INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW
An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 5 | Issue 4 | 2026 Art. 16

Privacy in the Portal: An Analysis of ODR Compliance Under the Digital Personal Data Protection Act, 2023

Shivanshu Pal
Research Scholar,
Faculty of Law, University of Lucknow

Recommended Citation
Shivanshu Pal, *Privacy in the Portal: An Analysis of ODR Compliance Under the Digital Personal Data Protection Act, 2023,* 5 IJHRLR 211-228 (2026).
Available at www.ijhrlr.in/current-issues/.

Privacy in the Portal: An Analysis of ODR Compliance Under the Digital Personal Data Protection Act, 2023

ABSTRACT

The rapid growth of the dispute resolution from the courtrooms towards digital platforms has caused a drastic change in the manner of dispute resolution of the litigants in India. It gives the rise of online Disputes Resolution popularly known as ODR. Online Dispute Resolution ("ODR") sites are exposed to vast quantities of personal, financial and sometimes even confidential information, and there are acute concerns about confidentiality, consent and informational self-determination. This article reviews privacy architecture in the context of ODR in India in the background of the Digital Personal Data Protection Act, 2023, and provides a background to the constitutional principles established by the Supreme Court in Justice K.S. Puttaswamy v. Union of India, and developed in subsequent cases. What it does do is explain the development of ODR mechanisms, highlight the main privacy concerns of digital adjudication and assess how well the obligations of the DPDP Act are attuned to the realities of arbitration, mediation and online negotiation. The article also provides the overview of the judiciary's contribution to digital privacy jurisprudence and argues that, notwithstanding the DPDP Act's enactment, ODR platforms in India continue to face significant compliance gaps relating to consent architecture, data minimisation, cross-border transfers, and algorithmic transparency. It concludes with a set of doctrinal and policy recommendations directed at regulators, ODR service providers, and the judiciary, with the aim of embedding privacy-by-design principles into the next generation of India's digital justice infrastructure.

KEYWORDS

ODR, DPDP Act, Privacy, Data Protection, Digital Justice, Online Arbitration, Online Mediation, Judiciary

I. INTRODUCTION

A. Rise of Online Dispute Resolution in India

Online Dispute Resolution describes a cluster of techniques negotiation, mediation, and arbitration conducted wholly or partly through digital

means, typically without the physical presence of the parties.[1]The rise of e-commerce, digital lending, and the government's push towards digital payment platforms in India generated a massive number of micro-disputes, many of which were of low value but occurred at high frequency, placing an added burden on traditional courts. In its 2021 policy paper, NITI Aayog noted that ODR provided a scalable solution to such a backlog, especially in disputes related to digital transactions where the underlying evidence was also digital in nature.[2]Thus, private platforms have been established everywhere, sometimes in collaboration with banks, fintech firms and e-commerce intermediaries, to adjudicate consumer grievances, arbitrate commercial disputes and more.

B. Digital Transformation of the Justice Delivery System

The COVID-19 pandemic also helped in giving institutional recognition to dispute resolution outside the physical courtroom, as the judiciary had also adopted virtual hearings, e-filing, and digital case management. The Department of Justice's Vision Document on Online Dispute Resolution (ODR) envisioned ODR as a complementary tool to court-annexed mediation centres, with the expectation of integration with private ODR services.[3] The merger of public and private digital justice systems creates a global flow of personal information, whether it be within cloud systems, video-conferencing applications, or on third-party case management software.

C. Privacy and Confidentiality Concerns in ODR Proceedings

Dispute resolution has always presupposed a degree of confidentiality, whether through the closed-door nature of arbitration or the without-prejudice character of mediation communications. The digitisation of these processes introduces new vectors of exposure: data in transit between parties and platforms, data at rest on third-party servers, and data shared with ancillary service providers such as payment gateways or translation services. Commentators have noted that the absence of uniform data governance standards across ODR providers leaves litigants without a consistent baseline of protection.[4] A more recent SSRN study specifically cataloguing privacy and confidentiality risks across Indian ODR platforms similarly found wide variation in disclosure

