanisms for considering public interest. The challenge is to apply those provisions in a way that protects legitimate confidentiality without turning exemptions into a routine barrier to scrutiny.[20]

The earlier section 8(1)(j) did not require disclosure of personal information unrelated to public activity or interest, or of information that would cause an unwarranted invasion of privacy, unless the larger public interest justified disclosure. The substituted text changes the wording of the personal-information exemption. Section 44(3) is among the provisions that G.S.R. 843(E) brought into force on 13 November 2025, so the substituted clause is already in operation. Its effect has to be read with the continued text of section 8(2), the other provisions of the RTI Act and the relevant judicial interpretation.[21]

---

[17] *Id.* § 17(1)–(2). The research, archiving and statistical-purpose exemption is conditional and is not a general exemption from all legal obligations.

[18] *See id.* § 17(1)–(2) (listing the exempted purposes, none of which is framed in terms of journalism).

[19] Digital Personal Data Protection Act, No. 22 of 2023, § 44(3), INDIA CODE (2023) (substituting § 8(1)(j) of the Right to Information Act, No. 22 of 2005).

[20] Right to Information Act, No. 22 of 2005, pmbl., §§ 3–4, 8, INDIA CODE (2005).

[21] *Id.* § 8(1)(j) (prior to substitution by the Digital Personal Data Protection Act, No. 22 of 2023, § 44(3)); MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY, Notification G.S.R. 843(E), *supra* note 11, cl. (a) (bringing § 44(1) and (3) into force on publication).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

Section 8(2) of the RTI Act provides a public-interest override in relation to the exemptions contained in the Act, subject to its wording. It permits access where the public interest in disclosure outweighs the harm to protected interests, notwithstanding the Official Secrets Act, 1923 or an exemption in section 8(1). Its continuing operation is therefore relevant to any interpretation of the amended personal-information exemption, although its precise application will depend on the statutory text and the facts of each request.[22]

IX. INVESTIGATIVE JOURNALISM: PUBLIC VALUE AND PRIVACY RISKS

Investigative journalism often concerns matters that powerful institutions would prefer not to disclose. It may involve tracing public expenditure, identifying undisclosed conflicts of interest, examining corporate relationships, testing claims made by public officials, or exposing failures in the delivery of public services. Such reporting can require the handling of personal information, but its social value depends on the relevance and reliability of the information rather than on the mere fact that it is personal.[23]

A journalist may receive a spreadsheet containing names, contact details and payment records. Some columns may be essential to identify irregularities; others may be irrelevant. The responsible approach is to preserve evidence securely, verify the data, identify the public-interest question, minimise unnecessary exposure and consider redaction before publication. Data protection principles can support this discipline rather than undermine it.[24]

A different situation arises where a story concerns a private individual whose personal data has no meaningful connection to a public issue. Publication of an address, phone number, medical diagnosis or intimate photograph may expose the person to harm without improving public understanding. Privacy law has an important role in preventing such disclosure.[25]

X. DIGITAL PLATFORMS, SOCIAL MEDIA AND CITIZEN EXPRESSION

The relationship between data protection and expression extends beyond traditional newspapers and broadcasters. Individuals increasingly publish information through social media, blogs, messaging services, video platforms and community forums. Citizen journalism can expose local issues that may not receive attention from established media. At the same time, online publication can spread personal information rapidly and make it difficult to reverse harm once content has been copied or redistributed.[26]

---

[22] Right to Information Act, No. 22 of 2005, § 8(2), INDIA CODE (2005).
[23] INDIA CONST. art. 19(1)(a); *Bennett Coleman*, *supra* note 5, at 797.
[24] Digital Personal Data Protection Act, No. 22 of 2023, § 8(1), INDIA CODE (2023).
[25] *Puttaswamy*, *supra* note 1, ¶¶ 323–28.
[26] INDIA CONST. art. 19(1)(a); *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637, 697 (India).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

