International Journal of Humanities and Social Science
ISSN (Online): 2208-2174
Volume 11 Issue 01 January 2026
DOI: https://doi.org/10.53555/qc80v285

THE TRANSPARENCY - PRIVACY PARADOX IN INDIA: A STUDY OF THE CONFLICT BETWEEN RTI AND DATA PROTECTION LAW

Shreya Gautam[1*], Aman Kumar[2]

[1](Asst. Prof - RMLNLU)*
[2](Research Scholar - RMLNLU)

ABSTRACT
The increasing digitisation of governance has intensified the interaction between transparency and data protection, raising complex questions for constitutional democracies. In India, this tension is most visibly manifested in the interface between the Right to Information Act, 2005 and the Digital Personal Data Protection Act, 2023. While both statutes possess independent normative legitimacy, their coexistence has generated institutional and doctrinal uncertainty, particularly following the amendment to Section 8(1)(j) of the RTI Act.

This paper examines how statutory design can reshape the practical operation of constitutional rights without formally reordering their hierarchy. Drawing on doctrinal analysis, statutory interpretation, and comparative experience from the United Kingdom, the European Union, and Mexico, the study demonstrates that the DPDP Act reconfigures transparency obligations by displacing the RTI Act's contextual balancing framework through indirect legislative mechanisms. The paper argues that this shift does not reflect an explicit prioritisation of privacy over transparency, but rather a transformation of institutional incentives that favours categorical exclusion over proportional evaluation.

Conceptually, the study advances the idea of information constitutionalism by showing how constitutional values are mediated through legislative architecture and administrative practice. It concludes that the sustainability of democratic accountability in a digital state depends less on abstract rights recognition than on institutionalised mechanisms capable of holding transparency and privacy in principled tension.

KEYWORDS: *Right to Information; Data Protection Law; Transparency and Privacy; Digital Governance; Information Constitutionalism.*

INTRODUCTION

The Right to Information Act, 2005 (RTI Act) has long been regarded as one of India's most transformative democratic enactments, reshaping the relationship between citizens and the State by institutionalising transparency as a constitutional value. Rooted in Article 19(1)(a) of the Constitution, the RTI regime reframed access to information not as administrative benevolence but as a legal entitlement central to democratic accountability. Over time, it enabled citizens, journalists, and civil society actors to scrutinise public decision-making, expose corruption, and demand reasoned governance, thereby embedding openness within the everyday functioning of the administrative state.[1]

Parallel to this trajectory, India's constitutional discourse underwent a significant recalibration with the recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v. Union of India.*[2] Anchored in Article 21, the right to privacy particularly informational privacy responded to the realities of digital governance, data aggregation, and algorithmic decision-making. The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) represents the legislative culmination of this shift, signalling the State's attempt to regulate personal data processing through consent, purpose limitation, and accountability of data fiduciaries.

The coexistence of these two statutory regimes has generated a profound constitutional tension. As governance processes become increasingly datafied, requests under the RTI Act now routinely intersect with personal data held by public authorities. Information that once existed in discrete paper files is today embedded within integrated databases containing extensive personal and sensitive data, often collected without meaningful consent. Public authorities are consequently placed in a position of normative conflict: whether to disclose information in furtherance of democratic accountability, or to withhold it in deference to data protection obligations. This tension has been amplified by the amendment to Section 8(1)(j) of the RTI Act introduced through the DPDP Act, which alters the legal architecture governing disclosure of personal information.

This dissonance is not merely administrative; it is constitutional in nature. The RTI Act embodies the principle that an informed citizenry is a prerequisite for democratic participation and accountable governance, while the DPDP Act operationalises the constitutional recognition of privacy as intrinsic to dignity and personal autonomy. When these rights intersect in the digital domain, neither can be treated as absolute. The challenge, therefore, lies not in privileging one right over the other, but in designing legal principles and institutional mechanisms capable of reconciling transparency and privacy without diminishing either.

Despite the significance of this intersection, scholarly engagement with the RTI–privacy conflict remains fragmented. Studies on the RTI Act have predominantly focused on implementation challenges, corruption control, and administrative compliance, while privacy scholarship has evolved largely in isolation, anchored in surveillance, data sovereignty, and technology regulation. Very few works examine how these two regimes interact as part of a unified constitutional information order, particularly in a context where the State simultaneously functions as data collector, data fiduciary, and transparency regulator. As a result, the debate is often framed as a zero-sum contest between disclosure and protection, rather than as a problem of constitutional design and institutional reconciliation.

Existing approaches have also struggled to account for the practical consequences of this unresolved tension. Judicial interpretations of Section 8(1)(j) of the RTI Act, which previously exempted personal information from disclosure subject to a larger public interest test, have been inconsistent. Administrative practice, especially following the enactment of the DPDP Act, has increasingly defaulted to non-disclosure, shaped by regulatory uncertainty and the fear of statutory penalties. The cumulative effect is a creeping privatisation of public data, where public authorities err on the side of opacity, undermining democratic accountability and eroding public trust in institutions.

This paper intervenes in that gap. It departs from implementation-centric RTI analyses and privacy- centric data protection narratives by conceptualising transparency and privacy as co-constitutive constitutional guarantees that together constrain arbitrary state power in an information society. Drawing on constitutional doctrine, judicial interpretation, and comparative institutional models, the study frames the RTI–DPDP interface as a question of information constitutionalism that is, how constitutional principles governing rights, proportionality, and accountability should structure the State's control over information in a digital democracy.

The paper advances three central claims. First, it demonstrates that Indian constitutional jurisprudence, particularly post-Puttaswamy, has consistently favoured contextual balancing through proportionality rather than categorical prioritisation of either transparency or privacy. Second, it argues that the 2023 amendment to the RTI Act risks displacing this judicially evolved equilibrium by transforming a qualified public-interest test into a near-absolute exemption, thereby enabling administrative opacity under the guise of data protection. Third, through comparative analysis of jurisdictions such as the United Kingdom, the European Union, and Mexico, the paper shows that sustainable reconciliation of informational rights depends on institutionalised balancing mechanisms rather than statutory silos.

Methodologically, the study adopts a qualitative doctrinal and comparative approach, combining constitutional analysis with insights on institutional design. Normatively, it proposes a model of principled reconciliation in which transparency and privacy operate as complementary safeguards of democratic accountability and individual dignity. By reframing the RTI–DPDP conflict as a structural constitutional problem rather than a statutory anomaly, the paper contributes to emerging scholarship on digital constitutionalism and democratic governance, and seeks to inform judicial interpretation, legislative refinement, and institutional coordination at a critical juncture in India's information regime.