[1] Ethan Katsh& Janet Rifkin, Online Dispute Resolution: Resolving Conflicts in Cyberspace 9-14 (2001).
[2] NITI Aayog, Designing the Future of Dispute Resolution: The ODR Policy Plan for India 22-29 (2021).
[3] Department of Justice, Ministry of Law and Justice, Government of India, Vision Document on Online Dispute Resolution 4-7 (2021).
[4] Ujwala Uppaluri& Sandeep Menon, Online Dispute Resolution in India: Trends and Challenges, 4 Indian J.L. & Tech. 112, 116-19 (2021).

practices and an absence of standardised breach-notification protocols.[5]

D. Importance of Data Protection in Virtual Dispute Resolution

ODR platforms often deal with special information, such as financial information in financial disputes, health information in personal injury disputes, or family information in matrimonial disputes, which can have serious reputational and even physical implications if there is a data breach. The enactment of the DPDP Act, 2023 thus comes at an opportune time as it provides the first ever comprehensive legal instrument which can be directly applied by a regulator to this type of processing.[6]

E. Objectives of the Study

The purpose of this article is to first identify the constitutional and statutory underpinnings of privacy as they relate to ODR, to second identify specific privacy concerns that arise throughout the life cycle of an ODR proceeding, to third analyze the applicability and adequacy of the obligations under the DPDP Act to ODR service providers, and to fourth examine how the judiciary can serve as a tool to develop privacy standards relevant to digital adjudication, and to fourth propose a framework for compliance with the obligations under the DPDP Act that can reconcile the efficiency benefits of ODR with the constitutional and privacy rights to informational privacy.

II. CONSTITUTIONAL AND LEGAL FOUNDATIONS OF PRIVACY IN INDIA

A. Evolution of the Right to Privacy under the Indian Constitution

The journey of privacy as a constitutional value in India culminated in the nine-judge bench decision in Justice K.S. Puttaswamy v. Union of India, which unanimously held that the right to privacy is intrinsic to the right to life and personal liberty guaranteed under Article 21.[7] Justice Chandrachud's plurality opinion described privacy as a necessary condition for the meaningful exercise of other guaranteed freedoms, encompassing bodily autonomy, decisional privacy, and informational self-determination.[8]

B. Privacy as a Facet of Article 21

[5] Shashank Atreya, Online Dispute Resolution in India: Privacy and Confidentiality Concerns, SSRN Working Paper (2022) [author, title, and pinpoint to be verified by the author against the original SSRN listing].
[6] The Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023) [hereinafter DPDP Act].
[7] K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India).
[8] Id. at 142 (Chandrachud, J.).

Article 21 protects the right to life and personal liberty, and its content has been progressively expanded since Maneka Gandhi v. Union of India to include rights not expressly enumerated in the text of the Constitution.[9] The Puttaswamy Court situated privacy within this expansive reading, holding that any State action infringing privacy must satisfy the threefold test of legality, legitimate aim, and proportionality.[10] The Aadhaar judgment subsequently applied this framework to a large-scale biometric identification system, underscoring the judiciary's willingness to scrutinise digital data architectures against constitutional standards.[11]

C. Informational Privacy and Data Protection

Informational privacy, as distinct from spatial or decisional privacy, concerns an individual's control over the collection, processing, and dissemination of personal data. The Puttaswamy bench recognised informational privacy as a distinct facet of the constitutional right, while leaving its detailed regulation to legislation an invitation that Parliament answered, after several iterations, with the Digital Personal Data Protection Act, 2023.

D. Legislative Framework Governing Digital Privacy

Several overlapping statutes bear upon the privacy of data processed in ODR proceedings.

1. Constitution of India

Article 21 remains the substantive anchor for any privacy claim, supplemented by Article 19(1)(a)'s protection of speech and expression, which the courts have extended to digital communication.[12]

2. Information Technology Act, 2000

The IT Act remains the principal statute governing electronic records, digital signatures, and cyber offences, and continues to apply to ODR platforms insofar as they handle electronic contracts and communications.[13]

3. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules,

[9] Maneka Gandhi v. Union of India, (1978) 1 S.C.C. 248 (India).
[10] K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India), at 638 (Sapre, J., setting out the proportionality standard for restrictions on privacy).
[11] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 S.C.C. 1 (India) (Aadhaar judgment).
[12] The Constitution of India art. 21.
[13] The Information Technology Act, No. 21 of 2000, India Code (2000).