A single post may include a person's photograph, workplace, location, contact details or allegations about private conduct. Some disclosures may be necessary to warn the public about fraud or immediate danger; others may amount to harassment, doxxing or targeted humiliation. The distinction requires attention to purpose, accuracy, context, proportionality and foreseeable harm.[27]

Data protection rules should not be interpreted in a way that makes ordinary democratic conversation impossible. The legal analysis should distinguish personal or domestic activity, public-interest communication and large-scale or systematic processing by organisations. It should also avoid assuming that every online post is journalism or that every disclosure is protected merely because it is described as expression.[28]

The balance is especially important for regional-language journalism and community reporting. Smaller publishers may lack legal teams and may rely on public records, local sources and community-generated information. Unclear rules can therefore have a disproportionate chilling effect on reporting about local administration, public services and grassroots concerns.

XI. ACADEMIC RESEARCH, ARCHIVING AND CIVIL SOCIETY

Academic researchers and civil society organisations often process personal data to study social conditions, evaluate public programmes, identify discrimination or document human rights concerns. Their work may involve interviews, surveys, administrative datasets, photographs, case records or public documents. The public value of research may depend on the ability to identify patterns across individuals, but publication of identifiable data can create risks for participants.[29]

Research ethics already recognises principles such as informed consent, confidentiality, data minimisation, secure storage and careful publication. Data protection law can reinforce these standards. However, research sometimes requires processing without obtaining fresh consent from every person, particularly when using historical records, large datasets or information necessary to study institutional practices. The statutory research exemption and its conditions therefore require careful attention.[30]

---

[27] INDIA CONST. arts. 19(1)(a), 21; *Puttaswamy*, *supra* note 1, ¶¶ 323–28.

[28] Digital Personal Data Protection Act, No. 22 of 2023, § 3(c), INDIA CODE (2023) (excluding from the Act personal data processed by an individual for any personal or domestic purpose, and certain personal data made publicly available).

[29] Digital Personal Data Protection Act, No. 22 of 2023, § 17(2)(b), INDIA CODE (2023); Universal Declaration of Human Rights arts. 12, 19, G.A. Res. 217A (III) (Dec. 10, 1948).

[30] Digital Personal Data Protection Act, No. 22 of 2023, § 17(2)(b), INDIA CODE (2023).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

An exemption for research should not be read as an unlimited permission to collect or publish personal information. The statutory conditions must be satisfied, and researchers should still consider whether identifiable data is necessary, whether access can be restricted and whether publication can use anonymised or aggregated results. Research value does not automatically justify public disclosure of every underlying record.[31]

Archiving presents a related issue. Historical records may contain personal information that remains relevant to public memory, accountability and scholarship. A proportionate framework should distinguish preservation for a legitimate archival purpose from unrestricted public dissemination, and should consider access controls, redaction and the historical significance of the material.

XII. Proportionality as a Method of Reconciling Competing Rights

Proportionality is a useful constitutional method for assessing restrictions on rights. It is not a substitute for statutory interpretation, nor does it automatically determine every dispute. It provides a disciplined framework for asking whether an interference pursues a legitimate objective, is rationally connected to that objective, is necessary in the circumstances and strikes a fair balance between the public benefit and the harm to rights.[32]

In privacy-related cases, the objective may be preventing unauthorised disclosure, protecting dignity, reducing discrimination or preventing misuse of sensitive data. In expression-related cases, the objective may be informing the public about corruption, enabling scrutiny of public institutions or communicating matters of public concern. A court or decision-maker should identify the actual objective rather than rely on abstract labels.[33]

The rational-connection stage asks whether the measure is capable of advancing the objective. For example, redacting a home address from a public report may protect privacy while leaving the central findings intact. By contrast, suppressing an entire report because it contains one personal identifier may be broader than necessary. The example illustrates why less intrusive alternatives matter.[34]

Necessity requires consideration of whether a less restrictive measure could achieve the legitimate objective with comparable effectiveness. Possible measures include anonymisation, pseudonymisation, partial disclosure, delayed publication, aggregation, limiting access to