1. RESEARCH METHODOLOGY

This study adopts a qualitative doctrinal and comparative legal research methodology, supplemented by normative constitutional analysis, to examine the evolving interface between transparency and privacy in India's digital governance framework.

1.1 Doctrinal Legal Analysis

The core of the research is doctrinal, focusing on constitutional provisions, statutory texts, and judicial interpretation. Primary sources include the Right to Information Act, 2005, the Digital Personal Data Protection Act, 2023, and leading constitutional judgments of the Supreme Court of India. Judicial decisions were selected based on their precedential significance, engagement with informational rights, and explicit balancing of transparency and privacy, particularly in the context of Articles 19(1)(a) and 21 of the Constitution.

Key cases such as State of U.P. v. Raj Narain, Justice K.S. Puttaswamy (Retd.) v. Union of India, and CPIO, Supreme Court of India v. Subhash Chandra Agarwal were analysed to trace the jurisprudential evolution of the right to know and the right to privacy, and to identify the constitutional standards especially proportionality used to reconcile competing rights. The doctrinal analysis also examines statutory exemptions under Section 8 of the RTI Act and the implications of the amendment introduced by Section 44(3) of the DPDP Act.

1.2 Normative Constitutional Analysis

Beyond doctrinal exposition, the study employs normative constitutional reasoning to evaluate whether the current statutory framework aligns with India's constitutional commitment to democratic accountability and individual dignity. Privacy and transparency are treated not as isolated statutory entitlements but as co-constitutive constitutional values that structure the relationship between the citizen and the State in an information society.

The research draws on the proportionality doctrine articulated in Puttaswamy, using it as an evaluative lens to assess whether legislative and administrative practices strike a constitutionally justifiable balance between disclosure and data protection. This normative approach enables the paper to interrogate not only what the law is, but whether it coheres with constitutional principles governing limitation of fundamental rights.

1.3 Comparative Functional Analysis

To contextualise India's evolving framework, the study undertakes a comparative functional analysis of selected jurisdictions namely the United Kingdom, the European Union, and Mexico. These jurisdictions were chosen because each operates parallel regimes of freedom of information and data protection, and has developed institutional or doctrinal mechanisms to manage conflicts between the two.

The comparative inquiry focuses on:

- The presence and operation of public interest overrides;
- The role of proportionality or balancing tests in disclosure decisions involving personal data; and
- Institutional design, particularly whether oversight bodies for access to information and data protection operate in coordination or isolation.

Rather than transplanting foreign models, the comparative analysis is used to identify structural principles and institutional design choices that may inform a constitutionally compatible reconciliation of transparency and privacy within the Indian context.

1.4 Scope and Limitations

The study is primarily theoretical and doctrinal in nature. It does not undertake empirical fieldwork or quantitative analysis of RTI outcomes post-2023, owing to the nascent stage of DPDP implementation and limited publicly available data. However, the absence of empirical measurement does not undermine the study's contribution, as its objective is to evaluate constitutional coherence, institutional design, and normative consistency rather than administrative efficiency.

The paper recognises that judicial interpretation of the DPDP Act is still developing. Accordingly, the analysis is framed as an early constitutional assessment, intended to guide future adjudication, legislative refinement, and empirical inquiry.

2. DOCTRINAL COLLISIONS IN INDIAN JURISPRUDENCE: JUDICIAL BALANCING OF PRIVACY AND TRANSPARENCY

The Indian judiciary has played a foundational role in shaping both the right to know and the right to privacy, long before their formal statutory articulation. As governance has increasingly shifted to digital and data-driven modes, courts have been required to confront a growing overlap between public information and personal data. The resulting jurisprudence reflects a gradual though not linear movement from transparency as the default position toward heightened concern for privacy, necessitating judicial balancing of competing constitutional imperatives.

2.1 Early Judicial Foundations: The Right to Know as a Democratic Instrument

The right to information in India emerged through constitutional interpretation well before the enactment of the Right to Information Act, 2005. In *State of U.P. v. Raj Narain*, the Supreme Court famously affirmed that "the people of this country have a right to know every public act, everything that is done in a public way," anchoring the right to know within Article 19(1)(a) of the Constitution and positioning it as integral to democratic accountability.[3]

This principle was further developed in *S.P. Gupta v. Union of India*, where the Court rejected claims of blanket privilege over state-held information and declared that "open government is the new democratic culture of an open society."[4] Subsequent decisions, including *Secretary, Ministry of Information & Broadcasting v. Cricket Association of Bengal and People's Union for Civil Liberties v. Union of India*, expanded the doctrine by linking the free flow of information to meaningful participation in democratic governance. These early rulings conceived transparency not merely as a procedural entitlement but as a substantive constitutional value underpinning equality, liberty, and accountable administration.

The enactment of the RTI Act institutionalised this jurisprudence, reversing traditional information hierarchies by requiring the State to justify non-disclosure rather than compelling citizens to justify their demand for information. In practice, the RTI regime functioned as a democratic audit mechanism, facilitating public scrutiny of governance failures and maladministration. At a deeper level, the right to information resonates with what Amartya Sen describes as the "capability dimension" of freedom, access to information being both instrumental to participation and constitutive of substantive citizenship. However, the digitalisation of governance fundamentally altered this equilibrium. As data replaced documents and algorithmic systems replaced file-based administration, the informational power of the State expanded exponentially, intensifying the interface between transparency and privacy.

2.2 Judicial Recognition of Privacy: From Margins to Constitutional Core

For much of India's constitutional history, privacy occupied an uncertain position. In *Kharak Singh v. State of U.P.*, the Court remained divided on whether privacy enjoyed constitutional protection under Article 21.[5] This ambiguity persisted until the nine-judge bench decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, which unanimously recognised privacy as a fundamental right intrinsic to dignity and personal liberty.[6]

The Puttaswamy judgment articulated privacy as a multi-dimensional right encompassing spatial control, decisional autonomy, and informational self-determination. Of particular relevance is informational privacy, the individual's ability to control the collection, use, and dissemination of personal data, which the Court identified as central to autonomy in the digital age. The judgment further established that privacy operates not as a privilege against the State but as a structural limitation on state power, especially where large-scale data collection and processing are involved.

In recognising privacy, the Court articulated a four-pronged test - legality, legitimate aim, proportionality, and procedural safeguards, for assessing any infringement of the right. Drawing upon comparative constitutional jurisprudence, the Court embedded proportionality as the governing standard for evaluating state action affecting informational rights. This doctrinal framework laid the constitutional foundation for subsequent data protection legislation.