2011

The Rules of 2011 contain requirements for collection and disclosure of certain "sensitive" personal data, such as financial data and health records, and remain in effect until the Rules of the DPDP Act are fully notified.[14]

4. Digital Personal Data Protection Act, 2023

The DPDP Act establishes a comprehensive, consent-centric framework for the processing of digital personal data by data fiduciaries, of direct relevance to ODR providers acting in that capacity.

5. Arbitration and Conciliation Act, 1996

The Arbitration Act, as amended in 2019, introduced an express confidentiality obligation upon arbitrators, institutions, and parties, which interacts with the data protection obligations now imposed by the DPDP Act.[15]

6. Mediation Act, 2023

The Mediation Act similarly mandates confidentiality of mediation communications, reinforcing though not displacing the statutory data protection regime applicable to online mediation platforms.[16]

III. UNDERSTANDING ODR AND PRIVACY RISKS IN DIGITAL DISPUTE RESOLUTION

A. Concept and Evolution of ODR

ODR emerged in the late 1990s as an extension of alternative dispute resolution into the digital domain, initially confined to resolving disputes arising from online transactions themselves.Its scope has since expanded well beyond its origins to encompass consumer, commercial, and even certain categories of civil and family disputes.[17] Indian scholarship tracking the NITI Aayog's ODR initiative has similarly emphasised the shift from a transaction-specific tool to a general-purpose mechanism for

[14] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) (India).
[15] The Arbitration and Conciliation Act, No. 26 of 1996, India Code (1996), § 42A (confidentiality of arbitral proceedings, inserted by the Arbitration and Conciliation (Amendment) Act, 2019).
[16] The Mediation Act, No. 32 of 2023, India Code (2023), § 22 (confidentiality of mediation communications).
[17] Faye Fangfei Wang, Online Dispute Resolution: Technology, Management and Legal Practice from an International Perspective 45-52 (2009).

addressing court backlog.[18]

B. Types of ODR Mechanisms

ODR mechanisms are generally classified into three broad categories, each carrying distinct privacy implications.

Online Negotiation involves direct, often automated, exchange of offers between parties, frequently mediated by algorithmic settlement tools that process transaction histories and behavioural data.

Online Mediation introduces a neutral third party who facilitates communication through video conferencing, chat, or asynchronous messaging, each generating its own data trail.

Online Arbitration abolished the binding determination and typically involves the most extensive exchange of documentary evidence, such as financial statements, contracts, and correspondence.

C. Stakeholders in the ODR Ecosystem

These are the disputing parties, the neutrals (mediators and arbitrators), the operators of the ODR platforms, cloud service providers, payment service providers, and video-conferencing service providers and, increasingly, artificial intelligence service providers for case triage and document review. Every other stakeholder is a possible data exposure opportunity.

D. Nature of Personal Data Processed in ODR

The ODR platforms also process information which may be deemed to be sensitive by most of the comparative data protection regimes, such as identity, contacts, financial information, transaction history, and, in the case of a family or employment dispute, even information regarding family or employment relationships. All of this data is able to be consolidated in one case file, increasing the impact of any unauthorised access.

E Privacy and Confidentiality Challenges

1. The collection of the personal information.

It is not always necessary for ODR platforms to gather the amount of data required to settle the dispute at hand, which conflicts with the data minimisation principle that is also outlined in the DPDP Act.

[18] Rangin Pallav Tripathy & Vasundhara Majithia, Online Dispute Resolution in India: Reflections on the NITI Aayog Initiative, 6 Indian J.L. & Tech. 1, 5-11 (2021).

2. Digital Records Storage and Retention

Some platforms maintain cases indefinitely, with no clear retention periods, which means that there is a risk that that this will not comply with the DPDP Act's storage limitation obligations.

3. Data sharing third parties

If ODR providers use third parties like cloud providers or AI vendors, personal data might be transferred outside India, triggering the provisions of the DPDP Act on cross-border transfers. [19]

4. Cyber security Threats

ODRs are also likely to be attractive targets for cyber attacks, especially because they store confidential, valuable personal and financial information, and a breach while an arbitration is pending could not only affect the privacy of the information, but also the fairness of the proceedings.

