

# Impact of the Digital Personal Data Protection Act, 2023 on Third-Party Information under the Right to Information Act, 2005: A Critical Analysis

**Mr. Dharmendra Kumar**

Research Scholar, School of Law and Governance, Central University of South Bihar

## Abstract

The Digital Personal Data Protection Act, 2023 (DPDP Act 2023) introduces a comprehensive digital data protection framework in India. This paper examines the Right to Information Act, 2005 (RTI Act, 2005) on the disclosure of third-party information. The RTI Act seeks to enhance transparency and accountability while allowing third-party access to information under certain conditions. The DPDP Act establishes strict consent and data processing regulations. The DPDP Act, 2023 aims to safeguard personal data and govern its processing to provide data protection, potentially limiting such disclosures.

This paper examines the conflicts between the personal data protection established by the DPDP Act and the RTI Act, emphasizing critical clauses, legal interpretations, and practical issues. The DPDP Act enhances personal data protections but may unintentionally compromise transparency by limiting access to third-party data: hence, it requires a coordinated strategy to balance these conflicting rights. The study concludes with suggestions for legislative clarity and procedural mechanisms to ensure the effective coexistence of both laws within India's developing digital landscape.

**Keywords:** Digital Personal Data Protection Act, Right to Information Act, Third-party information, Privacy, Transparency, accountability, Consent and Public interest.

## 1. Introduction

India is not going behind in the global surge of digitalization. The rapid digitalization in India has transformed the processing, storage, and sharing of personal data, prompting significant concerns around transparency and privacy. India is not going behind in the global surge of digitalization. Rapid digitalization in India has changed the way personal data is processed, stored, and shared, raising serious concerns about transparency and privacy. The DPDP Act, 2023, marks an important innovation in India's data protection landscape, establishing a comprehensive framework to safeguard personal data while balancing the need for lawful data processing.<sup>1</sup> Enacted on August 11, 2023, following the landmark Supreme Court ruling in *Justice K.S. Puttaswamy v. Union of India* (2017), which recognized privacy as a fundamental right under Article 21, the constitution of India. The DPDP Act responds to the growing need for robust data privacy regulations in an era of increasing digital transactions (Supreme Court of

---

<sup>1</sup> The Digital Personal Data Protection Act, 2023 (Act 22 OF 2023).

India, 2017).<sup>2</sup> Conversely, the RTI Act, 2005 has been a cornerstone of India's commitment to transparency, empowering citizens to access information held by public authorities, including third-party information, subject to specific exemptions.<sup>3</sup> However, the interplay between these two legislations, particularly the DPDP Act's amendment to Section 8(1)(j) of the Right To Information Act, 2005 introduces potential conflicts between privacy and the public's right to know (PRS Legislative Research, 2023).<sup>4</sup> This tension is especially pronounced in the context of third-party information, where personal data disclosure under the RTI Act may now be restricted under the broader ambit of the Digital Personal Data Protection Act, 2023.

## 2. Overview of the DPDP Act, 2023, and the RTI Act, 2005

The significance of this research lies in critically analyzing how the DPDP Act's privacy-centric framework impacts the disclosure of third-party information under the Right To Information Act. As India navigates its digital transformation, understanding the balance between their rights to privacy and public transparency is crucial for policymakers, legal practitioners, and citizens. This study aims to address the legal, ethical, and practical implications of this intersection, offering insights into harmonizing these fundamental rights in a democratic society.

## 3. Definition and relevance of third-party information under RTI

Under the RTI Act, third-party information refers to information relating to an individual or organization distinct from the requester or the public authority, including personal data such as names, addresses, or other identifiable details. The RTI Act, Section 11 governs the disclosure of third-party information, requiring public authorities to notify the third party and consider their objections before disclosure, providing under the provision Section 8 of Right to Information Act, 2005 the information is not exempt.<sup>5</sup> The relevance of third-party information lies in its frequent involvement in RTI requests, such as those seeking details about government officials, beneficiaries of public schemes, or private entities contracted by public authorities. The amendment to Section 8(1)(j) of the DPDP Act's may limit such disclosures by prioritizing privacy, raising questions about the balance between transparency and data protection<sup>6</sup>.

## 4. Objectives of the study

Analyze the interplay between the Right to Information Act, 2005 and the Digital Personal Data Protection Act, 2023 focusing on the impact of the Digital Personal Data Protection Act's amendment to Section 8(1)(j) on the disclosure of third-party information.

