International Journal of Economic Practices and Theories (IJEPT)
ISSN:2247-7225
Volume 2025 Issue 1

Data Privacy and Implications for India's Online Dispute Resolution Economy

Akash Gupta[1*], Dr. Apoorva Dixit[2]

[1*]PhD Scholar, School of Law, GD Goenka University, Sohna, Haryana, India; akash.tnnls@gmail.com
[2]Associate Professor, School of Law, GD Goenka University, Sohna, Haryana, India; apoorva.dixit@gdgu.org

Abstract: With the rise of digitalization in the legal process, Online Dispute Resolution (ODR) has developed a role to play in the provision of accessible costing justice digitally and providing access to justice. More importantly, the challenge has presented itself to the ODR environment to now find balance between information protection as ODR platforms process vast amounts of personal and sensitive data with need for positive technical performance. This paper will look at how the legal framework of ODR is going to be affected with the coming of the Digital Personal Data Protection Act, 2023 (DPDP Act). The paper explores the DPDP Act's framework and guiding principles of legitimate permission, data minimization, purpose limitation, legal claims to be asserted, and user rights, before examining the implications for platforms, disputing parties, neutrals, and others involved in the ODR ecosystem. The paper highlights emerging issues regarding consent management, cross-border data flow, AI incorporating into dispute systems and deploying its services not as a legally appointed decision maker but as a data fiduciary to support procedural fairness. The paper sheds light on how advanced privacy regulations use tools like a privacy-by-design framework and Data Protection Impact Assessments to include security, accountability, and transparency in digital dispute processes. The paper advocates a privacy-focused ODR framework for India that preserves user trust while promoting innovation in dispute resolution by analyzing legal lacunae, real-life disputes, and policy implications. It concludes with specific recommendations on how to operationalize data security ideas into India's new on-line justice system.

Keywords: Online Dispute Resolution (ODR), Alternative Dispute Resolution (ADR), Data Protection, Privacy, Enforcement

I. Introduction

Online Dispute Resolution (ODR) is a way of resolving disputes on digital platforms without the necessity for courts in real-life settings by using technology in legal processes. ODR's promise of inexpensive, convenient, and meaningful justice particularly involving disputes in consumer, corporate, and employment sectors has led to its rising popularity in India.[1] At the same time, the risks to data privacy and information self-determination have risen as these platforms utilize more and more user data to help settle disputes; data such as transaction histories, personally identifiable information, communications, and documentary evidence.

Recent changes brought by the enactment of the Digital Personal Data Protection Act of 2023 (DPDP Act) have set India's data governance on a remarkable new path.[2] The DPDP Act governs data processors and data fiduciaries in their collection, processing, storage, and transfer of personal data in India on the basis of the Supreme Court's recognition of the basic right to privacy in Justice K.S. Puttaswamy (Retd.) v. Union of India.[3] The DPDP Act expressly governs legal-tech platforms, especially those that are engaged with dispute resolution, but its main thrust will be on the digital governance of administration and commerce.

The dual functions of ODR platforms providing fair and neutral resolution of disputes while also acting as stewards of sensitive user data are at the centre of this regulatory conflict. The majority of existing ODR solutions often lack solid data lifecycle governance, nor do they consider the DPDP Act's stipulations for informed consent,[4] purpose limitation[5]and data minimisation[6]. Further, starting with the DPDP Act that will apply to all use of AI and algorithmic tools in the area of digital justice, this sphere raises concerns of algorithmic bias, profiling, and opaque decision-making, AI will be present in the ODR landscape in various ways like virtual mediators, automated negotiating bots, predictive analytics tools, etc. From a consumer and data protection standpoint, the DPDP Act seeks to address some of these issues by establishing accountability and transparency in the use of tools and methods of justice.

