



Right to Know to Right to Deny: Critical Analysis of the Data Protection Effects on RTI in India

Harsh¹

Abstract:

This paper views the balance of transparency and confidentiality in Indian governance as dynamic and constantly evolving. It contends that the transparency will assure accountability, citizens involvement, and trust, whereas secrecy is necessary for ensuring national security, information secrets, and individual privacy. This study uses a mixed method design of doctrinal legal analysis, case law analysis and empirical survey data. The most important laws such as the Right to Information Act (2005) and Digital Personal Data Protection Act (2023) are examined critically and landmark judicial decisions are examined. Results indicate that there is a big disparity between the high awareness levels of the general population on transparency measures especially the RTI Act and lack of awareness of data protection laws, even as there is a rising concern on digital privacy. This paper concludes that Indian governance is at a transitory stage and suggests a more balanced and principle-driven model to reconcile transparency and confidentiality in terms of good and responsible governance.

Keywords: Transparency, Confidentiality, RTI Act, Data Protection, Governance, Privacy, Accountability, India

Introduction

The modern development of government in India is characterized by a multifaceted and more and more decisive interaction of normative obligations towards transparency and the demands of confidentiality. The Right to Information Act, 2005 is a landmark in the Indian democratic movement that has revolutionized the relations between the citizens and the state, making access to information a constitutional right, as well as a tool of accountability. The operationalization of the right to know has facilitated the citizens to challenge the administrative decision-making process, uncover corruption, and engage in political life more significantly through the Act. Through this, it has transformed the nature of information to a public good

¹ Ram Lal Anand College, University of Delhi



instead of a state-owned resource. Conceptualizing the Privacy and Freedom, on a theoretical level, views privacy as a right of an individual to control personal information and, therefore, brings out the necessary tension between informational access and personal autonomy, whereas The Right to Know emphasizes transparency as a precondition of democratic responsibility and good governance.

At the same time, the emergence of digital governance and the enormous increase in data creation have pre-empted the necessity of strong data protection systems. This change is reflected in the Digital Personal Data Protection Act, 2023, which in turn introduces privacy as a key principle that guides the organization of governance. But the co-existence of the regimes of transparency and data protection creates a structural conflict, especially in the cases when access to the information conflicts with personal data. According to The Transparent Society, the current form of governance may be marked by a paradox that when transparency increases, the citizens will be empowered and individuals will be at risk. The current paper is a critical analysis of the evidence of a gradual transformation of a right to know into a right to deny in India and whether there is a way to balance the two opposing imperatives under a sound system of governance.

Objectives

1. The purpose of the research is to critically analyse the interface of the Right to Information Act, 2005 and the Digital Personal Data Protection Act, 2023.
2. To determine how data protection affects the coverage and performance of RTI regime.
3. To consider the consequences to democratic accountability and access to information by citizens.
4. To analyze the social perception and awareness using empirical evidence.
5. To suggest a moderate model to mediate transparency and confidentiality.

Methodology

The research design of this study will be a mixed-method research design involving both doctrinal legal analysis and empirical research to investigate the interface between transparency and data protection in India. The doctrinal aspect entails the critical analysis of the statutory provisions of the Right to Information Act, 2005 and the Digital Personal Data Protection Act, 2023, as well as the judicial interpretations. Key principles, including the public interest, privacy, proportionality, and accountability are analyzed using a



thematic and interpretative approach. The empirical element is based on the survey information that indicates the public awareness, and their perception of transparency and data protection. Discussion of the results is done to establish trends, loopholes, and other emerging problems in the governance model. Such a mixed methodology approach enables us to see the entire picture of the fluctuating balance between openness and confidentiality.