2.3 The RTI–Privacy Interface: Section 8(1)(j) and Judicial Interpretation

Prior to the enactment of the DPDP Act, Section 8(1)(j) of the RTI Act functioned as the statutory fulcrum for balancing transparency and privacy. The provision exempted disclosure of personal information unrelated to public activity or interest, or information that would cause an unwarranted invasion of privacy, unless disclosure was justified by a larger public interest. This public interest override enabled contextual adjudication by courts and information commissions.

In *Girish Ramchandra Deshpande v. Central Information Commission*, the Supreme Court held that personal details contained in a public servant's service records and asset declarations constituted private information, subject to disclosure only upon demonstration of overriding public interest.[7] Similarly, in *R.K. Jain v. Union of India*, the Court denied access to confidential service records while acknowledging that transparency and privacy must be weighed against each other on a case- by-case basis.[8] These decisions reflect a cautious judicial pragmatism, one that protected individual privacy without extinguishing the citizen's right to accountability.

This jurisprudence demonstrates that the RTI regime was never premised on absolute openness. Rather, it institutionalised a structured balancing mechanism that allowed adjudicators to mediate conflicts between disclosure and privacy through public interest assessment.

2.4 Constitutional Limits on Privacy as an Instrument of State Opacity

Post-Puttaswamy jurisprudence reveals an emerging constitutional dilemma. A right originally conceived as a safeguard against arbitrary state intrusion increasingly risks being invoked by the State itself to resist public scrutiny. This tension became particularly visible in *Central Public Information Officer, Supreme Court of India v. Subhash Chandra Agarwal*, where the Court addressed whether judges' asset declarations and correspondence with the Chief Justice of India could be disclosed under the RTI Act.[9]

The Court held that neither the right to information nor the right to privacy is absolute and that both must be harmonised through a proportionality-based analysis. While permitting limited disclosure, it cautioned against "intrusive fishing enquiries" into personal domains. The decision constitutionalised proportionality within RTI adjudication, reinforcing

that privacy claims must be evaluated contextually rather than treated as categorical exclusions.[10]

Read together, Puttaswamy and Subhash Chandra Agarwal establish a clear doctrinal position: privacy cannot operate as an absolute exclusionary claim, particularly when invoked by the State. Informational privacy functions as a limitation on state power, not as a mechanism for insulating public authorities from accountability. Where personal data is embedded within public decision- making processes, disclosure cannot be foreclosed automatically; it must be assessed through a structured inquiry into legitimacy, necessity, and proportionality. Any statutory or administrative framework that removes this evaluative space risks departing from constitutional doctrine by converting a contextual right into an effective veto over transparency.

Recent judicial developments further underscore this tension. In *Shailesh Gandhi v. Union of India (pending)*, the Bombay High Court was called upon to examine the constitutional validity of the amendment to Section 8(1)(j) of the RTI Act introduced through the DPDP Act. The Court's interim observations, acknowledging the need to reconcile statutory privacy with constitutional openness, signal an emerging judicial unease with absolutist approaches to data protection.[11]

The doctrinal position that emerges from Indian constitutional jurisprudence is thus neither a hierarchy nor a binary opposition between transparency and privacy. Instead, it reflects a commitment to contextual balancing grounded in proportionality, recognising both rights as essential components of democratic governance. Privacy may protect individual dignity, but it cannot be deployed as a structural shield to obscure public accountability.

This doctrinal concern is not merely theoretical. Institutional reporting indicates that public authorities and information commissions have increasingly relied on personal-information exemptions under the RTI framework, contributing to a more restrictive disclosure environment.[12] The Central Information Commission's recent annual reports note a sustained rise in appeals and complaints involving exemption claims, while independent monitoring has observed that uncertainty following the DPDP-linked amendment to Section 8(1)(j) has encouraged administrative over-caution and a default preference for non-disclosure, particularly in matters implicating personal data.[13]

3. LEGISLATIVE AND JUDICIAL INTERFACES BETWEEN TRANSPARENCY AND DATA PROTECTION

The collision between transparency and privacy is most visibly manifested at the intersection of statutory design and judicial interpretation. Having established the constitutional doctrine governing informational rights in the preceding section, this section turns to the legislative and institutional interface between the Right to Information Act, 2005 (RTI Act) and the Digital Personal Data Protection Act, 2023 (DPDP Act). It then situates India's emerging framework within a comparative context, principally drawing on the United Kingdom and European Union, to examine how similar tensions between access to information and personal data protection have been institutionally managed elsewhere. Through this comparative lens, the section identifies points of convergence and divergence, and clarifies why India's current configuration carries significant implications for institutional accountability and informational justice.

3.1 India: Legislative Amendment and Institutional Strains

The RTI Act, enacted in 2005, articulated a robust statutory entitlement: citizens are presumptively entitled to access information held by public authorities. This legislative commitment rested on a jurisprudential foundation laid in earlier constitutional decisions such as State of U.P. v. Raj Narain and S.P. Gupta v. Union of India, where the Supreme Court affirmed that the people have a right to know every public act performed by the State.[14] Within the statutory architecture of the RTI Act, Section 8(1)(j) embodied a calibrated compromise. While recognising privacy interests in personal information, it preserved a public-interest override, enabling disclosure where transparency considerations outweighed potential privacy harm.

The enactment of the DPDP Act in 2023 altered this statutory architecture. Through Section 44(3), the DPDP Act amended Section 8(1)(j) of the RTI Act in a manner widely understood to remove the explicit public-interest override in cases involving personal data.[15] Academic commentary has observed that this change transforms what had previously been a qualified exemption into a substantially more rigid disclosure standard, thereby reconfiguring the statutory balance between access and protection.[16] Some critiques have gone so far as to argue that the amendment risks significantly diminishing the operational effectiveness of the RTI framework in practice.[17] The concern is not merely abstract: information commissions and public authorities now face practical dilemmas when navigating the twin statutory obligations of transparency under the RTI Act and confidentiality under the DPDP Act.

Institutional reporting lends weight to these concerns. Independent monitoring of information commissions has documented growing uncertainty among adjudicatory bodies regarding the post- amendment scope of permissible disclosure, particularly in cases involving personal data. Key findings from recent assessments indicate that the removal of the explicit public-interest qualifier has encouraged administrative over-caution, with officials increasingly defaulting to non-disclosure in order to avoid potential liability under data protection norms.[18] This pattern is reinforced by observations in the Central Information Commission's annual reports, which note sustained increases in appeals and complaints involving exemption claims and highlight the interpretive challenges faced by public authorities in applying overlapping statutory regimes.[19]

On the judicial front, India has yet to develop a substantial body of post-DPDP case law directly addressing these tensions. Early commentary nonetheless points to a structural mismatch: while the RTI regime was designed around a presumption of openness mediated by contextual balancing, the DPDP regime embeds consent-based processing, purpose limitation, and broad exemptions for State action.[20] Public authorities are thus placed in a contradictory position, whether to disclose information in furtherance of public accountability or to withhold it in compliance with data protection mandates. The cumulative institutional effect is increased caution, reduced disclosure, and a gradual constriction of the transparency space that historically animated the RTI framework.

