INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY

VOLUME 3 AND ISSUE I OF 2025

APIS – 3920-0012 | ISSN - 2583-7990

Published by

Institute of Legal Education

https://iledu.in

REIMAGINING TRANSPARENCY IN THE DIGITAL AGE: THE RIGHT TO INFORMATION ACT, 2005 AND THE CHALLENGES OF AI, ICT, AND E-GOVERNANCE

AUTHOR - MR. GANESH SHRIRANG NALE SATARKAR, M.A. SOCIOLOGY, 2ND YEAR, DEPARTMENT OF SOCIOLOGY, CENTRAL UNIVERSITY OF HARYANA.

BEST CITATION *- MR. GANESH SHRIRANG NALE SATARKAR, REIMAGINING TRANSPARENCY IN THE DIGITAL AGE: THE RIGHT TO INFORMATION ACT, 2005 AND THE CHALLENGES OF AI, ICT, AND E-GOVERNANCE, INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY, 3 (1) OF 2025, PG. 61-66, APIS – 3920-0012 | ISSN - 2583-7990*

Abstract

The *Right to Information Act, 2005* (RTI Act) symbolises India's transition from administrative opacity to democratic accountability. Over the past two decades, it has empowered citizens to hold public institutions answerable. Yet the rapid expansion of digital governance—driven by Information and Communication Technology (ICT), Artificial Intelligence (AI), and automation—has transformed how information is created, stored, and accessed. While these technologies can strengthen proactive disclosure and efficiency, they also raise complex challenges concerning privacy, cybersecurity, algorithmic bias, and equitable access.

This paper critically evaluates India's RTI framework within the context of digital transformation. It argues that existing institutions must adapt to an environment where governance data are mediated by digital infrastructures and algorithmic systems. The study uses a policy-research lens to examine statutory provisions, administrative practice, and case law, and proposes reforms aimed at building a digitally resilient and citizen-centric transparency regime. The paper concludes that sustaining India's "right to know" in the age of digital governance requires harmonising openness with technological accountability and data protection.

Keywords: RTI Act, Digital Governance, Artificial Intelligence, Cybersecurity, Data Protection, Policy Reform.

1. Introduction

Transparency is a foundational value of democratic governance. The framers of the *Constitution of India* embedded accountability within the constitutional scheme through Article 19(1)(a), which guarantees freedom of speech and expression. Judicial interpretation gradually expanded this freedom to include the *right to know*—a right that became concretised with the passage of the *Right to Information Act, 2005*.[1] The Act revolutionised citizen-state relations by institutionalising access to government-held information. However, governance in India is no longer confined to paper files or physical offices. Digitalisation has redefined how public authorities generate, store, and communicate information. Ministries maintain electronic records, decision-making is increasingly data-driven, and service delivery is mediated by AI-enabled platforms. This shift poses a central policy question: *Can the RTI framework remain effective when information itself is digitised, automated, and algorithmic?* The digital era brings dual possibilities. On one hand, ICT tools can improve proactive disclosure, streamline record management, and make citizen interaction frictionless. On the other, technological opacity, cybersecurity threats,

and privacy concerns may erode the very transparency RTI was designed to protect. The paper therefore analyses RTI's interface with digital governance to determine how legal and institutional reforms can sustain transparency in a technological age.

2. Evolution of the Right to Information in India

2.1 Pre-Legislative Foundations

India's transparency movement originated from grassroots struggles rather than top-down policy. The *Mazdoor Kisan Shakti Sangathan (MKSS)* in Rajasthan pioneered demands for public access to wage rolls and development accounts during the 1990s. Their campaign for *jan sunwais* (public hearings) demonstrated that information is a tool for social justice.[2] Civil-society activism gradually pushed state governments—Rajasthan, Tamil Nadu, and Delhi—to adopt limited right-to-information laws prior to 2005.Judicial pronouncements reinforced this trajectory. In *State of U.P. v. Raj Narain*[3] and *S.P. Gupta v. Union of India*,[4] the Supreme Court declared that citizens have a right to know about the functioning of government. These cases laid the constitutional groundwork for an enforceable right to information.