Conceptual Framework: Transparency, Privacy, and Democratic Governance

The ideals of transparency and privacy normative frameworks, the concept of transparency and privacy, are conceptually connected because they are necessitated yet may be conflicting values of democratic governance. No secret that transparency is one of the key principles of democracy that enables citizens to get the information, audit state activity as well as hold the representatives of the hierarchy on their feet. It turns the governance process participative and it develops trust, legitimacy and responsiveness. Availability of information is essential because it is a significant factor to hold the power accountable because it inspires the citizens to have the authority to take part in the decision-making process as it sparks accountability in how power is used as described in The Right to Know. In this instance, transparency would extend beyond the administrative transparency and be a structural requirement to the retention of democratic accountability and institutional integrity.

On the other hand, privacy is one of the basic requirements of personal autonomy and dignity, especially in the age of the blistering development of digital technologies and data government. Privacy and Freedom conceptualize privacy to be the power of the individual to regulate personal information thus directly connecting it to personal liberty and freedom. This view highlights the dangers of not controlling transparency where too much information can be misused by surveillance, misuse of information, and loss of personal rights. The safety of personal information has become one of the paramount demands of the modern system of governance, making sure that people have the control over their informational identity in an ever-growing digital space.

The conflict between transparency and privacy is highly acute in the situations when the interest of the population collides with the information about individuals, which poses a dilemma that would be difficult to govern. According to The Transparent Society, a paradox in the contemporary societies is that the higher the level of transparency, the more power a citizen will have and at the same time the more vulnerable they will be. This duality points out the necessity of having a balanced and context-sensitive strategy, which avoids the prevalence of either of the two principles. Too much transparency can undermine the privacy



and the personal security, whereas too little can undermine accountability and become opaque. Hence, transparency and privacy need to be perceived as mutually supporting concepts that need to be fine-tuned especially in the Indian context whereby legal developments are an indication of a struggle to balance the right to know with the right to privacy in a system of democracy.

Intersecting Regimes: Frictions between Disclosure and Data Protection

The normative commitment to transparency and the need to protect personal data in India have an important intersection point in the point where the Right to Information Act, 2005 and the Digital Personal Data Protection Act, 2023 meet. Whereas the RTI Act is founded on the notion of maximum disclosure as an accountability measure, the DPDP Act is organized based on the protection of individual privacy based on limiting data processing and dissemination. This difference presents a complicated legal and administrative quandary especially in situations where the information requested under RTI includes personal information. The RTI model permits the disclosure when the social good can be deemed significant than the privacy concern, however, DPDP regime revolves around the concept of consent and data security and consequently, can limit such disclosure. This means that the public authorities are becoming more and more obliged to walk the fine line between two sets of duty with no clear statutory advice on how to harmonize the two, and so interpretative uncertainty results, and mixed decision-making in practice.

This paradox shows a bigger paradox in the framework of the modern information governance whereby the spread of data protection principles may become an obstacle to transparency by default. The demand to enjoy privacy in high network societies as proposed in The Transparent Society commonly march with the objectives of openness and accountability, and opposing them even in certain instances. This opens up a danger where data protection issues might be invoked as a justification to refuse any request of information and hence re-institute the default orientation of governance as disclosure to restriction. Such a change that cannot be prevented might destabilize the transformational power of the RTI regime and weaken democracy. Meanwhile, it will be simplistic to consider this tension as one that is simply antagonistic because the two frameworks are aimed at safeguarding legitimate interests, namely, public accountability and individual dignity. The difficulty is thus to be able to create a principled and context-specific solution that will not allow the instrumentalization of privacy in the form of obstacle to openness and yet the revelation of information will not lead to any unnecessary encroachment on personal information.



Juridical Strategy: A Right to Know/Right to Privacy Balance

The Indian judiciary has taken the centre stage in reconciling the conflict between transparency and privacy by establishing a constitutional structure that respects both of these ideals in a balanced and principled way. The courts have come to understand through its developing jurisprudence that neither the right to know nor the right to privacy is absolute and both require balancing against the overall constitutional purposes. This was a breakthrough with the acknowledgment of informational privacy as a fundamental right as in Justice K.S. Puttaswamy v. Union of India (2017), privacy was definitely entrenched in the framework of Article 21. Meanwhile, the judicial interpretation of the Right to Information Act, 2005 has continually reiterated that the Act is a very important tool in promoting transparency and accountability. The importance of this dual recognition is that it shows the judiciary has devoted itself to ensuring both individual autonomy and democratic control through a constitutional system.