3.2 Comparative Practice: United Kingdom and European Union

Comparative experience offers useful contrasts. In the United Kingdom, the Freedom of Information Act, 2000 (FOIA) establishes a statutory right to access information held by public authorities, while personal data processing is regulated by the UK General Data Protection Regulation and the Data Protection Act, 2018. The UK's institutional approach explicitly acknowledges the tension between these regimes. The Information Commissioner's Office (ICO) has consistently emphasised that where an information request engages personal data, authorities must carefully balance the case for transparency against the data subject's right to privacy.[21]

Academic analysis notes that the GDPR has raised the threshold for disclosure of personal data under FOIA, particularly through Section 40 exemptions.[22] Crucially, however, the public-interest test remains embedded within the UK framework. Disclosure decisions continue to be guided by an assessment of fairness, necessity, and proportionality rather than by categorical exclusions.

A similar approach characterises the European Union's jurisprudence. While personal data protection is entrenched as a fundamental right, it is not treated as hierarchically superior to freedom of expression or access to information. In *Satakunnan Markkinapörssi Oy v. Finland*, the European Court of Human Rights held that privacy and expression must be jointly assessed and balanced in context, rather than ranked in the abstract.[23] The comparative lesson is consistent: the coexistence of transparency and privacy is most effectively managed through institutionalised balancing mechanisms, not through rigid statutory silos that privilege one right at the expense of the other.

3.3 Points of Divergence and Implications for India

When India's post-amendment framework is viewed against these models, three points of divergence become apparent.

First, the statutory weakening of the public-interest override marks a departure from the RTI Act's original design, which treated transparency as the default position subject to justified limitation. Post-amendment, the continued operation of this balancing principle has become uncertain.[24]

Second, the DPDP Act grants broad exemptions for State processing on grounds such as national security and public order, reinforcing a legislative architecture that prioritises privacy claims asserted by the State over disclosure sought for accountability.[25]

Third, India's institutional design remains fragmented. Unlike the UK and EU, where oversight bodies and regulatory guidance facilitate coordination between freedom-of-information and data- protection regimes, India's information commissions and data protection authorities operate within largely siloed frameworks, with limited formal mechanisms for harmonised interpretation.[26]

These divergences have tangible implications. When a requester seeks information regarding government beneficiaries or public programmes, authorities may now invoke the DPDP Act's expansive definition of personal data to withhold information that would previously have been disclosed under RTI on public-interest grounds. The result is not only legal uncertainty but functional paralysis of transparency mechanisms. Over time, this risks diluting the ethos of open governance and participatory oversight that the RTI regime was designed to foster.

3.4 Implications for Institutional Design

The comparative and legislative analysis underscores a deeper structural insight: information- regulating regimes must embed procedural mechanisms for balancing competing rights rather than leaving resolution to ad hoc discretion or categorical exemptions. The UK experience illustrates that transparency and privacy can coexist when treated as co-equal rights mediated through structured tests of fairness and public interest. By contrast, India's current trajectory reflects a legislative tilt toward treating privacy as an effective veto within the RTI framework.

Comparative jurisprudence reinforces this concern. The FOIA–GDPR interface in the UK retains a functional public-interest test, while European human-rights law rejects hierarchical ranking between privacy and expression.[27] India's post-amendment framework, however, risks privileging privacy claims asserted by public authorities without a commensurate institutional mechanism for contextual evaluation.

Accordingly, the analysis points toward the need for a reframed institutional architecture grounded in information constitutionalism. Such a framework would emphasise coordination between RTI and data-protection oversight bodies, reaffirm the centrality of public-interest assessment through legislative or regulatory guidance, and encourage disclosure decisions based on structured harm– benefit analysis rather than blunt exemption rules. Without such recalibration, the statutory collision between transparency and privacy may continue to erode the accountability-

enhancing function of the RTI Act in India's digital governance landscape.

4. THE DPDP ACT AND THE RECONFIGURATION OF DISCLOSURE OBLIGATIONS

The Digital Personal Data Protection Act, 2023 represents India's first comprehensive legislative framework governing the collection, processing, and use of personal data across public and private domains. Enacted in the aftermath of the Supreme Court's recognition of privacy as a fundamental right, the Act seeks to operationalise informational privacy through a statutory regime centred on consent, purpose limitation, and fiduciary accountability. At the same time, the DPDP Act performs an additional and less explicit function: it recalibrates the legal environment within which other information regimes, most notably the Right to Information Act, 2005, operate.

This section examines the DPDP Act not as a constitutional text, but as a statutory design instrument. The analysis proceeds by first unpacking the internal logic of the Act, the core principles, obligations, and differentiated treatment of State processing before turning to the manner in which these design choices interact with, and potentially displace, the balancing architecture embedded in the RTI framework. This approach allows the DPDP Act to be assessed on its own terms, prior to evaluating its institutional consequences for transparency and accountability.

4.1 The Internal Logic of the DPDP Act: Consent, Purpose Limitation, and State Processing

The Digital Personal Data Protection Act, 2023 is structured around a rights–obligations framework intended to regulate the processing of personal data through a combination of individual consent, purpose limitation, and fiduciary accountability.[28] At its core, the Act conceptualises personal data protection not merely as a negative restraint on data collection, but as a regulatory mechanism governing the entire lifecycle of data processing from collection and use to storage and erasure.[29] This architecture reflects the influence of contemporary global data protection models premised on informational self-determination and processor accountability.[30]

Central to the DPDP Act is the requirement that personal data be processed only for lawful purposes and, in most cases, with the consent of the data principal.[31] Consent under the Act is framed as informed, specific, and revocable, signalling an attempt to vest individuals with meaningful control over their personal information.[32] Purpose limitation operates as a complementary constraint: data may be processed only for purposes explicitly communicated at the time of collection, and further use beyond those purposes is generally impermissible.[33] Together, these principles are designed to curb excessive or opportunistic data exploitation, particularly in digital governance contexts characterised by large-scale data aggregation.

The Act further introduces the concept of "data fiduciaries," imposing duties of care, transparency, and security on entities that determine the purpose and means of processing personal data.[34] These obligations such as ensuring data accuracy, implementing reasonable safeguards, and responding to data principal requests are intended to operationalise accountability across both public and private sectors. From a statutory design perspective, this framework positions the DPDP Act as a general code governing personal data processing, rather than a sector-specific privacy statute.