5. AI Assisted Dispute Resolution and Algorithmic Risks

As algorithmic tools are increasingly used to triage disputes, to suggest a range of feasible settlements, or even to draft awards, there are unique concerns over due process and transparency as affected parties have little visibility into the data inputs or the reasoning behind the process[20]. A recent paper from SSRN, titled Algorithm Accountability under the DPDP Act, suggests that the legislation's current provisions around automated processing are not sufficiently 'tuned' to deal with explainability concerns in adjudicatory contexts. [21]

IV. APPLICABILITY OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 TO ODR PLATFORMS

A. Key Features of the DPDP Act, 2023

The DPDP Act adopts a consent-based, principle-driven framework applicable to the processing of digital personal data within India, as well as processing outside India where it relates to offering goods or services to data principals in India. Comparative commentary has noted that this consent-centric model departs in important respects from the GDPR's

[19] The Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023), § 16 (cross-border transfer of personal data).
[20] Aniruddha Rajput, Algorithmic Decision-Making in ODR: A Due Process Critique, 13 NUJS L. Rev. 215, 221 (2020).
[21] Renuka Medury& Vidushi Marda, The Digital Personal Data Protection Act and the Future of Algorithmic Accountability in India, SSRN Working Paper (2023).

broader array of lawful processing grounds, a divergence with direct consequences for sectors, such as ODR, that rely on standardised, non-negotiable terms of engagement.[22]

B. Data Fiduciaries and ODR Service Providers

An ODR platform that determines the purpose and means of processing personal data submitted by disputing parties falls squarely within the statutory definition of a data fiduciary.[23] This characterisation is significant because it places the full weight of the Act's obligations rather than the lighter obligations of a data processor upon the platform itself.

C. Consent-Based Processing in ODR Proceedings

Processing of personal data generally requires free, specific, informed, unconditional, and unambiguous consent from the data principal, communicated through a clear affirmative action.[24] In the ODR context, this raises the practical question of how consent is to be meaningfully obtained from parties who may have little choice but to use a particular platform mandated by a contractual arbitration clause.

D. Rights of Data Principals

Data principals enjoy rights of access, correction, erasure, and grievance redressal, including the right to have personal data corrected or erased once the purpose of processing has been served.[25] These rights sit uneasily alongside the evidentiary and record-keeping requirements of arbitration, which often demand the indefinite preservation of case files.

E. Duties and Compliance Obligations of ODR Platforms

Data fiduciaries must implement reasonable security safeguards to prevent personal data breaches and must notify both the Data Protection Board and affected data principals in the event of a breach.[26]

F. Data Breach Reporting and Accountability

The Act imposes significant financial penalties for non-compliance, including failures of security safeguards, which can run into hundreds of crores of rupees depending on the nature and scale of the breach.[27]

---

[22] Graham Greenleaf, India's Data Privacy Bill: Open for Business?, 184 Privacy L. & Bus. Int'l Rep. 16, 18-20 (2023).
[23] The Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023), § 2(h) (defining "data fiduciary").
[24] The Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023), § 4.
[25] The Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023), § 13 (right to correction and erasure).
[26] The Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023), § 8(5).
[27] The Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023), § 33

G. Role of the Data Protection Board of India

The Data Protection Board of India, established under the Act, is empowered to inquire into breaches, impose penalties, and direct remedial measures, functioning as the principal regulatory body for ODR platforms acting as data fiduciaries.[28]