Evaluate the regulatory and practical implications of reconciling personal data rights under the DPDP Act with the public's right to information under the RTI Act.

Assess the effectiveness of the DPDP Act's framework in protecting third-party personal data while ensuring transparency in governance.

Propose suggestions for harmonizing the two legislations to balance their personal privacy with public interest in accessing third-party information.

<sup>2</sup> Justice K.S. Puttaswamy v. Union of India, AIR 2017 SC 4161

<sup>3</sup> The Right to Information Act, 2005 (Act 22 of 2005), s.1.

<sup>4</sup> The Digital Personal Data Protection Bill, 2023(Bill No. 113 of 2023).

<sup>5</sup> The Right to Information Act, 2005 (Act 22 of 2005), ss. 8, 11.

<sup>6</sup> Saumya Tripathi and Ashish Srivastava. "Existence And Misuse Of Section 8 Of The RTI Act: A Critical Analysis." *Indian Journal Of Integrated Research In Law* 5 (2025).

## 5. Research Methodology

This study adopts a doctrinal legal research methodology to critically investigate the impact of the DPDP Act, 2023 on third-party information disclosures under the Right to Information Act, 2005. The methodology focuses exclusively on analyzing legal texts, judicial precedents, and authoritative secondary sources to address the study's objectives: analyzing the interplay between the two acts, evaluating legal implications, assessing the DPDP Act's effectiveness, and proposing suggestions for harmonizing privacy and transparency. The methodology is structured around a qualitative and analytical approach, systematic data collection, and a comparative study, ensuring a rigorous and coherent doctrinal investigation.

## 6. Overview of the DPDP Act, 2023.

The DPDP Act 2023, adopted on August 11, 2023, represents India's first extensive law to regulate the digital individuals data processing, establishing a robust framework to safeguard privacy in an increasingly digitalized society.<sup>7</sup> Promulgated in response to the SC historical case *Justice K.S. Puttaswamy v. U.O.I.*, which established the right to privacy as a fundamental right under Article 21 of the Constitution of India, the Act addresses the urgent need for data protection amidst India's digital transformation.<sup>8</sup> Its relevance to this study lies in the RTI Act, 2005 its amendment to Section 8(1)(j), which significantly impacts the disclosure of third-party information, a key focus of the research.<sup>9</sup> This overview details the Act's key provisions, mechanisms for protecting personal data and associated exemptions, and the data principles and rights of individuals, providing a foundation for analyzing its interplay with the RTI Act.

## 7. Key provisions of the DPDP Act, 2023.

The DPDP Act establishes a structured regulatory framework for data protection, introducing definitions, obligations, enforcement mechanisms, and amendments that shape India's privacy landscape. The following are its core provisions:

**Scope and Applicability:** The Act deals with the process of managing of digital personal data within India, including data collected online or digitized from offline sources, and extends to data processed outside India if it involves offering services or goods to Indian residents.<sup>10</sup> Personal data is defined as any information relating to an identified or identifiable individual, such as names, addresses, or digital identifiers.<sup>11</sup> The Act excludes non-digital data, publicly available data, and personal or domestic data processed for purposes.<sup>12</sup>

### Definitions:

*Data Principal:* The individual whose personal data is processed.<sup>13</sup>

*Data Fiduciary:* The entity (public or private) determining the means purpose of data processing, such as companies or government agencies.<sup>14</sup>

*Significant Data Fiduciary:* Entities established by the Central Government according to measures such as data volume, sensitivity, or societal impact, subject to improved compliance obligations.<sup>15</sup>

---

<sup>7</sup> *Supra* note 1.

<sup>8</sup> *Supra* note 2.

<sup>9</sup> *Supra* note 3.

<sup>10</sup> The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 3.

<sup>11</sup> The Digital Personal Data Protection Act, 2023 (Act 22 OF 2023) s. 2(t).

<sup>12</sup> The Digital Personal Data Protection Act, 2023 (Act 22 OF 2023) s. 2(c).

<sup>13</sup> The Digital Personal Data Protection Act, 2023 (Act 22 OF 2023) s. 2(j).

<sup>14</sup> The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 2(i).

<sup>15</sup> The Digital Personal Data Protection Act, 2023 (Act 22 OF 2023), s. 2(z).