The application of this framework to State actors, however, introduces a distinct dimension. The Act recognises that governmental processing of personal data frequently occurs in pursuit of sovereign or public functions and accordingly permits certain categories of State processing without consent where such processing is authorised by law.[35] These include processing necessary for the provision of public benefits or services, compliance with legal obligations, and functions relating to public order and security.[36] This differentiated treatment reflects a legislative judgment that a purely consent-centric model, suitable for private actors, cannot be transposed wholesale onto the State without impairing administrative capacity.

At the same time, this accommodation alters the balance between individual informational control and institutional discretion. While the DPDP Act frames privacy as a right enforceable against both private and public data processors, its design embeds a degree of latitude for non-consensual State processing. The statute thus contains an internal tension: it aspires to protect informational autonomy while simultaneously enabling expansive data-driven governance. This tension is not framed as an exception to the Act's logic but is integral to its structure.

Understanding this internal statutory logic is essential before assessing the DPDP Act's interaction with transparency obligations under the RTI framework. The Act does not directly regulate access- to-information regimes; instead, it governs the permissibility of data processing itself. Consequently, when personal data held by public authorities becomes the subject of disclosure requests, the consent- and purpose-based architecture of the DPDP Act inevitably intersects with and may constrain the disclosure-oriented logic of transparency law. It is this structural configuration, rather than any express prioritisation of privacy over transparency, that sets the stage for the reconfiguration of disclosure obligations examined in the subsequent sub-sections.

4.2 Statutory Exemptions and the State as a Privileged Data Fiduciary

A distinctive feature of the DPDP Act lies in its treatment of the State as a data processor operating under a differentiated legal standard. While the Act formally applies to both public and private entities, it embeds a set of statutory exemptions and relaxations that substantially recalibrate the obligations imposed on State actors. This design

choice reflects an underlying legislative assumption that governmental data processing, particularly in areas of governance and public administration, warrants greater operational latitude than comparable private-sector activities.

Section 7 of the DPDP Act permits the State to process personal data without consent where such processing is necessary for the performance of functions authorised by law. This includes, inter alia, the delivery of public services and benefits, compliance with statutory obligations, and activities connected with public order and security.[37] Section 17 further empowers the Central Government to exempt specified State agencies from the application of selected provisions of the Act in the interests of sovereignty, integrity, national security, and maintenance of public order.[38] Collectively, these provisions construct a statutory category of privileged data processing for the State, one that departs from the consent-centric model governing private data fiduciaries.

From a legislative design perspective, these exemptions are not framed as anomalies but as integral components of the DPDP framework. They acknowledge the practical reality that many core functions of the modern administrative State ranging from welfare delivery to law enforcement depend upon large-scale data collection and processing that cannot feasibly operate on an individualised consent model. The statute thus prioritises administrative functionality and continuity of governance, even where this entails a partial dilution of individual informational control.

However, this privileging of State processing carries significant normative implications. By permitting broad categories of non-consensual data processing and by vesting the executive with discretionary exemption powers, the DPDP Act repositions the State not merely as a regulated data fiduciary but as an actor endowed with enhanced control over personal data. This statutory asymmetry alters the balance between data principal rights and institutional discretion, particularly in contexts where the same public authority functions simultaneously as data collector, data user, and decision-maker.

The implications of this asymmetry are magnified when State-held personal data intersects with transparency obligations. Although the DPDP Act does not explicitly address access-to-information regimes, its exemption architecture indirectly conditions how public authorities perceive their disclosure responsibilities. Where personal data is processed under broad statutory authorisations or executive exemptions, officials may be incentivised to treat such data as presumptively protected from disclosure, irrespective of its relevance to public accountability. The result is not a direct conflict between privacy and transparency statutes, but a structural environment in which privacy protections asserted by the State acquire heightened weight.

It is important to emphasise that the DPDP Act does not declare privacy to be hierarchically superior to transparency. Rather, it achieves this effect indirectly through statutory design. By granting the State enhanced processing privileges while remaining silent on the downstream implications for disclosure, the Act reshapes the legal context within which transparency decisions are made. This reconfiguration sets the groundwork for the displacement of the RTI Act's balancing logic, a process examined more directly in the following subsection.

4.3 Section 44(3) and the Displacement of the RTI Act's Balancing Architecture

The most consequential point of intersection between the DPDP Act and India's transparency framework arises through Section 44(3) of the DPDP Act, which amends Section 8(1)(j) of the Right to Information Act, 2005. This amendment alters the statutory conditions under which personal information held by public authorities may be disclosed, with significant implications for the balancing architecture that historically governed RTI adjudication.

Prior to the amendment, Section 8(1)(j) of the RTI Act exempted personal information from disclosure only where such information bore no relationship to any public activity or interest, or where disclosure would cause an unwarranted invasion of privacy, unless the larger public interest justified disclosure. This public-interest override functioned as the statutory mechanism through which transparency and privacy were reconciled in practice, enabling information officers and adjudicatory bodies to assess disclosure requests contextually rather than categorically.

Section 44(3) of the DPDP Act modifies this provision by removing the explicit reference to public- interest-based disclosure in cases involving personal data.[39] The revised formulation narrows the scope for discretionary balancing by reframing personal information as presumptively protected, without expressly retaining the evaluative space that previously allowed competing considerations to be weighed. From a statutory design perspective, this represents not merely a procedural amendment but a substantive reconfiguration of the RTI Act's disclosure logic.

Importantly, this displacement does not operate through an express declaration of priority between privacy and transparency. The DPDP Act does not state that personal data protection overrides the right to information. Instead, the effect is achieved indirectly, by excising the statutory language that authorised contextual assessment. In doing so, Section 44(3) transforms what had been a conditional exemption into a more rigid threshold, reducing the normative flexibility available to decision-makers under the RTI framework.

This reconfiguration also shifts the locus of discretion. Whereas the earlier formulation empowered information officers and commissions to justify disclosure on public-interest grounds, the amended provision encourages a defensive orientation, in which withholding becomes the safer institutional choice. The absence of explicit statutory guidance on how to reconcile DPDP obligations with RTI disclosure duties further amplifies this tendency, particularly in light of the penalties and compliance expectations embedded within the data protection regime.