This paper analyzes the DPDP Act's effects on the design, operation, and legal duties of India's ODR platforms. The paper also discussed how ready the platforms are for the privacy requirements of the Act, and highlights whether current practices are consistent with "privacy by design" concept informing modern data protection

1 SAMA, "Resolving Disputes Digitally," SAMA ODR, https://www.sama.live
2 The Digital Personal Data Protection Act, No. 22 of 2023, § 2, Acts of Parliament, 2023 (India)
3 *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India)
4 DPDP Act § 7 (requiring clear, specific, and informed consent from data principals)
5 Id. § 6(1)(b) (limiting processing to specific, lawful purposes)
6 Id. § 6(1)(c) (mandating minimization of data collection to what is necessary for the stated purpose)

laws. The paper considers the European Union's General Data Protection Regulation (GDPR) regime and how it regulates the EU's ODR procedures to provide comparative perspective. The paper uncovers policy hurdles, regulatory deficiencies, and best practices for the tension between digital justice and data privacy.
As India solidifies its role as a global hub for ODR, especially in cross-border commercial disputes, it will be crucial to assure users of fair decisions and secure data. Thus, the relationship between ODR and data privacy regulation is not merely of compliance; it is also intrinsically related to the legitimacy, dependence, and ethical foundation of future digital justice.

II. Legal Framework of India's Digital Personal Data Protection Act, 2023 (DPDP Act)

India's first comprehensive data privacy framework is the Digital Personal Data Protection Act, 2023. It requires that personal information can only be gathered and used for legitimate reasons, with informed consent, and in accordance with certain duties placed on data fiduciaries (those who gather and use data). Additionally, it establishes standards for data security, purpose limitation, storage restriction, and data minimization.

Data privacy, also known as information privacy, refers to the right of individuals to control how their personal information is collected, used, stored, and shared. It encompasses the ability of a person to determine for themselves when, how, and to what extent personal information about them is communicated to others. This includes data such as names, addresses, identification numbers, financial details, and online behaviors. The concept is rooted in the recognition of privacy as a fundamental human right in many jurisdictions, and is protected by a range of legal frameworks globally.[7]

Modern data privacy regimes, such as the EU General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act (DPDP Act), are built on foundational principles that guide the lawful and ethical handling of personal data.[8] Personal data must be processed lawfully, fairly, and in a transparent manner.[9] Individuals should be informed about how their data is being used, and organizations must ensure compliance with applicable laws. Data should only be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.[10] Only data that is necessary for the intended purpose should be collected and processed, reducing the risk of misuse or unauthorized access.[11] Personal data must be accurate and, where necessary, kept up to date. Inaccurate data should be rectified or erased without delay. Data should not be retained for longer than necessary for the purposes for which it was collected. Appropriate security measures must be implemented to protect personal data against unauthorized or unlawful processing, accidental loss, destruction, or damage. Data controllers are responsible for, and must be able to demonstrate, compliance with all data protection principles.[12]

III. DPDP Act and Online Dispute Resolution

The advent of the DPDP Act has brought a new framework governing the processing & the protection of the personal Data in India. However, a pertinent question that emerges in this context is whether disputes arising under the DPDP Act can be subject to arbitration or whether they fall exclusively within the jurisdiction of statutory authorities such as the Data Protection Board of India ("DPB")[13].
The DPB, a quasi-judicial body with the authority to decide violations of the Act, receive complaints, and administer sanctions, was established by the Central Government under Section 18[14] of the DPDP Act. Interestingly, the Act also encourages the use of ADR, or alternative dispute resolution. Legislative aim to

[7] JISA Softech, Digital Personal Data Protection Act 2023 vs. GDPR (2025), https://www.jisasofttech.com/blog/digital-personal-data-protection-act-2023-vs-gdpr/
[8] Latham & Watkins, India's Digital Personal Data Protection Act 2023 vs. the GDPR (2023), https://www.lw.com/thoughtLeadership/indias-digital-personal-data-protection-act-2023-vs-the-gdpr
[9] GDPR v India's DPDPA: Key Differences and Compliance Implications, LEGAL500 (2024), https://www.legal500.com/developments/thought-leadership/gdpr-v-indias-dpdpa-key-differences-and-compliance-implications/
[10] AZB & Partners, Indian Data Protection Law versus GDPR – A Comparison (2024), https://www.azbpartners.com/bank/indian-data-protection-law-versus-gdpr-a-comparison/
[11] Leegality, What is the difference between GDPR and DPDP Act? (2023), https://www.leegality.com/blog/what-is-the-difference-between-gdpr-and-dpdp-act
[12] Comparing GDPR and DPDPA, SECUREPRIVACY (2024), https://secureprivacy.ai/blog/comparing-gdpr-and-dpdpa
[13] Tarun Krishnakumar," Data Protection in India & Arbitration: Key Questions Ahead", Kluwer Arbitration Blog, 2019
[14] Digital Personal Data Protection Act,2023, § 18, No. 22 of 2023, Aug. 11, 2023 (India).