[31] *Id.* § 17(2)(b).
[32] *Modern Dental College & Research Centre v. State of Madhya Pradesh*, (2016) 7 SCC 353, 411–15 (India); *Puttaswamy*, *supra* note 1, ¶ 325.
[33] *Puttaswamy*, *supra* note 1, ¶ 325.
[34] *Modern Dental College*, *supra* note 32, at 411–15.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

sensitive annexures or publishing a summary that preserves the relevant public-interest information. The appropriate option depends on the case; redaction is not always sufficient if identity is essential to understanding the wrongdoing.[35]

XIII. Comparative analysis: the European Union GDPR

The European Union's General Data Protection Regulation is a useful comparative reference because it expressly recognises the need to reconcile data protection with freedom of expression and information. Article 85 requires Member States to provide exemptions or derogations where necessary to reconcile the right to personal data protection with freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.[36]

The GDPR does not create a single uniform journalistic exemption with identical wording across every Member State. Instead, it requires national law to establish the necessary reconciliation. This allows differences in national constitutional traditions and media systems while ensuring that the conflict is addressed expressly. The provision demonstrates that data protection and expression can be placed within the same legislative framework without treating either as irrelevant.[37]

The comparative lesson for India is not that every GDPR provision should be transplanted. India's constitutional structure, statutory history, media environment, institutional capacity and social conditions differ. The GDPR is also embedded in a broader European human-rights framework. A direct copy may therefore create uncertainty or inappropriate results.

XIV. International human rights standards

International human rights instruments recognise both privacy and freedom of expression. Article 12 of the Universal Declaration of Human Rights protects against arbitrary interference with privacy, family, home or correspondence and attacks upon honour and reputation. Article 19 protects the freedom to hold opinions and to seek, receive and impart information and ideas through any media. The two provisions reflect the same basic insight: individuals require both personal security and communicative freedom.[38]

The International Covenant on Civil and Political Rights contains corresponding protections in Articles 17 and 19. Article 17 addresses unlawful or arbitrary interference with privacy, family,

[35] *Id.* at 411–15.
[36] Regulation (EU) 2016/679, art. 85, 2016 O.J. (L 119) 1.
[37] *Id.* art. 85(2)–(3).
[38] Universal Declaration of Human Rights, *supra* note 29, arts. 12, 19.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

home or correspondence and unlawful attacks on honour and reputation. Article 19 protects expression while permitting restrictions only where provided by law and necessary for specified legitimate purposes. These provisions are relevant to India's international commitments and to comparative interpretation, while domestic constitutional questions must ultimately be resolved under Indian law.[39]

XV. Regulatory design, enforcement and procedural safeguards

The effectiveness of a data protection statute depends not only on its substantive rules but also on the quality of its enforcement institutions. The Data Protection Board of India has statutory responsibilities under the Act. Its procedures, independence, expertise, transparency and ability to provide reasoned decisions will influence public confidence in the framework.[40]

Where a complaint concerns publication of information, the Board or another competent authority should be attentive to the distinction between data processing and the content of expression. A data protection complaint should not become an indirect route for deciding the truth of a news report or suppressing criticism of public officials. Questions of privacy, defamation, contempt and other legal issues may overlap, but each has its own legal elements and procedures.[41]

Procedural safeguards should include notice of the case to the affected party, an opportunity to respond, disclosure of the material relied upon where legally permissible, reasoned findings, proportionate remedies and access to judicial review. Emergency action may be necessary in exceptional cases involving imminent and serious harm, but it should be narrowly tailored and subject to prompt review.[42]

Transparency reporting can improve accountability. Publication of aggregate information about complaints, directions, response times and remedies can help the public assess whether enforcement is consistent and proportionate, provided that such reporting does not itself disclose protected personal information or compromise pending proceedings.