It bears emphasis that Section 44(3) does not repeal Section 8(2) of the RTI Act, which permits disclosure of exempt information where public interest outweighs the harm to protected interests.[40] However, the relationship between Section 8(2) and the amended Section 8(1)(j) remains legally unsettled. In the absence of clarificatory legislative guidance or authoritative judicial interpretation, the practical operation of Section 8(2) as a residual safeguard is uncertain. This ambiguity reinforces the perception that the statutory balance has shifted away from disclosure, even if

not formally extinguished.
Accordingly, Section 44(3) functions as a pivot point in India's contemporary information law framework. By altering the statutory conditions under which personal data may be disclosed, it displaces the RTI Act's embedded balancing architecture and reorients transparency adjudication toward categorical exclusion rather than contextual evaluation. The institutional consequences of this shift particularly for information commissions and public authorities are examined in the following subsection.

4.4 From Balancing to Categorical Exclusion: Institutional Consequences

The cumulative effect of the DPDP Act's statutory design choices is most clearly visible at the institutional level, where transparency obligations are operationalised by public authorities and adjudicated by information commissions. The combined impact of differentiated State processing, broad exemption powers, and the amendment to Section 8(1)(j) of the RTI Act has been to narrow the discretionary space within which disclosure decisions are made.[14] What was previously a context-sensitive balancing exercise has increasingly been replaced by a presumption of non- disclosure in cases involving personal data.
Under the pre-amendment RTI framework, information officers and commissions were statutorily encouraged to justify disclosure by articulating public interest considerations that outweighed potential privacy harm. The removal of the explicit public-interest qualifier in Section 8(1)(j), read alongside the DPDP Act's emphasis on consent and lawful purpose, alters this institutional calculus.[41] Disclosure now appears as an exception requiring heightened justification, while withholding becomes the default position consistent with data protection compliance.
This shift has practical implications for institutional behaviour. Public authorities, confronted with overlapping statutory obligations and asymmetrical enforcement risks, are incentivised to adopt a risk-averse posture. The penalties, compliance expectations, and oversight mechanisms embedded in the data protection regime contrast sharply with the comparatively weaker enforcement incentives for disclosure under the RTI Act.[42] In such an environment, institutional actors may rationally prioritise data protection obligations over transparency, even in cases where disclosure would advance democratic accountability.
Information commissions are similarly affected. In the absence of explicit statutory guidance on reconciling the DPDP Act with RTI disclosure mandates, commissions must navigate interpretive uncertainty when adjudicating appeals involving personal data.[43] This uncertainty constrains the development of consistent jurisprudence and undermines the commissions' ability to function as robust balancing institutions. The result is not the elimination of transparency as a legal value, but its gradual marginalisation through institutional practice.
Crucially, these consequences do not flow from an express legislative declaration that privacy trumps transparency. Rather, they emerge from the indirect interaction of statutory provisions that reconfigure decision-making incentives. By reshaping the conditions under which disclosure decisions are taken, the DPDP Act alters the institutional environment in which transparency operates.[44] This transformation marks a shift from a model of contextual balancing toward one of categorical exclusion, with significant implications for the functioning of India's information governance framework.

5. COMPARATIVE LESSONS AND INSTITUTIONAL PATHWAYS FOR HARMONISATION

The tension between transparency and privacy examined in the preceding sections is not unique to India. It reflects a broader global challenge faced by constitutional democracies seeking to recalibrate governance in the digital age. However, comparative experience demonstrates that this tension need not collapse into a binary choice between disclosure and denial. Jurisdictions that have successfully navigated this terrain have done so by embedding structured balancing mechanisms within their legal and institutional frameworks, ensuring that neither transparency nor privacy operates as an absolute. Viewed against this backdrop, India's post-DPDP framework reveals specific design and institutional gaps that merit closer examination.

5.1 Comparative Lessons: Institutionalising the Reconciliation of Competing Imperatives

(a) United Kingdom: Unified Oversight and Procedural Balancing

The United Kingdom offers a well-developed model of institutionalised reconciliation between access to information and data protection. The Freedom of Information Act, 2000 and the Data Protection Act, 2018 are administered by a single oversight authority, the Information Commissioner's Office (ICO), which applies a unified interpretive framework across both regimes.[45] This institutional convergence ensures that requests implicating personal data are assessed through a consistent decision-making process rather than through fragmented or adversarial silos.
Under the UK framework, personal data exemptions under FOIA particularly Section 40 do not operate categorically. Instead, disclosure decisions are guided by a public interest assessment that weighs privacy harm against democratic necessity.[46] The principal advantage of this model lies in procedural predictability and doctrinal coherence: the same authority interprets the same factual matrix under overlapping statutes, reducing interpretive conflict and enhancing accountability. In contrast, India's bifurcated oversight structure dividing authority between information commissions and the Data Protection Board lacks formal coordination mechanisms, increasing the risk of inconsistent outcomes.

(b) European Union: Proportionality as a Structuring Principle

Within the European Union, proportionality functions as the central organising principle for reconciling privacy and transparency. Article 52(1) of the Charter of Fundamental Rights of the European Union requires that any limitation

on fundamental rights satisfy standards of legality, necessity, and proportionality.[47] The General Data Protection Regulation reinforces this approach by explicitly recognising, in Recital 154, that data protection must be harmonised with freedom of information and expression, leaving Member States the task of reconciling these rights through legislative design.[48]

The EU experience underscores an important lesson: conflicts between informational rights are not resolved by ranking one right above another, but by subjecting interferences to contextual justification. This proportionality-based model aligns closely with the constitutional doctrine articulated in Puttaswamy, while also demonstrating how such doctrine can be operationalised through statutory and institutional mechanisms.

(c) Mexico: Statutory Symbiosis and Default Balancing

Mexico presents perhaps the most integrated statutory approach. Constitutional and legislative reforms between 2014 and 2017 established a dual framework for transparency and data protection administered by a single autonomous authority, the Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).[49] Under this regime, public interest balancing is not treated as an exception but as a default decision-making standard. Article 183 of the Mexican General Law on Transparency explicitly permits disclosure where the social relevance of publicity outweighs the harm to privacy.[50]

This codified balancing standard mitigates bureaucratic tendencies toward risk-averse denial and embeds accountability within the statutory text itself. Together, the UK, EU, and Mexican models illustrate a shared insight: transparency and privacy coexist most effectively where balancing is institutionalised rather than left to ad hoc discretion.

5.2 India's Structural Deficit: Fragmentation, Ambiguity, and Concentrated Discretion

Against these models, India's post-DPDP framework exhibits three interrelated structural limitations.

First, institutional fragmentation persists. The Central Information Commission and the Data Protection Board of India operate within distinct statutory silos, with no formalised procedures for coordination or cross-referencing. This separation increases the likelihood of conflicting interpretations when disclosure requests implicate personal data.

Second, legislative ambiguity remains pronounced. The amendment to Section 8(1)(j) of the RTI Act removes the explicit public interest qualifier without providing interpretive guidance for adjudicators.[51] As demonstrated in Sections 3 and 5, this silence effectively shifts discretion from law to administration, fostering uncertainty and encouraging defensive decision-making.