*Data Processor*: An entity processing data on behalf of a Data Fiduciary.<sup>16</sup>

**Obligations of Data Fiduciaries**: Data Fiduciaries are required to secure voluntary, informed, explicit, and unambiguous consent for data processing, with clear notification to Data Principals.<sup>17</sup> They are required to ensure data accuracy, implement security safeguards, and erase data when its purpose is fulfilled or consent is withdrawn, unless retention is legally mandated.<sup>18</sup> Data Fiduciaries must also appoint a Data Protection Officer and the Data Protection Board notify data breaches to affected Data Principals.

**Data Protection Board of India**: The Act establishes an independent adjudicatory body, the DPB, to enforce compliance, investigate breaches, and mediate disputes.<sup>19</sup> The Board can impose up to INR 250 crore penalties for violations, such as failure to secure data or obtain consent.<sup>20</sup>

**Amendment to the Right to Information Act**: Section 44(3) of the DPDP Act updates Section 8(1)(j) of the Right To Information Act, which used to exempted individual information from publication unless it benefited a broader public interest.<sup>21</sup> The amendment reduces individuals advantage, allowing public authorities to deny RTI requests involving personal data unless consent is obtained or disclosure is legally permitted, significantly impacting third-party information disclosures.<sup>22</sup>

**Penalties and Remedies**: Non-compliance, such as unauthorized data processing or failure to report breaches, attracts penalties from INR 10 crore to INR 250 crore ranging, depending on the violation's severity.<sup>23</sup> Data Principals can seek remedies through the Data Protection Board, with appeals lying to the Telecom Disputes Settlement and Appellate Tribunal.<sup>24</sup>

These provisions collectively aim to regulate data processing while balancing privacy with legitimate uses, but the RTI amendment raises concerns about transparency, a key issue for this study.

### Protection of Personal Data and Exemptions

The DPDP Act prioritizes the protection of personal data through stringent obligations and safeguards, while providing exemptions for specific purposes to ensure practical implementation.

#### Protection Mechanisms:

**Consent Framework**: Data processing requires explicit consent from Data Principals, obtained through a clear and accessible notice detailing the purpose, data type, and rights.<sup>25</sup> Consent can be withdrawn at any time, triggering data erasure obligations unless retention is legally required.

**Security Safeguards**: Data fiduciaries are required to establish both technological and organizational safety measures to avoid data breaches, including encryption and access restrictions.<sup>26</sup> In case of a breach, they must the DPB notify and affected Data Principals promptly.<sup>27</sup>

<sup>16</sup> The Digital Personal Data Protection Act, 2023(Act 22 OF 2023), s. 2(k).

<sup>17</sup> The Digital Personal Data Protection Act, 2023(Act 22 OF 2023), s. 6.

<sup>18</sup> The Digital Personal Data Protection Act, 2023(Act 22 OF 2023), s. 8(3), (7).

<sup>19</sup> Chaisse Julien, "Arbitration in cross-border data protection disputes" *Journal of International Dispute Settlement* 15 (2024).

<sup>20</sup> The Digital Personal Data Protection Act, 2023(Act 22 OF 2023), s. 33.

<sup>21</sup> Supra note 36.

<sup>22</sup> Supra note 4.

<sup>23</sup> Supra note 20.

<sup>24</sup> R. U. S. Prasad, "Resolving Disputes in Telecommunications: Global Practices and Challenges" Oxford University Press, (2010).

<sup>25</sup> The Digital Personal Data Protection Act, 2023, s. 6(1).

<sup>26</sup> The Digital Personal Data Protection Act, 2023, s. 8(5).

<sup>27</sup> Id. s. 8(6).

**Data Accuracy and Minimization:** Fiduciaries must ensure data is accurate and limit collect data to what is necessary for the specified purpose, reducing privacy risks.<sup>28</sup>

**Accountability:** Significant Data Fiduciaries must conduct data security Effect Investigations and appoint Data Protection Officers to ensure compliance.<sup>29</sup> The Data Protection Board enforces accountability through inspections and penalties.<sup>30</sup>

**Exemptions:**

**State Functions:** The Central Government can exempt state agencies from certain provisions for purposes like national security, public order, or prevention of offenses, subject to safeguards prescribed by rules.<sup>31</sup>

**Specified Purposes:** Exemptions apply for judicial proceedings, research, statistical analysis, or journalistic purposes, provided processing does not harm Data Principals' rights.<sup>32</sup>

**Public Interest:** Certain provisions may be relaxed for mergers, acquisitions, or credit assessments, balancing commercial needs with privacy protections.<sup>33</sup>

**Children's Data:** While the Act imposes stricter consent requirements for children (under 18), exemptions allow guardians to consent on their behalf.<sup>34</sup>

These protections strengthen privacy but may conflict with the RTI Act's transparency goals, particularly when third-party personal data is sought, as exemptions under the DPDP Act could limit disclosures previously permitted under the RTI Act.