XVI. Practical scenarios

Scenario one concerns a report alleging that a public authority awarded contracts to entities connected with a senior official. The underlying records contain names, company relationships

[39] International Covenant on Civil and Political Rights arts. 17, 19, Dec. 16, 1966, 999 U.N.T.S. 171; U.N. Human Rights Comm., General Comment No. 34, ¶¶ 21–36, U.N. Doc. CCPR/C/GC/34 (Sept. 12, 2011); U.N. Human Rights Comm., General Comment No. 16, ¶ 3, U.N. Doc. HRI/GEN/1/Rev.9 (Vol. I) (1988).
[40] Digital Personal Data Protection Act, No. 22 of 2023, §§ 18–26, India Code (2023); Ministry of Electronics & Information Technology, Notification G.S.R. 843(E), *supra* note 11.
[41] Digital Personal Data Protection Act, No. 22 of 2023, §§ 18–27, India Code (2023).
[42] *Id.* §§ 28–30; India Const. art. 226.

and payment details. The public interest in examining procurement integrity is substantial. The reporter should verify the records, identify the connection to official decision-making and avoid publishing unrelated personal details. Redaction may be appropriate for home addresses, personal phone numbers or family information that does not advance the story. The public-interest value of the contract relationship may justify publication of relevant facts, subject to applicable law.[43]

Scenario two concerns the publication of a private person's medical records to make a story more sensational. If the medical information is unrelated to a matter of public concern, publication is difficult to justify. The person's vulnerability and the sensitivity of the information weigh strongly in favour of privacy. Even where the person is involved in a public controversy, the publisher should explain why the specific medical details are necessary. A general claim of public curiosity is not equivalent to public interest.[44]

Scenario three concerns a researcher examining whether a public welfare scheme is reaching eligible beneficiaries. The dataset contains names, addresses, identity numbers and payment information. The research may be valuable, but publication of identifiable records may expose beneficiaries to fraud or stigma. The researcher should use aggregation, pseudonymisation or secure access where possible.[45]

Scenario four concerns a public archive containing historic records of a public programme. A researcher seeks access to understand how eligibility decisions were made over time. The archive's public and historical value should be weighed against the risk of exposing living individuals to avoidable harm. Where names are not necessary to establish the historical pattern, controlled access, redaction or aggregate publication may preserve the research value while reducing privacy risks.

XVII. Challenges in implementation

A first challenge is legal certainty. Individuals and organisations need to know which provisions apply, when they commence and how exemptions operate. Phased commencement can make the framework more complex because different provisions may become operative at different times. Guidance should clearly identify the commencement status of each relevant obligation and should be updated when notifications or amendments are issued.[46]

[43] Right to Information Act, No. 22 of 2005, §§ 8(2), 10, India Code (2005).
[44] *Puttaswamy*, *supra* note 1, ¶¶ 323–28.
[45] Digital Personal Data Protection Act, No. 22 of 2023, § 17(2)(b), India Code (2023).
[46] Ministry of Electronics & Information Technology, Notification G.S.R. 843(E), *supra* note 11; Digital Personal Data Protection Rules, 2025, r. 1(2)–(4), *supra* note 11.

A second challenge is institutional capacity. Public authorities, small businesses, media organisations, schools, hospitals and non-profit entities may have different levels of technical and legal expertise. A uniform compliance expectation without accessible guidance may produce uneven results. Capacity-building, model notices, security guidance and sector-specific examples can improve compliance.

A third challenge concerns the quality of consent. Digital users often face lengthy notices and complex interfaces. Consent may become formal rather than meaningful if individuals cannot understand the purposes of processing or exercise real choice. The law's effectiveness depends on plain-language notices, accessible grievance mechanisms and practical control over data.

A fourth challenge is cross-border processing. Digital services often rely on global infrastructure, cloud providers and international transfers. The statutory framework must be applied in a way that protects individuals while giving organisations predictable rules. Restrictions or conditions concerning transfers should be clear, transparent and consistent with the Act.