V. ROLE OF THE JUDICIARY IN SHAPING PRIVACY STANDARDS FOR ODR PLATFORMS

A. Judicial Recognition of Privacy as a Fundamental Right

1. Early Foundations: Gobind v. State of Madhya Pradesh and R. Rajagopal v. State of Tamil Nadu

The Supreme Court had already started to establish the right to privacy in the Constitution long before Puttaswamy definitively settled the question. In Gobind v State of Madhya Pradesh, the Court determined that the privacy interest could be a component of personal liberty guaranteed by Article 21. Still, it limited recognition of such a right by subordinating it to a compelling state interest, the latter being established through due process.[29]However, Justice Mathew's opinion did not envision privacy as a separate guarantee, but as an emanation of a set of constitutional freedoms, and was therefore very circumspect in his reasoning, which nevertheless became the cornerstone of future cases.[30]In R. Rajagopal v. State of Tamil Nadu, which came before the court about 20 years later, the Court extended the reasoning it had applied in the context of publication and disclosure, to find that a person had a right to be let alone, and that no disclosure of personal facts, even if it was factually correct, could be permitted to give rise to liability, unless in any given case there was a defence related to public records and matters of legitimate public interest.[31] The same separation between what can rightfully be placed in the public domain and what can be held within an individual's protected sphere is directly relevant to ODR, which involves the case file and settlement terms being located on this very boundary between resolution and information that platforms might wish to hold, analyse and share for institutional purposes.[32]

(penalties).

[28] The Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023), § 18 (constitution of the Data Protection Board of India).

[29] Gobind v. State of Madhya Pradesh, (1975) 2 S.C.C. 148 (India).

[30] Id. at 22 (Mathew, J., recognising a limited fundamental right to privacy subject to compelling state interest).

[31] R. Rajagopal v. State of Tamil Nadu, (1994) 6 S.C.C. 632 (India).

[32] Id. at 26-28 (holding that the right to privacy includes the right to be let alone and protects against unauthorised publication of personal information, subject to exceptions for matters of public record).

2. Justice K.S. Puttaswamy v. Union of India and Informational Privacy

Puttaswamy remains the foundational precedent, establishing that informational privacy is a constitutionally protected interest subject to reasonable restriction only through a law that is fair, just, and proportionate.

3. District Registrar and Collector v. Canara Bank and Protection of Personal Information

In Canara Bank, the Supreme Court struck down a state statute permitting unrestrained access to bank records, holding that the right to privacy extends to personal information held by third parties such as financial institutions.[33] The Court was emphatic that the mere fact a third party lawfully possesses an individual's data does not extinguish that individual's privacy interest in it, a principle directly transposable to ODR platforms holding financial and transactional data on behalf of disputing parties who never directly consented to its onward use.[34]

4. People's Union for Civil Liberties v. Union of India and Communication Privacy

PUCL recognised that the interception of communications, even telephonic, infringes the right to privacy absent procedural safeguards, a principle with obvious resonance for the interception or unauthorised access of video-conferencing and chat-based ODR communications.[35]

5. Selvi v. State of Karnataka, X v. Hospital Z, and Sharda v. Dharmpal: Consent, Disclosure, and Bodily and Medical Privacy

A separate line of authority addresses privacy not in the context of state surveillance but in the context of compelled disclosure and consent, questions that translate readily into the data-protection setting. In Selvi v. State of Karnataka, the Supreme Court held that subjecting an individual to narcoanalysis, polygraph, or brain-mapping tests without free and informed consent violates both the right against self-incrimination under Article 20(3) and the right to mental privacy under Article 21.[36] The Court's insistence that consent must be genuinely voluntary, and not merely procedurally recorded, offers a useful analogy for assessing whether the consent obtained by ODR platforms through standard-form terms of service can be regarded as free in the sense the DPDP Act requires.[37]In X v. Hospital Z, the Court addressed the converse

[33] District Registrar and Collector v. Canara Bank, (2005) 1 S.C.C. 496 (India).
[34] Id. at 41.
[35] People's Union for Civil Liberties v. Union of India, (1997) 1 S.C.C. 301 (India).
[36] Selvi v. State of Karnataka, (2010) 7 S.C.C. 263 (India).
[37] Id. at ,218-23 (holding that involuntary administration of narcoanalysis, polygraph,

problem, holding that a patient's right to medical confidentiality, while real, is not absolute and may yield where disclosure is necessary to protect the health or safety of a third party.[38] This balancing exercise anticipates the kind of conflict an ODR platform may face when statutory disclosure obligations, court directions, or the legitimate interests of an opposing party compete with a data principal's expectation of confidentiality.[39] Sharda v. Dharmpal extended similar reasoning to matrimonial proceedings, holding that a court could direct a party to undergo a medical examination notwithstanding a privacy objection, provided the direction served a legitimate purpose connected to the adjudication itself.[40]These three decisions together indicate that Indian courts have long practiced a "purpose-based" balancing test when determining issues of consent and disclosure, which is in line with the "proportionality" test to be formalized in Puttaswamy and now part of the framework of the DPDP Act itself in relation to processing personal data..[41]