## 8. Data Principles and Rights of Individuals

The DPDP Act, 2023 establishes a robust framework for data safeguard, grounded in core principles and individual rights that align with worldwide standards like the European Union's GDPR<sup>35</sup>, significantly impacting third-party information disclosures under the Right to Information Act, 2005. principles-lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality and accountability<sup>36</sup> ensure ethical data processing, requiring Data Fiduciaries to process personal data lawfully, communicate clearly with Data Principals about data use limit collection to specified purposes, ensure accuracy, erase data when no longer needed or consent is withdrawn required, implement security measures, and remain accountable to the Board.<sup>37</sup> Complementing these principles, the DPDP Act grants Data Principals significant rights to access details about their data's purpose, recipients and processing to correct inaccurate or incomplete the rights data to erasure when data is no longer needed or consent is withdrawn, the right to limited processing in cases like disputed accuracy, the right to nominate a representative for exercising rights in cases of death or incapacity and the grievance redressal right to through Data Fiduciaries or the Data Protection Board.<sup>38</sup> These principles and rights permit persons to control their personal information, in accordance with GDPR's emphasis on individual

<sup>28</sup> Id. S. 8(3).

<sup>29</sup> Id. S. 10(2).

<sup>30</sup> Id. 19.

<sup>31</sup> The Digital Personal Data Protection Act, 2023, s. 17(1)

<sup>32</sup> Id. S. 17(2).

<sup>33</sup> Id. S. 17(3).

<sup>34</sup> Id. S. 9.

<sup>35</sup> Paul Voigt and Vondem Bussche Axel (ed.), *The general data protection regulation (GDPR) A practical guide, 1st ed*, Cham, (Springer International Publishing, 2017).

<sup>36</sup> Perera, Harsha, et al. "Towards integrating human values into software: Mapping principles and rights of GDPR to values." *27th international requirements engineering conference*, (2019).

<sup>37</sup> Supra note 4.

<sup>38</sup> Supra note 20.



autonomy.<sup>39</sup> However, their application to third-party information under the Right to Information Act, 2005 creates significant challenges, as the right to erasure or restriction may prevent public authorities from disclosing personal data sought through RTI requests, even when public interest previously justified disclosure under the RTI Act's framework. For instance, if a third party exercises their right to erasure, data critical to public accountability may be withheld, undermining the RTI Act's transparency objectives, as argued.<sup>40</sup> This tension, exacerbated by the DPDP Act's amendment to the Right to Information Act's Section 8(1)(j), which removes the public interest test, necessitates a critical analysis to harmonize privacy protections with the RTI Act's goal of fostering open governance, a core focus of this study.<sup>41</sup>

### Third-Party Information and the RTI Act, 2005

The RTI Act, 2005 promotes openness by allowing citizens to access details held by governmental authorities, including third-party information, subject to exemptions.<sup>42</sup> Third-party information, defined under Section 2(n) as data relating to an individual or organizations other than the requester or public authority, is critical in RTI requests concerning government officials, scheme beneficiaries, or contracted entities.<sup>43</sup> This section examines the RTI Act's provisions, judicial interpretations, and the impact of the DPDP Act, 2023 on third-party disclosures.

Section 8(1)(j) of the Right to Information Act, 2005 exempts individuals information from disclosure if it has no public interest or would cause an unjustified breach of privacy, unless the public interest outweighs privacy concerns.<sup>44</sup> Section 11 governs third-party information, requiring public authorities to notify the third party and consider their objections before disclosure, provided the under Section 8 is not exempt information.<sup>45</sup> These provisions balance transparency with privacy, ensuring third-party data is disclosed only when justified, such as in cases of public accountability.<sup>46</sup>