A fifth challenge is the risk of over-removal. A request to erase personal data may be legitimate in some contexts, but it may also intersect with legal retention duties, public records, archives or the preservation of evidence.[47]

XVIII. THE DISTINCTION BETWEEN PRIVACY, SECRECY AND CONFIDENTIALITY

Privacy, secrecy and confidentiality are related but distinct concepts. Privacy concerns the individual's interest in controlling access to aspects of personal life and information. Secrecy generally refers to keeping information unknown or undisclosed. Confidentiality is a duty or expectation governing how information received in a particular relationship should be handled. A person may have a privacy interest in information even if the information is not secret, and a public authority may owe confidentiality in respect of information that is not inherently intimate. These distinctions matter because data protection law should not transform every fact about an identifiable person into information that can never be disclosed.[48]

For example, the name of a public official who signed an official order is not necessarily private in the same way as the official's medical history. The name may be part of an official record and may be necessary to understand responsibility for a decision. By contrast, the official's

[47] Digital Personal Data Protection Act, No. 22 of 2023, § 12(3), INDIA CODE (2023) (requiring erasure on request 'unless retention of the same is necessary for the specified purpose or for compliance with any law for the time being in force').

[48] *Puttaswamy*, *supra* note 1, ¶¶ 323–28; Universal Declaration of Human Rights, *supra* note 29, art. 12.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

personal health information may have no legitimate connection with the decision. A legal test that treats both categories identically would ignore context and could undermine accountability.

XIX. Public figures, public officials and private individuals

The expectation of privacy may vary with context, but public status does not eliminate privacy. Public officials exercise authority on behalf of the community and may properly face greater scrutiny concerning the performance of official functions. Their decisions, conflicts of interest, use of public resources and compliance with legal duties are matters of legitimate public concern. Yet public officials remain entitled to privacy in relation to intimate, medical, family and other unrelated aspects of life.[49]

Public figures who voluntarily participate in public debate may also attract scrutiny, but the extent of legitimate scrutiny depends on the connection between the information and the public role or controversy. A celebrity's public profile does not make every private communication newsworthy. A business leader's control over a major public-facing enterprise may justify scrutiny of corporate conduct, but it does not automatically justify disclosure of family details. Private individuals generally have a stronger claim to protection, especially where they are vulnerable, are children, or have not voluntarily entered public life.

A contextual approach prevents two errors. The first is to assume that public status removes all privacy. The second is to treat every personal detail concerning a public figure as inherently newsworthy. The relevant question is whether the information bears a genuine and proportionate connection to the person's public role, the issue under discussion or the exercise of public power.

XX. Data minimisation and editorial responsibility

Data minimisation is commonly understood as limiting personal data to what is necessary for the purpose for which it is processed. In journalism, the principle can be translated into an editorial question: what is the minimum amount of personal information required to communicate and substantiate the public-interest finding? The answer may differ between investigation and publication. A reporter may need to examine a full document to verify a transaction, while the published story may need only the relevant amount, date and institutional relationship.[50]

---

[49] *Central Public Information Officer, Supreme Court of India v. Subhash Chandra Agarwal*, (2020) 5 SCC 481, 526 (India).

[50] Regulation (EU) 2016/679, *supra* note 36, art. 5(1)(c); Digital Personal Data Protection Act, No. 22 of 2023, § 8(1)(a), INDIA CODE (2023).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

The distinction between internal access and public dissemination is important. A newsroom may have a legitimate reason to retain source documents securely, but that does not mean the entire document should be placed online. Publishing a searchable database of personal identifiers can create risks beyond those necessary to explain the story. A carefully designed publication may present the evidence, explain the methodology and redact details that would expose individuals without advancing the public interest.[51]

Editorial responsibility also requires accuracy. Incorrect personal information can cause severe harm, particularly where it concerns alleged criminal conduct, financial misconduct or professional wrongdoing.