promote amicable resolution is indicated by Section 31[15]'s authority for the DPB to submit complaints to mediation. Nonetheless, the Act is silent on arbitration but specifically prohibits the jurisdiction of civil courts.

Under Indian law, arbitral tribunals are not regarded as "courts," and arbitral proceedings are not categorized as civil processes. One Therefore, there is no statutory restriction on using the DPDP Act to send conflicts to arbitration in the absence of an express ban and in light of established jurisprudence. Data privacy disputes can straddle both rights in rem and rights in personam. For instance, breaches of contractual data-processing agreements or confidentiality obligations primarily concern specific parties and thus pertain to rights in personam, rendering them arbitrable. However, where the violation implicates systemic issues or affects the data subject's rights broadly, such as unlawful mass data collection or failure to notify breaches, the dispute may acquire a public character, making arbitration unsuitable.
The arbitrability of data privacy disputes under the DPDP Act must be determined on a case-by-case basis, applying the Vidya Drolia test[16] to evaluate whether the dispute predominantly concerns private contractual rights or broader regulatory compliance and public interest.

IV. Challenges Related to ODR and DPDP Act

As India moves towards embracing technology-driven solutions in dispute resolution, Online Dispute Resolution has emerged as a prominent mechanism that promises efficiency, accessibility, and cost-effectiveness. However, this transition also brings forth a host of challenges, particularly in terms of safeguarding data privacy and complying with regulatory frameworks like the Digital Personal Data Protection Act, 2023. In this context, it is critical to examine how ODR affects data protection and informational privacy in India’s evolving legal ecosystem.
ODR refers to the use of digital platforms and tools such as video conferencing, AI-driven mediators, or automated negotiation interfaces to resolve disputes, often without the need for physical presence. Its growing appeal lies in its potential to bridge geographical distances and reduce judicial backlogs. However, as Orna Rabinovich-Einy highlights[17], ODR inherently alters the private-public nature of dispute resolution by facilitating digitization, storage, and possible dissemination of data that were traditionally confined to closed-door proceedings.
In India, while arbitration and mediation have conventionally been valued for their confidentiality, the online medium complicates this expectation. With the use of third-party platforms, cloud storage, automated tools, and real-time recordings, sensitive information often including financial, commercial, and personal data is at risk of exposure, misuse, or unauthorized sharing.
Arbitration and mediation, whether online or offline, necessarily involve the exchange of sensitive data contracts, identity documents, proprietary information, health records, financial data, etc. What makes ODR distinct, however, is that such data is now subject to digital transmission, storage, and processing[18] often on third-party platforms that may be located outside India. The involvement of multiple actors (such as digital service providers, cloud hosts, legal tech companies, and even AI mediators) complicates the enforcement of traditional confidentiality norms.
Further, unlike in-person ADR, ODR platforms often log metadata (e.g., IP addresses, timestamps, user actions), increasing the surface area for potential data leaks. In the absence of robust encryption, anonymization protocols, or clear access control, these vulnerabilities raise significant privacy concerns.
The arbitrators, arbitral institutions, and ODR platforms must comply with obligations under the DPDP Act, such as obtaining valid consent, limiting data processing, and ensuring data protection measures. Many Indian parties engage with international arbitration institutions (e.g., SIAC, ICC) which may host data overseas. The DPDP Act allows such transfers only to countries that the Indian government designates as permissible, creating compliance friction for international ODR. The Act doesn’t clearly talk about anonymization in dispute