B. Judicial Development of Digital Privacy Jurisprudence

1. State of Maharashtra v. Praful B. Desai and the Legitimacy of Virtual Proceedings

Before ODR became a policy priority, the Supreme Court had already confronted the question of whether a proceeding conducted partly through technology could satisfy constitutional standards of fairness. In Praful B. Desai, the Court held that recording evidence by video-conferencing was permissible and did not, by itself, offend an accused's right to a fair trial, provided the process preserved the substance of an in-person examination.[42] The judgment's insistence that technological mediation must not dilute procedural safeguards, even as it expands access, supplies an important interpretive anchor for evaluating whether ODR platforms' video and chat-based proceedings meet equivalent standards of fairness and data integrity.[43]

---

and brain-mapping tests violates Article 20(3) and the right to mental privacy under Article 21).

[38] X v. Hospital Z, (1998) 8 S.C.C. 296 (India).

[39] Id. at 26-28 (holding that the duty of medical confidentiality is qualified and may yield to the public interest in preventing harm to an identifiable third party).

[40] Sharda v. Dharmpal, (2003) 4 S.C.C. 493 (India).

[41] Id. at 35-39 (holding that a court-directed medical examination in matrimonial proceedings does not violate the right to privacy where it serves a legitimate adjudicatory purpose).

[42] State of Maharashtra v. Praful B. Desai, (2003) 4 S.C.C. 601 (India).

[43] Id. at 19-22 (holding that recording of evidence by video-conferencing is permissible under the Code of Criminal Procedure, 1973, and does not violate the accused's right to a fair trial, provided adequate safeguards are maintained).

2. Shreya Singhal v. Union of India and Protection of Online Freedoms

Although Shreya Singhal primarily concerned the constitutionality of Section 66A of the IT Act, its insistence on precision and proportionality in regulating online conduct has informed subsequent judicial scrutiny of digital governance measures generally.[44]

3. Karmanya Singh Sareen v. Union of India and Data Sharing Concerns

The Delhi High Court's consideration of a messaging platform's data-sharing policy in Karmanya Singh Sareen illustrates judicial sensitivity to the unilateral alteration of privacy terms by digital service providers.[45] The petitioners had argued that a sudden change to the platform's policy, permitting data sharing with an affiliated company, deprived users of meaningful choice once they had already become dependent on the service a concern equally applicable to ODR platforms that revise their data practices midway through a pending arbitration or mediation, leaving parties with little practical option but to acquiesce.

4. Anuradha Bhasin v. Union of India and Digital Rights

Anuradha Bhasin recognised that access to the internet is itself constitutionally protected under Articles 19(1)(a) and 19(1)(g), and that any restriction on such access must satisfy the doctrine of proportionality.[46] The judgment's reasoning carries an important implication for the accessibility dimension of ODR: since participation in a virtual proceeding presupposes reliable connectivity, the digital divide can, in practice, foreclose a litigant's ability to participate in good faith, raising fairness concerns that sit alongside, and sometimes in tension with, the privacy concerns this article addresses.[47]

C. Judicial Standards Relevant to ODR Platforms

1. Consent and User Autonomy

Judicial pronouncements emphasising informed, specific consent inform the standard against which ODR platforms' consent architecture should be measured, particularly where consent is bundled into non-negotiable terms of service.

2. Transparency and Accountability

Courts have consistently demanded transparency from entities

[44] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).
[45] Karmanya Singh Sareen v. Union of India, (2017) S.C.C. OnLine Del 11304 (India).
[46] Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India).
[47] Id. at 70-73 (holding that the freedom to access the internet is protected under Articles 19(1)(a) and 19(1)(g)).

processing personal data, a standard ODR platforms must meet through clear privacy notices and accessible grievance mechanisms.