2.2 The RTI Act, 2005

The *RTI Act, 2005* institutionalised this right at the national level. It established Central and State Information Commissions, empowered citizens to seek information from public authorities, and imposed proactive disclosure obligations under Section 4. The preamble explicitly links transparency to democracy, declaring that the Act is meant "to contain corruption and to hold Governments and their instrumentalities accountable." Over two decades, the RTI Act has produced measurable impacts. Millions of citizens file RTI applications annually; investigative journalists rely on it to expose corruption; and marginalized groups use it to claim entitlements. Nevertheless, problems persist—backlogs, inconsistent implementation, and lack of awareness continue to weaken the system. The emergence of *Digital India* and e-Governance adds a new layer of complexity. Whereas the RTI framework was designed for a paper-based bureaucracy, governance today operates through databases, dashboards, and AI-assisted decision engines. Translating the Act's principles into this new environment is the challenge that the following sections address.

[41]3. The Digital Turn in Governance: Opportunities and Challenges

The launch of the *Digital India Mission* in 2015 marked a transformative moment in Indian public administration. By integrating information and communication technologies (ICT) into every tier of government, the initiative sought to create a digitally empowered society and knowledge economy.[1] Ministries, municipal bodies, and public-sector undertakings were encouraged to digitise records, migrate to online service platforms, and adopt cloud-based data systems. For the *Right to Information* regime, this digital shift presents both opportunity and risk. On the one hand, digitisation reduces physical barriers to information: citizens can file RTI applications online, access dashboards, and track responses in real time. Portals such as *RTI Online* of the Department of Personnel and Training (DoPT) and state-level systems in Maharashtra, Kerala, and Rajasthan demonstrate how e-governance can enhance procedural transparency.[2] Machine-readable datasets, once properly structured, also facilitate proactive disclosure under Section 4(2) of the Act.

On the other hand, the very technologies that enable openness may create new forms of opacity. Algorithms filter data, metadata may be withheld for "security" reasons, and proprietary software can conceal administrative logic. Furthermore, the "digital divide"—inequalities of connectivity, language,

[41] Constitution *of India*, Art. 19(1)(a).
Aruna Roy and Nikhil Dey, *The Right to Know: A Grassroots Perspective* (2001) Economic and Political Weekly 1550.
State of U.P. v. Raj Narain, AIR 1975 SC 865.
S.P. Gupta v. Union of India, AIR 1982 SC 149

and digital literacy—excludes large sections of rural India from effective participation.[3] True transparency must therefore be *inclusive* transparency. Finally, while electronic governance reduces discretion in information delivery, it simultaneously increases dependence on private contractors and cloud vendors for data storage. The absence of robust public-sector data-governance standards exposes the RTI framework to vulnerabilities such as data loss, unauthorised access, and cybercrime.

4. Artificial Intelligence, ICT, and Algorithmic Transparency

Artificial Intelligence (AI) is now deployed across Indian public institutions—from predictive policing to welfare-benefit targeting. When decisions affecting citizens are made by algorithmic systems, the need for transparency acquires a new dimension. Traditional RTI questions ("Who took this decision?" "On what file?") no longer suffice; citizens must also know *how* an algorithm arrived at its conclusion.

4.1 Potential of AI for RTI Administration

AI can dramatically improve the efficiency of the information regime. Natural-language chatbots may respond to routine RTI queries; pattern-recognition tools can identify frequently requested information and prompt automatic disclosure; and machine-learning models can detect delays or bottlenecks in departmental responses.[4] The *Madhya Pradesh Public Service Guarantee Act* and the *Seva Sindhu Portal* of Karnataka illustrate early successes in automating grievance-redress and disclosure systems.