Third, the DPDP Act concentrates significant discretionary power in the executive, particularly through exemption provisions applicable to State agencies.[52] While such exemptions may be justified on governance grounds, their breadth raises concerns regarding the erosion of accountability safeguards, especially in light of the proportionality requirements emphasised in Puttaswamy.[53]

The cumulative institutional effect is a constriction of the transparency space that the RTI Act was originally designed to protect. This is not the result of an express legislative rejection of openness, but of an incremental reconfiguration of incentives and discretion.

5.3 Institutional Pathways for Harmonisation

Comparative experience suggests several pathways through which India could mitigate these structural tensions.

At the statutory level, clearer articulation of the relationship between the DPDP Act and the RTI framework particularly the role of residual public interest safeguards such as Section 8(2) of the RTI Act would enhance interpretive coherence.[54]

At the institutional level, mechanisms for coordination between information commissions and data protection authorities could promote consistent application of balancing standards, reducing fragmentation without collapsing distinct mandates.

At the administrative level, capacity-building initiatives focused on proportionality analysis and ethical data governance would strengthen the interpretive competence of public information officers and data fiduciaries alike.[55]

Finally, judicial oversight remains critical. Pending legislative clarification, courts retain the capacity to operationalise proportionality principles within RTI adjudication, as reflected in decisions such as CPIO, Supreme Court of India v. Subhash Chandra Agarwal.[56] Judicial articulation of balancing standards can serve as an interim stabilising force, preventing the categorical exclusion of transparency claims.

5.4 Towards a Coherent Democratic Information Order

The comparative analysis reinforces a central insight of this study: transparency and privacy are not antagonistic rights but interdependent democratic guarantees. Transparency constrains state secrecy; privacy restrains state intrusion. A coherent democratic information order must therefore reconcile both through structured, principled mechanisms rather than through rigid statutory silos.

Such an order rests on three normative anchors: proportionality in rights limitation, institutional parity among oversight bodies, and the primacy of public interest as the animating purpose of informational rights. Reaffirming these anchors

would allow India's information governance framework to preserve the transformative promise of the RTI Act while respecting the dignitarian values embedded in the DPDP Act.

6. Conclusion

This study has demonstrated that the contemporary tension between transparency and privacy in India cannot be adequately understood as a simple clash of constitutional rights. Rather, it is a problem of statutory design and institutional incentives within an increasingly data-driven state. While the Right to Information Act, 2005 and the Digital Personal Data Protection Act, 2023 each possess independent normative legitimacy, their interaction reveals how legislative architecture can recalibrate the practical conditions under which constitutional values are realised. The shift observed in India's information regime is therefore not the result of an express rejection of openness, but of a subtler reconfiguration of how disclosure decisions are structured, justified, and constrained.

The core contribution of this paper lies in showing that constitutional balancing need not be doctrinally overturned to be functionally displaced. Through its consent-centric framework, differentiated treatment of State processing, and the amendment to Section 8(1)(j) of the RTI Act, the DPDP Act alters the institutional environment in which transparency operates. In doing so, it transforms contextual balancing into a more categorical mode of decision-making, without formally ranking privacy above transparency. This insight advances the concept of information constitutionalism by highlighting the central role of statutory design in mediating constitutional values in the digital age. Rights, as this analysis shows, are not realised solely through judicial articulation, but through the everyday incentives and constraints embedded in legislative and administrative frameworks.

The institutional stakes of this transformation are significant. Where discretion to balance competing interests is narrowed or rendered uncertain, public authorities and adjudicatory bodies are likely to gravitate toward risk-averse interpretations that favour non-disclosure. Over time, such patterns may reshape transparency from a presumptive democratic norm into an exception requiring special justification. This does not signal the erosion of privacy as a constitutional value; rather, it illustrates how privacy, when operationalised through statutory silence and executive discretion, may acquire an exclusionary force that was never constitutionally intended.

Ultimately, the coexistence of transparency and privacy is a measure of constitutional maturity in a digital democracy. Both function as safeguards against arbitrary power one constraining secrecy, the other intrusion. The challenge for India's evolving information order is not to choose between them, but to sustain forms of governance capable of holding both in principled tension. Whether the promise of calibrated openness can endure will depend less on the abstract recognition of rights than on the institutional arrangements through which information is governed, disclosed, and justified. In this sense, the future of democratic accountability in India will be shaped not only by what the law protects, but by how it structures the exercise of informational power.

7. REFERENCES

1. Constitutional Provisions

Constitution of India

- Article 19(1)(a)
- Article 21

2. Statutes and Legislative Material

Indian Legislation

- Right to Information Act, 2005
- Digital Personal Data Protection Act, 2023 Foreign Legislation
- Freedom of Information Act, 2000 (United Kingdom)
- Data Protection Act, 2018 (United Kingdom)
- Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR)
- Ley General de Transparencia Accesoca la Informacion Publica(General Law on Transparency and Access to Public Information 2015 (Mexico)

3. Judicial Decisions (Case Law)

Supreme Court of India

- State of U.P. v. Raj Narain, (1975) 4 SCC 428
- S.P. Gupta v. Union of India, AIR 1982 SC 149
- Kharak Singh v. State of U.P., AIR 1963 SC 1295
- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
- Girish Ramchandra Deshpande v. Central Information Commission, (2013) 1 SCC 212
- R.K. Jain v. Union of India, (2013) 14 SCC 794
- CPIO, Supreme Court of India v. Subhash Chandra Agarwal, (2019) 16 SCC 808
- People's Union for Civil Liberties v. Union of India, (1971) 1 SCC 301
- Secretary, Ministry of Information and Broadcasting v. Cricket Assn. of Bengal, (1995) 2 SCC 161

High Courts

• Shailesh Gandhi v. Union of India, W.P. No. 1013 of 2024 (Bombay High Court, pending) European Court of Human Rights
• Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, App Nos. 931/13 and 2874/13 (ECtHR, 2017)

4. Reports and Official Publications

• Central Information Commission, Annual Report 2022–23, prepared under Section 25 of the Right to Information Act, 2005
• Central Information Commission, Annual Report 2023–24, prepared under Section 25 of the Right to Information Act, 2005
• Department of Personnel and Training, Annual RTI Compliance and Capacity Building Report (2024)
• Ministry of Electronics & Information Technology, "DPDP Act, 2023 Upholds Privacy While Preserving Transparency under RTI", Press Information Bureau, 20 August 2025

5. Books

• Solove, D. J., Understanding Privacy (Harvard University Press, 2008)