3. Procedural Fairness in Digital Proceedings

The constitutional guarantee of a fair hearing extends to the digital environment, requiring that data security lapses not be permitted to compromise a party's ability to present its case.

4. Confidentiality of Arbitration and Mediation Records

Judicial recognition of confidentiality as integral to arbitration reinforces the statutory confidentiality obligations under Section 42A of the Arbitration Act and Section 22 of the Mediation Act. India's arbitration confidentiality regime and its data protection law similarly concludes that the two frameworks, while complementary in objective, remain poorly harmonised in operation.[48]

5. Balancing Privacy with Access to Justice

Courts have repeatedly had to balance privacy against competing public interests; in the ODR context, this translates into balancing data minimisation against the evidentiary completeness required for a fair adjudication.

D. Future Judicial Interpretation of the DPDP Act in ODR Disputes

Broader scholarship on the trajectory of Indian digital rights jurisprudence suggests that courts are likely to continue extending established privacy doctrine incrementally to new technological contexts rather than awaiting fresh legislative intervention.[49]

1. Determination of Data Fiduciary Liability

Courts will likely be called upon to determine the precise boundaries of data fiduciary status where ODR platforms operate through layered arrangements with panel arbitrators, institutions, and technology vendors.

2. Data Breach Litigation

As breach notifications under the DPDP Act become more frequent, litigation is likely to test the adequacy of reasonable security safeguard in the specific context of ODR infrastructure.

[48] Aparajita Lath, Data Protection and Arbitration in India: Mapping the Overlap, SSRN Working Paper (2021).
[49] Amber Sinha, The Networked Public: How Social Media Changed Democracy 112-19 (2019) (discussing judicial trends in Indian digital rights jurisprudence).

3. Enforcement of Data Principal Rights

Disputes are likely to arise over the tension between a data principal's right to erasure and an ODR platform's obligation to preserve records for appeal or enforcement proceedings.

4. Judicial Review of Automated Decision-Making Systems

As algorithmic tools assume a greater role in case triage and settlement recommendation, courts may be required to develop standards of explainability analogous to those already demanded in other administrative contexts.

VI. COMPLIANCE CHALLENGES UNDER THE DPDP ACT FOR ODR PLATFORMS

A. Valid and Informed Consent

Even where ODR is required to be provided under a pre-existing arbitration clause, securing consent that is truly free is a structural challenge the DPDP Act cannot head off.

B. Data Minimisation and Purpose Limitation

Platforms that are created to handle general case management may take in information that is more than required for a particular disagreement, which can bring tension with the objective limitation principle.

C. Protection of Confidential Arbitration and Mediation Records

An interpretive issue remains whether statutory confidentiality requirements can be balanced with the investigatory powers of the Data Protection Board.

D. Cybersecurity and Data Breach Risks

There are several smaller ODR providers who do not have the resources to adopt the security protections envisioned by the Act, which makes it easier for other providers to provide those services.

E. Cross-Border Data Transfers

Reliance on foreign-hosted cloud infrastructure and international video-conferencing tools implicates the Act's cross-border transfer restrictions, the precise contours of which remain to be fully notified. The broader policy debate over data localisation in India, including its costs to smaller digital service providers, bears directly on whether ODR platforms can realistically comply without prohibitive infrastructure investment.[50]

[50] Rishab Bailey & Smriti Parsheera, Data Localisation in India: Questioning the Means

F. Compliance Burden on Private ODR Service Providers

Smaller and newer ODR start-ups may find the compliance burden disproportionate relative to larger institutional providers, potentially entrenching incumbents.

G. Enforcement Challenges under the DPDP Regime

The effectiveness of the Data Protection Board will depend on its capacity and willingness to develop sector-specific guidance for dispute resolution platforms, an undertaking still in its early stages.

VII. FINDINGS AND SUGGESTIONS

This study points to several major findings.