Courts have also resorted to the doctrine of proportionality as a tool of court reasoning in the settlement of the conflicting rights to balance the competing interests. This method stipulates that any limitation on the right to information should be reasonable, essential, and commensurate to the privacy protection purpose. Cases involving judicial decisions as to the interpretation of the clauses that concern the personal information in the RTI framework have reiterated the fact that the exemption to privacy cannot be brought to bear in a mechanical manner, but must be balanced in relation to the greater populace interest. This is to make sure that refusal of information is not arbitrary but based on a justifiable reason. The proportionality framework thereby allows a contextualized analysis where the content of the information, its impact on the public interest, and the harm it could cause to the privacy of the individuals is well evaluated before making a decision.

Moreover, court decisions demonstrate awareness of evolving times of governance in the digital age where there is more permeability between the information that is publicly known and that which is privately known. The courts have realised that accountability must be enhanced with transparency to a great degree, yet on the other hand, careless disclosure of person data may undermine the integrity and security of individuals. This subtlety is in line with a broader theoretical perspective of transparency and privacy being mutually compatible, and the necessity of a balancing act. The judicial interventions have also tried to prevent the erosion of both principles by encouraging a balance, which is based on constitutional values. However, since the RTI Act and the DPDP Act are not harmonised at the statutory level, this imposes the additional burden of judicial interpretation, and there is therefore an urgent need to further elaborate a



consistent and coherent framework that will be in a position to regulate the administrative practice and secure the integrity of the two transparency and data protection regimes.

Empirical Findings: RTI and Data Protection Perception and Awareness

The results of the study in terms of empirical evidence demonstrate that the public is highly one-sided in their level of awareness and involvement into the system of transparency and data protection in India. The survey data shows that the Right to Information Act, 2005 is well-recognized among the respondents that show its presence and practical usefulness in the daily governance. A large percentage of respondents reported to be familiar with RTI processes and recognized it as a powerful tool in ensuring accountability, obtaining governmental information and grievances. The fact that RTI is seen by many respondents as a citizen-focused instrument that increases democratic engagement also suggests that the culture of transparency has been fairly cultivated in the minds of people. This level of awareness is possible because of the continued use, institutional visibility and direct relationship to the matters of governance and delivery of services to the people.

Conversely, the results indicate a relatively low sensitivity and knowledge level about the Digital Personal Data Protection Act, 2023 and larger data protection principles. Although the respondents raised the general concern of misuse of data, privacy breach, and surveillance by the Internet, there was little understanding of the legal rights, regulatory systems, and solutions in case of violation of the data protection system. This disjunction leads to the assumption that data protection is not an established field as it is in the case of RTI and has not yet penetrated the consciousness of the population. This state of ignorance is especially troubling, especially in the light of growing digitization, where people are being asked to give out personal information on a regular basis with little knowledge of the repercussions. These results therefore indicate a lack of a connection between increased privacy concerns and the extent of legal literacy needed to deal with them.

Moreover, the survey indicates a shifting social attitude that tries to balance the two conflicting demands of openness and confidentiality. Although most of the respondents were in support of the further empowerment of RTI as an accountability tool, there was an increasing awareness of the necessity to ensure that personal information does not find itself into the wrong hands. Such duality shows a new consciousness of the complicatedness of the modern governance, with citizens on one hand requiring openness on the part of the state, and protection on the other hand of their own data. Notably, a few respondents were concerned



that the laws to protect data might be abused to limit access to information, thus undermining the transparency systems. These results support the main thesis of the research that India is in a period of transition, and the coexistence of the regimes of transparency and data protection is transforming the expectations and governance practices of the population, and it is time to be more balanced and informed in harmonizing it.