XXI. Remedies, erasure and the public record

The right to erasure is important where personal data is no longer necessary for the purpose for which it was processed, where consent is withdrawn in circumstances covered by law, or where another statutory ground applies. However, erasure requests may intersect with journalism, legal proceedings, public archives, historical records and duties to preserve evidence. The correct result depends on the applicable provision and its exceptions; it should not be assumed that every online reference must be removed upon request.[52]

A distinction should be drawn between correcting inaccurate information, removing unlawfully processed data, limiting access to sensitive details and erasing a record that has continuing public or legal value. A person may have a legitimate claim to correct a false statement or remove an unnecessary identifier without having an automatic right to erase a verified report about a matter of public importance. The permanence of digital publication nonetheless creates a genuine privacy concern: search engines and platforms can make old information easily discoverable long after the public relevance of a story has diminished.

XXII. The role of courts in future constitutional adjudication

Courts are likely to play an important role in clarifying the relationship between the DPDP framework, freedom of expression and the RTI regime. Judicial review may be required where a statutory provision is challenged, where an administrative decision restricts publication, or where a public authority refuses access to information. Courts should distinguish facial challenges to legislation from challenges to particular applications of the law.[53]

---

[51] Regulation (EU) 2016/679, *supra* note 36, art. 5(1)(c).

[52] Digital Personal Data Protection Act, No. 22 of 2023, § 12, India Code (2023). Section 12 is scheduled to commence on May 13, 2027, under Notification G.S.R. 843(E) (Nov. 13, 2025).

[53] *Puttaswamy*, *supra* note 1; *Subhash Chandra Agarwal*, *supra* note 49.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

In reviewing a specific decision, a court should identify the legal basis for the restriction, the nature of the data, the public interest asserted and the reasons given by the authority. It should consider whether the authority examined less restrictive alternatives and whether the remedy is proportionate. A decision that simply repeats the phrase 'personal information' without analysing the context may fail to demonstrate proper application of the statutory framework.[54]

Courts should also be careful not to decide broad constitutional questions unnecessarily where a dispute can be resolved through statutory interpretation. At the same time, where a provision is genuinely ambiguous and has significant implications for expression, constitutional values should inform interpretation.

Judicial remedies should be tailored. Where possible, courts should prefer measures such as redaction, limited disclosure, correction or a narrowly framed direction over a blanket prohibition on publication. The remedy should address the demonstrated harm without unnecessarily suppressing information that serves a legitimate public purpose.

XXIII. Policy model for a journalistic and public-interest safeguard

A legislative safeguard could be designed around a defined purpose rather than an occupational label. It may cover processing necessary for publication, broadcast, communication or research directed to informing the public about a matter of public interest. The safeguard could apply to professional journalists, independent publishers, researchers and civil society actors where their activity genuinely performs that function. It should not automatically apply to every commercial use of personal data by a media company.[55]

The provision should identify which obligations may be modified and which core safeguards remain. For example, some consent or notice requirements may need flexibility where prior contact would defeat an investigation. Security, accuracy, data minimisation, purpose limitation and accountability principles may remain relevant, adapted to the circumstances. The law should make clear that an exemption from one obligation does not create immunity from all other applicable laws.

The safeguard could require a reasonable public-interest assessment. Relevant considerations may include the seriousness of the issue, the person's role, the relevance of the data, the degree

[54] *Modern Dental College*, *supra* note 32, at 411–15.
[55] Regulation (EU) 2016/679, *supra* note 36, art. 85; Digital Personal Data Protection Act, No. 22 of 2023, § 17, INDIA CODE (2023).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

of intrusion, the reliability of the source, the risk of harm and the availability of less intrusive means.

XXIV. FINDINGS OF THE STUDY

The first finding is that privacy is a fundamental constitutional right in India and includes informational privacy. The DPDP Act therefore responds to a legitimate constitutional need. Protection against unauthorised or unfair processing can strengthen dignity, autonomy and trust in digital services.[56]

The second finding is that freedom of speech and expression is also constitutionally protected and includes the importance of press freedom and the public's ability to receive information. Investigative journalism and access to public records support democratic accountability.[57]

The third finding is that the two rights cannot be reconciled through a simple rule that privacy always prevails or expression always prevails. The nature of the information, the purpose of processing, the public significance of the issue and the risk of harm must be considered.