4.2 The Opacity Problem

However, algorithmic decision-making raises issues of *explainability* and *accountability*. Proprietary AI systems often operate as "black boxes," where neither administrators nor citizens can interpret the model's reasoning. This conflicts with the spirit of Section 4 of the RTI Act, which mandates intelligible disclosure.[5] When a citizen requests "reasons" for an algorithmic classification—say, rejection of a subsidy application—officials must have technical competence to extract and communicate that reasoning. Without legal standards on *algorithmic transparency*, RTI's promise of participatory governance remains unfulfilled.

4.3 Institutional Response

India currently lacks a dedicated policy on transparency of public-sector algorithms. The *NITI Aayog's Responsible AI* framework (2021) recognises explainability as an ethical principle but provides no enforceable obligations. Integrating such standards into the RTI framework—either through amendment or subordinate legislation—would ensure that automated governance remains auditable and rights-compliant.

5. Cybersecurity and Data Protection: Reconciling Privacy with Transparency

Digitisation inevitably increases the quantity of sensitive data in government custody. The *RTI Act, 2005* protects privacy through Section 8(1)(j), exempting personal information unless disclosure serves an overriding public interest. The Supreme Court's ruling in *Central Public Information Officer, Supreme Court of India v. Subhash Chandra Agarwal*[6] balanced the citizen's right to know with informational privacy under Article 21 of the *Constitution*.

5.1 The Digital Personal Data Protection Act, 2023

The *Digital Personal Data Protection Act, 2023* (DPDPA) represents India's first comprehensive privacy law. It introduces consent-based processing, data-minimisation, and grievance-redress mechanisms. However, Section 44(2) of the DPDPA explicitly states that its provisions shall override inconsistent laws—potentially constraining RTI disclosure. Harmonisation is thus imperative: the two statutes must be read together to preserve transparency while safeguarding privacy.

5.2 Cybersecurity Imperatives

Government portals hosting RTI applications or proactive disclosures are frequent targets of

cyber-attacks. The *Indian Computer Emergency Response Team (CERT-In)* has reported multiple data breaches in public databases between 2021 and 2024.[7] Such incidents not only violate individual privacy but also undermine citizen confidence in e-governance. Policy measures should include mandatory encryption, regular vulnerability assessments, and appointment of dedicated cybersecurity officers within public authorities. The *Information Technology Act, 2000*, particularly Sections 43-A and 72, already provides a legal basis for data-security obligations; these provisions must be operationalised in the RTI context through government guidelines.[42]

6. E-Governance and Proactive Disclosure

6.1 Legal Mandate

Section 4(1)(b) of the RTI Act obliges every public authority to publish information on its functions, powers, procedures, and budgets at regular intervals. In the digital age, this requirement translates into online proactive disclosure. Portals such as *India Gov Portal* and the *Open Government Data (OGD) Platform* exemplify compliance.[8]

6.2 Implementation Gaps

Despite progress, compliance is uneven. Studies by the *Commonwealth Human Rights Initiative* reveal that over 40 per cent of central and state ministries fail to update disclosures annually.[9] Many websites lack search functionality, machine-readable formats, or regional-language interfaces. Moreover, the digital divide prevents marginalised communities from accessing online data.

6.3 The Way Forward

To strengthen proactive disclosure:

- **Standardisation:** The Department of Personnel and Training should issue uniform metadata standards and API formats.
- **Real-Time Updating:** Integration with departmental MIS dashboards can automate publication.
- **Accessibility:** Multilingual interfaces and text-to-speech options should be mandatory for inclusivity.
- **Periodic Audit:** Annual audits by Information Commissions should rate compliance publicly, creating positive competition among departments.

7. Policy Analysis and Recommendations

The following policy directions are proposed to secure RTI's future in the digital era:

7.1 Establish a Digital Transparency Commission

A statutory *Digital Transparency Commission (DTC)* should be constituted under the RTI Act to oversee algorithmic governance, ICT integration, and cybersecurity in information management. The DTC would set technical standards, certify AI systems used in public administration, and investigate violations of transparency norms.

7.2 Integrate RTI with Digital-Governance Architecture

The RTI Online portal must be synchronised with *DigiLocker*, *MyGov*, and *e-Office* systems, ensuring a single-window interface. Machine-readable open data should be released proactively through the *OGD Platform*, minimising individual RTI requests.