### Conditions for Sharing Third-Party Data under RTI

Third-party data can be shared under the Right to Information Act if (i) the requester demonstrates a public interest, (ii) the information is not exempt under Section 8(1)(j), and (iii) the third party, after notification under Section 11, does not object or their objection is overruled by the public interest.<sup>47</sup> For example, details of public officials' assets or scheme beneficiaries may be disclosed if they serve transparency, but personal details like addresses or medical records are typically protected unless public interest is compelling.<sup>48</sup>

Judicial interpretations have shaped the application of Sections 8(1)(j) and 11. In *G. R. D v. Central Information Commissioner* (2013), the Supreme Court held that personal information, such as an official's service records, is exempt unless public interest is clearly established.<sup>49</sup> Similarly, *R.K. Jain v. U.O.I* (2013) clarified that third-party information requires a public interest justification, reinforcing privacy

<sup>39</sup> Vrinda Bhandari and Faiza Rahman, "Constitutionalism during a crisis: the case of Aarogya Setu *Coronavirus Pandemic: Lessons and Policy Responses* Uma Kapila ed. (Academic Foundation, New Delhi, 2020) (2020).

<sup>40</sup> P. Arun, "Beyond Citizen Oversight Problems with the Trade-off between Transparency and Privacy" *Economic & Political Weekly*, (2025).

<sup>41</sup> The Right to Information Act, 2005 (Act of 2005), s. 8(1)(j).

<sup>42</sup> The Right to Information Act, 2005 (Act of 2005), s. 3.

<sup>43</sup> The Right to Information Act, 2005 (Act of 2005), s. 2).

<sup>44</sup> Id s. 8(1)(j).

<sup>45</sup> The Right to Information Act, 2005 (Act of 2005), s.11.

<sup>46</sup> Banisar David. "The right to information and privacy: balancing rights and managing conflicts." *World Bank Institute Governance Working Paper* (2011).

<sup>47</sup> The Right to Information Act, 2005 (Act of 2005) ss. 8(1)(j), 11.

<sup>48</sup> The Right to Information Act, 2005 (Act of 2005) s. 11(1).

<sup>49</sup> *Girish Ramchandra Deshpande v. Central Information Commissioner*, (2013) 1 SCC 212, para 13.

protections.<sup>50</sup> These rulings have strengthened transparency by ensuring disclosures serve public accountability but have also limited access to personal data, setting a high threshold for public interest.

### **Impact of the DPDP Act, 2023 on Third-Party Information under RTI**

The DPDP Act, 2023, introduces stringent privacy protections that significantly affect third-party information disclosures under the RTI Act.

### **Restrictions on Disclosure of Personal and Sensitive Personal Data**

Section 44(3) of the DPDP Act amends Section 8(1)(j) of the RTI Act, removing the public interest test and prohibiting disclosure of personal data without consent or legal authorization.<sup>51</sup> Personal data, defined as any information identifying an individual, includes sensitive data like financial or health records.<sup>52</sup> This amendment restricts public authorities from disclosing third-party data sought via RTI, even in cases previously justified by public interest, prioritizing privacy over transparency.<sup>53</sup>

### **Balancing Privacy with Public Interest**

The DPDP Act's emphasis on consent, reduction of data, and removal rights increases individual privacy but contradicts the RTI Act's public interest framework.<sup>54</sup> For instance, a Data Principal's right to erasure under Section 12 may prevent disclosure of third-party data, even if it pertains to public functions.<sup>55</sup> This shift undermines the RTI Act's objective of fostering accountability, as public interest no longer overrides privacy concerns.<sup>56</sup> Balancing these rights requires clear guidelines on when privacy exemptions apply, a key focus of this study.

### **Challenges in Ensuring Government Accountability**

The DPDP Act's restrictions complicate government accountability, as third-party data (e.g., details of officials or contractors) is often sought to expose corruption or mismanagement.<sup>57</sup> The amended Section 8(1)(j) may enable public authorities to deny such requests, reducing transparency in governance.<sup>58</sup> RTI activists, like Anjali Bhardwaj, argue that this amendment risks eroding the RTI Act's efficacy, particularly for marginalized communities seeking accountability.<sup>59</sup>

### **Conflicts with RTI Objectives**

The DPDP Act's privacy-centric framework conflicts with the RTI Act's transparency goals. While the RTI Act mandates disclosure to promote open governance, the DPDP Act's consent and exemption provisions limit access to third-party data.<sup>60</sup> For example, Section 17 of the DPDP Act exempts state agencies for national security, potentially broadening non-disclosure grounds under RTI. This conflict necessitates harmonization to preserve both rights.<sup>61</sup>

### **Judicial Precedents and Legal Interpretations**

<sup>50</sup> *R.K. Jain v. Union of India*, (2013) 14 SCC 794, para 25.