The fourth finding is that the Act's general framework and exemptions require careful application to journalistic, academic and civil society activity. The absence of an express general journalistic reconciliation provision may create uncertainty, even though the applicability of existing provisions must be examined case by case.

The fifth finding is that phased commencement is legally significant. As at November 2026, the Act's principal processing duties and most individual rights are not yet in force; they are scheduled to commence on 13 May 2027. Analysis must therefore distinguish the enacted framework from obligations that have not yet commenced.[58]

The sixth finding is that procedural safeguards are as important as substantive rights. Clear reasons, access to review, transparency and proportionate remedies can reduce the risk that data protection mechanisms are used to suppress legitimate criticism or public-interest reporting.

XXV. SUGGESTIONS AND RECOMMENDATIONS

First, Parliament should consider introducing a carefully drafted provision addressing processing for journalistic, academic, artistic and public-interest expression. Such a provision should identify the obligations from which a limited derogation may be necessary and should

[56] *Puttaswamy*, *supra* note 1, ¶¶ 323–28.
[57] INDIA CONST. art. 19(1)(a); *Bennett Coleman*, *supra* note 5, at 797.
[58] MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY, Notification G.S.R. 843(E), *supra* note 11, cls. (b)–(c).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

specify safeguards. It should not create a blanket immunity for all persons claiming to be journalists.[59]

Second, any journalistic safeguard should be purpose-based. It should cover activities genuinely undertaken to inform the public on matters of public concern, rather than merely activities carried out by an organisation with a media label. This would allow responsible citizen journalism and civil society investigations to be considered while preventing misuse of the exemption.

Third, the safeguard should require a reasonable connection between the personal data processed and the public-interest purpose. The publisher should consider whether the information is accurate, whether the person concerned is vulnerable, whether the details are sensitive, whether the public interest can be served by redaction and whether publication is likely to cause disproportionate harm.

Fourth, the government and the relevant regulator should publish clear guidance on the application of the Act to newsrooms, independent journalists, academic institutions, researchers, archives and civil society organisations. Guidance should include practical examples and should be developed through consultation with stakeholders.

Fifth, public information officers should apply the RTI Act as a whole. Decisions involving personal information should address the precise statutory exemption, the relevance of section 8(2), the possibility of severing exempt portions and the public interest in disclosure.

XXVI. CONCLUSION

The Digital Personal Data Protection Act, 2023 is an important step in the development of India's legal response to the risks of digital personal data processing. In an environment where personal information is continuously generated, combined and used, legal safeguards are necessary to protect dignity, autonomy and individual security. The constitutional recognition of privacy in *Puttaswamy* provides a strong foundation for this legislative project.

However, privacy does not exist in isolation. Freedom of speech and expression under Article 19(1)(a), press freedom and access to information are essential to democratic governance. Journalists, researchers, civil society organisations and citizens may need to process or disclose personal information to expose corruption, scrutinise public institutions and inform public debate. A framework that fails to account for these activities may create uncertainty or encourage excessive self-censorship.

[59] Regulation (EU) 2016/679, *supra* note 36, art. 85.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

The amendment to section 8(1)(j) of the RTI Act through section 44(3) raises particular concerns because it affects the statutory balance between personal information and transparency. The continued relevance of section 8(2) and the wider RTI scheme must be considered when interpreting the amendment. The legal position should be stated with precision and should develop through reasoned decisions rather than assumptions that either privacy or transparency has been completely displaced.

The comparative experience of the GDPR shows that data protection legislation can expressly recognise freedom of expression and information, and a proportionality-based approach offers a principled method for resolving difficult cases.

*****

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]