[15] Digital Personal Data Protection Act,2023, § 31, No. 22 of 2023, Aug. 11, 2023 (India).
[16] (2021) 2 SCC 1
[17] Orna Rabinovich-Einy, Going Public: Diminishing Privacy in Dispute Resolution in the Internet Age, 7 VA. J.L. & TECH. 1 (Summer 2002).
[18] Trina Grillo, The Mediation Alternative: Process Dangers for Women, 100 YALE L.J. 1545 (1991); Richard Delgado et al., Fairness and Formality: Minimizing the Risk ofPrejudice in Alternative Dispute Resolution, 1985 WIS. L. REv. 1359.

resolution. But as Rabinovich-Einy points out, anonymity is an important part of informational privacy, especially when parties want to keep the very existence of the dispute or their identity hidden.

Even after the DPDP Act, India still doesn't have uniform rules for how ODR platforms should handle sensitive data. The Act gives broad rules on data protection, but it doesn't have any specific guidance for online dispute resolution. This creates a grey area for arbitrators and mediators, who aren't sure what counts as proper compliance. Confidentiality is a well-accepted principle in arbitration, but there's no single standard for digital security. For instance, if sensitive documents are sent over unsecured email or stored on unregulated platforms, that could easily go against the DPDP's security requirements.

Rabinovich-Einy also notes that online mediation — and ODR in general — tends to reduce privacy because of its transparency and reliance on third-party systems.[19] But that doesn't mean ODR and privacy can't go hand in hand. Instead, it shows the need to rethink privacy in a digital setting, where ODR platforms are designed with "privacy by default" built into their systems.[20]

Another gap is enforcement. The board responsible under the Act hasn't yet clarified its role in handling ODR-related violations. Until that happens, parties may not have effective remedies if there's a data breach during an ODR proceeding.

Looking at India's past record like the hacking of the SC website and leaks from various government platforms tells us or exposes the fragility of its digital infrastructure. Without strong cybersecurity norms, ODR proceedings are vulnerable to espionage, ransomware attacks, and unauthorized access.

V. Conclusion

ODR platforms should adopt privacy-enhancing technologies like end-to-end encryption, multi-factor authentication, and access logs. Information should be stored for minimal durations and only when necessary. Until statutory clarity emerges, parties should contractually mandate NDAs and data protection clauses with ODR service providers, particularly when handling third-party tools or funders. Arbitration Institutions like MCIA or Delhi International Arbitration Centre should create standardized privacy protocols aligned with the DPDP Act and require compliance from affiliated arbitrators and service providers. There needs to be a legislative amendments which could clarify the status of arbitrators and mediators under the DPDP Act and lay down sector-specific rules for data handling during dispute resolution. The proposed Arbitration Council of India (ACI) can serve as a regulatory and training authority to promote tech-compliant and privacy-centric ODR practices. There is considerable ambiguity surrounding the obligations of technological service providers with regard to confidentiality and data privacy. Therefore, it would be wise for parties to add confidentiality and non-disclosure clauses in their agreements with the technology service providers until the necessary clarity is obtained. In a similar vein, they might also favor including provisions pertaining to data storage and privacy. It is necessary that the DPDP Act includes framework for ODR. Many foreign arbitral institutions may be already adhering to global data privacy standards because of mandatory compliance with foreign data protection laws. However, enacting this law would also mandate the indigenous service providers to pay attention to data privacy concerns.

The transition to online dispute resolution is inevitable and even desirable but only if privacy is treated as a core design principle, not a peripheral concern. The DPDP Act provides a long-overdue legal backbone for protecting personal data, but its true effectiveness in the ODR context depends on thoughtful implementation, cross-sector collaboration, and anticipatory policymaking. As India aspires to become a global hub for arbitration, the confluence of technology, privacy, and justice must be navigated with both care and foresight.

[19] Orna Rabinovich-Einy, Going Public: Diminishing Privacy in Dispute Resolution in the Internet Age, 7 VA. J.L. & TECH. 1 (Summer 2002).

[20] Julien Chaisse,"Redefending Resolution in Data Disputes: Why Arbitration Hold the Key" Kluwer Arbitration Blog, 2023