<sup>51</sup> The Digital Personal Data Protection Act, 2023 (Act of 2023) s. 44(3).

<sup>52</sup> The Digital Personal Data Protection Act, 2023 (Act of 2023) s. 2(t).

<sup>53</sup> The Digital Personal Data Protection Bill, 2023: Bill Summary 5 (2023).

<sup>54</sup> The Digital Personal Data Protection Act, 2023 (Act of 2023) ss. 6, 12.

<sup>55</sup> The Digital Personal Data Protection Act, 2023 (Act of 2023) s 12.

<sup>56</sup> Supra note 40.

<sup>57</sup> Usman Noval, "Legal Protection of Personal Data and Authority Accountability For Cyber Security: PDP Law Review" 10 *Law Research Review Quarterly* (2024).

<sup>58</sup> Pranshu Vats, "The Dark Side of Transparency: An Analysis of Misuse of Section 8 (1)(A) of The RTI Act." (2023).

<sup>59</sup> Venkat Vidya, "India's Democratic Revolution" *Diss. University of London*, (2024).

<sup>60</sup> Sh. Manoj Roy Sarkar, "The Evolving Landscape of Digital Privacy in India: Balancing Innovation and Data Protection by the Government", *International Centre for Information Systems and Audit*, (2024).

<sup>61</sup> Supra note 31.

Judicial rulings have been pivotal in navigating privacy versus transparency. In *Justice K.S. Puttaswamy v. Union of India* (2017), the Supreme Court recognized privacy as a fundamental right, influencing stricter interpretations of Section 8(1)(j).<sup>62</sup> *Girish Ramchandra Deshpande* (2013) and *Canara Bank v. C.S. Shyam* (2017) emphasized that personal information requires a strong public interest justification for disclosure.<sup>63</sup> Post-DPDP Act, courts may further prioritize privacy, potentially limiting RTI disclosures, as the amended Section 8(1)(j) aligns with *Puttaswamy*'s privacy framework.<sup>64</sup>

### Challenges and Future Implications

The DPDP Act's broad privacy exemptions and lack of clear guidelines on balancing RTI disclosures create legal uncertainties.<sup>65</sup> For instance, the absence of a public interest test in the amended Section 8(1)(j) leaves public authorities with discretionary power, risking inconsistent application.<sup>66</sup>

To align the DPDP Act and Right to Information Act, amendments are needed to reinstate a nuanced public interest test or clarify exemptions for third-party data in public functions.<sup>67</sup> Such reforms would ensure transparency without compromising privacy.

### Role of Regulatory Bodies

The Data Protection Board, established under the Digital Personal Data Protection Act, must collaborate with the Central Information Commission to issue guidelines harmonizing privacy and transparency.<sup>68</sup> These bodies can mediate disputes and ensure consistent application of both laws, safeguarding democratic accountability.

### Conclusion

The DPDP Act's amendment to the Right to Information Act creates significant challenges by prioritizing privacy over transparency, particularly for third-party information disclosures. Policy gaps, such as the lack of a public interest test and vague exemptions, lead to legal uncertainties and inconsistent application, threatening the RTI Act's role in ensuring accountability.<sup>18</sup> Legislative amendments to reinstate a balanced public interest test or clarify exemptions are crucial to align the two frameworks. The Data Protection Board and Central Information Commission must collaborate to issue guidelines and mediate disputes, ensuring consistent and fair application of both laws. This study seeks to address these challenges by proposing solutions to harmonize privacy and transparency, contributing to India's evolving legal framework for digital governance and democratic accountability.

---

<sup>62</sup> Supra note 2.

<sup>63</sup> Supra note 24.

<sup>64</sup> Supra note 19.

<sup>65</sup> Dr. Pradip Kumar Kashyap, "Digital Personal Data Protection Act, 2023: A New Light into The Data Protection and Privacy Law In India" 2 *ICREP Journal Of Interdisciplinary Studies*, (2023).

<sup>66</sup> Supra note 19.

<sup>67</sup> Supra note 31.

<sup>68</sup> The Digital Personal Data Protection Act, 2023(Act of 2023), s. 19.