Moving towards a Unified Framework: Balancing Transparency and Confidentiality

To amalgamate the Right to Information Act, 2005 and the Digital Personal Data Protection Act, 2023 in a dynamic relationship, it demands the articulation of a consistent principle-based construct that would accommodate the two demands of transparency and confidentiality in the Indian constitutional order. Rather than viewing these regimes as inimical, a less obvious pathway would be better to view these regimes as coordinating instruments to various yet mutually necessitating democratic finalities, which are accountability and personal autonomy. The ideological core of such harmonization is the doctrine of the public interest, which is carried out by a systematic utilization of proportionality, which examines the respectability, the need and impact of disclosure in privacy. It requires the necessity of going beyond two-polar approach to disclosure and denial and adopting situation-based approach where information governance is guided by intent, interest and harm. In this regard, privacy must not be reduced to a strict deterrent of transparency and transparency must not be a free ride but the two must be checked to uphold the sanctity of the democratic rule.

On an institutional level, this balance can be achieved through the formulation of strong interpretative principles and sound administrative customs that deal with the interface of these legal regimes. It has resulted in an absence of cohesion in the statutory harmonization, typically either through an excessively conservative approach or through an ad hoc approach. As much as this can be reduced by incorporating standardized balancing tests in the administrative procedures and having detailed guidelines on how to go about the request in personal information. It is also significant to increase institutional capacity through institutional training of information officers and data fiduciaries and improve the coordination of transparency and data protection agencies to encourage doctrinal consistency. Adequate supervisory measures, such as review and appeal avenues, should be strengthened as a protection against unnecessary information blockage as well as unreasonable interference with personal information. This form of institutional alignment would not only add to the legal certainty, but would also create popular confidence in the fairness and fairness of the procedures in governance.



At a more systemic level, harmonization must also be sensitive to the facts of digital governance in which the boundaries between the information of the state and the privately owned is becoming more permeable. The problem is not merely one of a trade-off between two rights which are competing anymore, but one of a restructuring of the governance of the information, per se, in a world of continuous data streams and information inter-dependence. This would demand the adoption of what can be termed responsible transparency whereby both transparency is pursued under well-established limits that do not infringe on the sense of individual dignity and confidentiality is exercised in such manner that the institutions before the people are not placed in transparent waters. The process mainly relies on the enhancement of the level of public awareness and legal literacy as educated citizens stand a higher possibility to bargain their right to information and their right to privacy. The ultimate aim is to possess a harmonized scheme, which is a dynamic balance one that safeguards personal data without reducing the visibility, and transparency without reducing privacy, therefore, keeping the governance responsible and rights-based in a more sophisticated, data-intensive society.

References

- Bhatia, G. (2019). *The transformative constitution: A radical biography in nine acts*. HarperCollins India.
- Brin, D. (1998). *The transparent society: Will we have to decide between privacy and freedom due to technology?* Perseus Books.
- Carey, P. (2020). *Data protection: A practical guide to UK and EU law (5th ed.)*. Oxford University Press.
- Central Board of Secondary Education v. Aditya Bandopadhyay, (2011) 8 SCC 497.
- De, R. (2018). *The everyday life of law in the Indian republic: A people constitution*. Princeton University Press.
- Florini, A. (Ed.). (2007). *The right to know: Openness to a transparent world*. Columbia University Press.
- Government of India. (2005). *The right to information Act, 2005*.
- Government of India. (2023). *The Digital Personal Data Protection Act, 2023*.
- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.



Matthan, R. (2018). *The privacy 3.0: Opening up our data-driven future*. HarperCollins India.

Ministry of Education. (2023). *Commentary on the Digital Personal Data Protection Act, 2023*. Government of India.

Solove, D. J. (2021). *Understanding privacy*. Harvard University Press.

Srikrishna Committee. (2018). *Free and fair digital economy: Safeguard privacy, empower Indians*. Government of India.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193–220.

Westin, A. F. (1967). *Privacy and freedom*. Atheneum.

Publisher's Note: *The views and opinions expressed in this article are solely those of the author(s) and do not necessarily reflect those of the publisher, editors, or the editorial board.*