6. Journal Articles and Academic Commentary

• Salman Qasmi, Impact of Data Protection Laws on the Right to Information: A Comparative Analysis of India and the United Kingdom, ILI Law Review, Summer Issue (2024)
• Curtis McCluskey, How Will the GDPR Affect FOI Law, Reed Smith Perspectives (June 2017)
• Right to Privacy & Data Protection: Strengths and Weaknesses of India's New DPDP Act, Common Cause Journal, Vol. XLII, No. 3 (2023)

7. Policy Briefs, NGO Reports, and Commentary

• Satark Nagrik Sangathan, Report Card on the Performance of Information Commissions in India 2023–24
• A Critical Analysis of the RTI Act Amendment via the DPDP Act, 2023, La Excellence IAS (Policy Commentary, 2025)
• Trailblazer Legal, "Privacy and Transparency under the DPDP Act: Analysis of MeitY Clarification" (2025)

8. Foreign Institutional and Regulatory Materials

• Information Commissioner's Office (UK), FOI and Other Laws: Guide to Managing an FOI Request
• Information Commissioner's Office (UK), Freedom of Information and Data Protection: Guidance on Personal Data and Disclosure (2023)
• Information Commissioner's Office (UK), Personal Data Exemptions under Section 40 FOIA

9. International Instruments

• Charter of Fundamental Rights of the European Union, Article 52(1)

Endnotes

1 State of U.P. v. Raj Narain, (1975) 4 SCC 428; S.P. Gupta v. Union of India, AIR 1982 SC 149.
2 Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
3 State of U.P. v. Raj Narain, (1975) 4 SCC 428.
4 S.P. Gupta v. Union of India, AIR 1982 SC 149.
5 Kharak Singh v. State of U.P., AIR 1963 SC 1295.
6 Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
7 Girish Ramchandra Deshpande v. Central Information Commission, (2013) 1 SCC 212.
8 R.K. Jain v. Union of India, (2013) 14 SCC 794.
9 CPIO, Supreme Court of India v. Subhash Chandra Agarwal, (2019) 16 SCC 808.
10 Ibid., para 73.
11 Shailesh Gandhi v. Union of India, W.P. No. 1013 of 2024 (Bombay HC, pending).
12 Central Information Commission, Annual Report 2022–23, prepared under Section 25 of the Right to Information Act, 2005, noting trends in appeals, complaints, and invocation of exemptions by public authorities.
13 Satark Nagrik Sangathan, Report Card on the Performance of Information Commissions in India 2023–24 (Key Findings), observing the impact of the DPDP-linked amendment to Section 8(1)(j) on disclosure practices and administrative decision-making under the RTI framework.
14 State of U.P. v. Raj Narain, (1975) 4 SCC 428; S.P. Gupta v. Union of India, AIR 1982 SC 149.
15 Digital Personal Data Protection Act, 2023, s. 44(3).

16 Salman Qasmi, Impact of Data Protection Laws on the Right to Information: A Comparative Analysis of India and the United Kingdom, ILI Law Review, Summer Issue (2024).

17 A Critical Analysis of the RTI Act Amendment via the DPDP Act, 2023, La Excellence IAS (Policy Commentary, 2025).

18 Satark Nagrik Sangathan, Report Card on the Performance of Information Commissions in India 2023–24 (Key Findings).

19 Central Information Commission, Annual Report 2022–23 and Annual Report 2023–24, prepared under Section 25 of the Right to Information Act, 2005.

20 Ministry of Electronics & Information Technology, "DPDP Act, 2023 Upholds Privacy While Preserving Transparency under RTI", Press Information Bureau, 20 August 2025.

21 Information Commissioner's Office (UK), FOI and Other Laws: Guide to Managing an FOI Request, ICO Guidance, available on the ICO website (accessed 18 November 2025).

22 Curtis McCluskey, How Will the GDPR Affect FOI Law, Reed Smith Perspectives (June 2017).

23 Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, App Nos. 931/13 and 2874/13, European Court of Human Rights (2017).

24 Salman Qasmi, supra note 3.

25 Right to Privacy & Data Protection: Strengths and Weaknesses of India's New DPDP Act, Common Cause Journal, Vol. XLII, No. 3 (2023).

26 Trailblazer Legal, "Privacy and Transparency under the DPDP Act: Analysis of MeitY Clarification", reporting on Ministry of Electronics & Information Technology clarification dated 22 August 2025 (accessed 6 December 2025).

27 Satakunnan Markkinapörssi Oy, supra note 10.

28 Digital Personal Data Protection Act, 2023 (hereinafter DPDP Act), Statement of Objects and Reasons.

29 DPDP Act, ss. 4–6.

30 D. J. Solove, Understanding Privacy (Harvard University Press, 2008).

31 DPDP Act, s. 6.

32 DPDP Act, s. 6(1)–(4).

33 DPDP Act, s. 4.

34 DPDP Act, ss. 7–10.

35 DPDP Act, s. 7.

36 DPDP Act, s. 17.

37 Digital Personal Data Protection Act, 2023, s. 7.

38 Digital Personal Data Protection Act, 2023, s. 17.

39 Digital Personal Data Protection Act, 2023, s. 44(3).

40 Right to Information Act, 2005, s. 8(2).

41 Digital Personal Data Protection Act, 2023, ss. 7, 17, and 44(3).

42 Right to Information Act, 2005, ss. 8(1)(j) and 8(2).

43 Digital Personal Data Protection Act, 2023, ss. 7, 17, and 44(3).

44 Digital Personal Data Protection Act, 2023, ss. 7, 17, and 44(3).

45 Information Commissioner's Office (UK), Freedom of Information and Data Protection: Guidance on Personal Data and Disclosure (2023).

46 ICO, Personal Data Exemptions under Section 40 FOIA, updated guidance; see also UK GDPR, art. 6(1)(f).

47 Charter of Fundamental Rights of the European Union, art. 52(1).

48 Regulation (EU) 2016/679 (General Data Protection Regulation), Recital 154.

49 Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), Ley General de Transparencia y Acceso a la Información Pública (2015); Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (2017).

50 Ibid., art. 183, provisions permitting disclosure where public interest or social relevance outweighs privacy harm.

51 Salman Qasmi, "Impact of Data Protection Laws on the Right to Information: A Comparative Analysis of India and the United Kingdom," ILI Law Review, Summer Issue 2024, pp. 263–269.

52 Digital Personal Data Protection Act, 2023, s. 17.

53 Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, paras 310–321.

54 Right to Information Act, 2005, s. 8(2).

55 Department of Personnel and Training, Annual RTI Compliance and Capacity Building Report (2024).

56 CPIO, Supreme Court of India v. Subhash Chandra Agarwal, (2019) 16 SCC 808.