7.3 Capacity Building

Public Information Officers (PIOs) require technical training in ICT, data analytics, and cybersecurity. The *Lal Bahadur Shastri National Academy of Administration* and state training institutes should include digital-transparency modules in their curricula.

[42] Government of India, *Digital India Programme: Vision and Action Plan* (MeitY, 2015).
Department of Personnel and Training, *RTI Online Portal*, available at https://rtionline.gov.in (last visited 27 Oct 2025).
NASSCOM Foundation, *Bridging the Digital Divide in Rural India* (2022) 12.
Kiran Sharma, "AI in Public Service Delivery: A Transparency Perspective" (2023) 45 (3) *Indian Journal of Public Administration* 78.

7.4 Cyber-Resilience Framework

Every public authority should maintain a *Cyber-Resilience Plan* incorporating incident-response protocols, encryption standards, and periodic audits. Non-compliance should attract penalties under Section 20 of the RTI Act read with Section 43-A of the *Information Technology Act, 2000*.

7.5 Legislative Harmonisation

An amendment to the RTI Act may be considered to:

- Define "digital records" and "algorithmic decisions";
- Mandate publication of source-code summaries or decision logs for AI systems affecting citizens;
- Clarify the relationship between RTI and DPDPA to prevent excessive invocation of privacy exemptions.

7.6 Strengthening Information Commissions

Commissions must evolve from quasi-judicial forums into *knowledge regulators*. They should issue *transparency advisories* on emerging technologies, maintain databases of AI-related RTI appeals, and collaborate with technical universities for research.

7.7 Community Participation

Digital transparency must not alienate the citizen. Local bodies should organise "RTI Digital Clinics" to assist rural applicants in filing online requests. Civil-society partnerships can bridge the literacy gap and democratise technology use.

8. Conclusion

Twenty years after the *Right to Information Act, 2005*, India stands at a digital crossroads. The State's administrative apparatus now operates through data flows, cloud storage, and automated analytics. Transparency can no longer be confined to physical files; it must extend[43] into algorithms, code, and cyberspace.

This paper has demonstrated that while AI and ICT offer unparalleled tools for openness, they also threaten to reproduce opacity through complexity. The challenge is not technological inevitability but *institutional adaptation*. India's transparency regime must internalise digital ethics—fairness, accountability, and explainability—without abandoning inclusivity. A policy-driven synthesis of RTI, data protection, and digital-governance norms can ensure that the right to information remains the cornerstone of participatory democracy in the twenty-first century. The citizen's "right to know" must evolve into a *right to understand* how technology governs them.

References

- *Constitution of India*, Art. 19(1)(a) and 21.
- *Right to Information Act, 2005*.
- *Digital Personal Data Protection Act, 2023*.
- *Information Technology Act, 2000*.
- Department of Personnel and Training, *Guidelines for Proactive Disclosure under Section 4* (DoPT, 2021).
- Government of India, *National Cyber Security Strategy 2023* (MeitY, 2023).
- Supreme Court of India, *State of U.P. v. Raj Narain*, AIR 1975 SC 865.
- Supreme Court of India, *S.P. Gupta v. Union of India*, AIR 1982 SC 149.
- NITI Aayog, *Responsible AI for All: Operationalising Ethics and Trustworthy AI* (New Delhi, 2021).
- Aruna Roy & Nikhil Dey, *The Right to Know: A Grassroots Perspective* (2001) *EPW* 1550.

[43] *Right to Information Act, 2005*, s. 4(2).

Central Public Information Officer, Supreme Court of India v. Subhash Chandra Agarwal, (2019) 16 SCC 689.
Indian Computer Emergency Response Team (CERT-In), *Annual Cyber Security Report 2023* (New Delhi, 2024).
Government of India, *Open Government Data Platform (India)* (2020) available at https://data.gov.in.
Commonwealth Human Rights Initiative, *Proactive Disclosure Audit Report* (2023) 18.