- A significant amount of personal and confidential information is utilized on ODR platforms and the volume of information gathered in negotiation, mediation and arbitration is much greater than is generally recognized by the parties before the process begins.
- The Digital Personal Data Protection Act, 2023 places both very heavy obligations on ODR providers and very light obligations on ODR providers, but the obligations are lengthy and not formulated particularly with the realities of running a dispute resolution platform in mind.
- There are no common privacy or data governance principles across existing ODR frameworks and no sector-specific regulation, which has led to significant variation in the privacy practices of platforms.
- Judicial privacy jurisprudence remains the interpretive lens through which the DPDP Act obligations will be followed and Puttaswamy and its offspring continue to provide the normative framework for the compliance of the DPDP Act.
- Consent management, cybersecurity, and data retention issues remain a challenge, and these are the three most critical compliance gaps that were pointed out in this study.
- A number of steps would make a difference in closing these gaps. Platform design needs to incorporate privacy considerations at the architectural level and not be added after deployment, otherwise ensuring data minimisation and security will be added

and Ends, NIPFP Working Paper No. 242, at 9-14 (2018).

on top of the platform and not part of it. Guidance from the Data Protection Board, in conjunction with the Department of Justice, is needed for the dispute resolution sector, given that the general provisions of the DPDP Act are inadequate to deal with the specific dynamics that exist in arbitration and mediation. Platforms that handle critical categories of personal information, like those in family or employment conflicts, should be subject to regular data protection impact assessments, so that potential risks can be spotted before they turn into data breaches.

- Wherever a case is communicated, the end to end encryption of the case communication should be required, irrespective of the size or resources of the individual provider. Clear, sector-wide retention and deletion schedules would minimize compliance uncertainty and the likelihood of unjustified retention of data, especially where a data principal's right to erasure and the need of an institution to retain data for enforcement or appeal are at odds. There should be structured training for neutrals and platform administrators on data protection requirements applicable to their role, as adherence to these requirements will be dependent on the actions of those managing systems on a day-to-day basis.

- Courts supervising arbitration should be able to provide some guidance for how data should be handled in ODR, derived from the principles of court established privacy law, as presented above. The Data Protection Board would improve accountability beyond just an after-the-fact audit by conducting proactive audits of high volume ODR platforms. Parties shall be informed on the use of the algorithmic tools – and afforded a meaningful opportunity to challenge automated recommendations – in their case rather than having outcomes before them which they have no meaningful opportunity to question. Last but not least, the establishment of a single national ODR privacy compliance framework, aligning the requirements of the DPDP Act with those of the Arbitration and Conciliation Act and the Mediation Act, would offer a much-needed degree of clarity to platforms and litigants alike, and would replace the existing patchwork of overlapping and sometimes confusing obligations.

VIII. CONCLUSION

Online Dispute Resolution is not just a marginal experiment but an increasingly mainstream part of the system of justice delivery in India, which provides speed and accessibility to the justice system that can often be unattainable with litigation. With the number of conflicts spawned by digital transactions increasing, ODR platforms are poised to

take on even more of the normal functions of courts and tribunals today.

But this evolution is grounded in litigants' trust that their private and confidential facts will be treated like those of face-to-face proceedings. Success in ODR depends on privacy not being an incidental; it is key to the foundation upon which parties must trust a faceless, server-mediated process. If that scepticism, however, is widespread without parties realizing they are losing their case, the efficiency benefits of digital dispute resolution may be lost.

For the first time, the Digital Personal Data Protection Act, 2023 offers a comprehensive yardstick against which data practices of ODR platforms can be measured and enforced. It forces platforms to shift from the format of an informal or inconsistent privacy approach to a formal system of consent, accountability, and breach notification. Despite this, the Act is written in a general manner and will almost certainly present some interpretive issues because of the unique features of arbitration, mediation and online negotiation.

Despite the development of statutory regulation, the constitutional framework around Article 21 will continue to be the benchmark for disputes regarding the quality and quantity of data used by an ODR service, the extent of a data principal's rights and interests, and the limits of what is allowed in algorithmic decision-making. It is from this constitutional basis that courts will have to build as they attempt to make up for the gaps left by the necessarily general statute.

Finally, if ODR is to be successful in India in the long term, the attitude of ODRs, regulators and courts, to privacy as a compliance feature, rather than a fundamental component of digital justice, will need to change. A system that is acceptable to the litigants who will be using it is a system that will work; a system that is not intact with its data will not work.