



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

REGULATING ODR IN INDIA:

THE NEED FOR A DEDICATED ODR AUTHORITY IN INDIA

~ Shrushti Dumbre

ABSTRACT

*Online Dispute Resolution (ODR) integrates digital technology with the traditional methods of Alternative Dispute Resolution (ADR), and its adoption across sectors such as e-commerce, banking, fintech, and consumer protection demonstrates its potential to deliver efficient, accessible, and cost-effective justice. In India, ODR derives legal recognition from the **Arbitration and Conciliation Act, 1996**, the **Mediation Act, 2023**, the **Information Technology Act, 2000**, and the **Digital Personal Data Protection Act, 2023**, none of which was enacted to regulate the technological ecosystem within which ODR platforms operate.*

This paper examines the adequacy of that framework and identifies the regulatory gaps arising from cybersecurity, data protection, platform accountability, Artificial Intelligence (AI), and user protection. It argues that while existing ADR laws provide a procedural foundation for ODR, they cannot regulate its technological and institutional dimensions, and accordingly advocates a dedicated regulatory framework supported by an independent ODR Regulatory Authority to ensure accountability, transparency, and public trust in digital dispute resolution.

KEYWORDS

Online Dispute Resolution (ODR), Alternative Dispute Resolution (ADR), Artificial Intelligence, Regulatory Framework, ODR Regulatory Authority, Digital Justice, Access to

Justice.

INTRODUCTION

The justice delivery system is undergoing an important transformation in the digital era. As technology reshapes consumer interactions, contractual relationships, and financial services, the nature of disputes is itself becoming increasingly digital, while conventional mechanisms remain constrained by procedural complexity, cost, and geographical barriers. The scale of the challenge is considerable: according to the **National Judicial Data Grid**, more than **5.15 crore cases** were pending before the Supreme Court, the High Courts, and the district and subordinate courts as of November 2024.¹ Backlogs of this magnitude have intensified the search for faster, more accessible, and more affordable dispute resolution.

Online Dispute Resolution (ODR) has emerged as one of the most significant innovations in this regard. By integrating digital technology with established methods of Alternative Dispute Resolution (ADR), it enables parties to resolve disputes through online platforms, virtual hearings, electronic communication, and automated processes. This growth has also exposed ODR to concerns of data privacy, cybersecurity, transparency, user protection, and platform accountability, while the growing use of Artificial Intelligence (AI) raises further questions about the competence of the existing legal framework.

This paper therefore asks whether the present framework is sufficient to govern India's growing ODR ecosystem and, by examining the existing legal landscape, identifying regulatory gaps, and evaluating emerging challenges, proposes a framework capable of supporting its sustainable development.

LITERATURE REVIEW

The rise of ODR has attracted considerable academic and policy attention over the past two decades, with early research concentrating on the capacity of technology to make dispute resolution more efficient, cost-effective, and accessible. **Ethan Katsh**, widely regarded as the father of ODR, argued that it should not be viewed merely as a medium of ADR but as a mechanism capable of creating new forms of dispute resolution suited to the digital

¹ National Judicial Data Grid, <https://njdg.ecourts.gov.in> (over 5.15 crore cases pending across the Supreme Court, High Courts, and District and Subordinate Courts as of November 2024).

environment.² **Pablo Cortés** later examined its practical applications, highlighting its value in addressing the low-value, high-volume disputes that often remain unresolved in conventional legal processes.³

In India, policy reports and institutional studies have focused primarily on the capacity of ODR to reduce judicial backlog and improve access to justice. The **NITI Aayog reports**⁴ and the initiatives of **Agami**⁵ have emphasised these opportunities and advocated adoption across banking, e-commerce, fintech, and consumer protection.⁶

Scholars have equally acknowledged the challenges: digital accessibility, cybersecurity, confidentiality, data privacy, procedural fairness, and enforceability of outcomes. More recent scholarship examines the effects of artificial intelligence and automated decision-making within dispute resolution, raising questions of accountability, algorithmic bias, and transparency.

This literature offers valuable insight into the benefits and challenges of ODR, but the majority of contributions analyse it as an extension of arbitration, mediation, and negotiation. Limited attention has been paid to regulatory governance, particularly in the Indian context.

RESEARCH GAP

Scholarship has thus concentrated on the potential, adoption, and challenges of ODR, while its regulatory dimension has received comparatively little attention. In India, ODR is governed by a fragmented framework, whether this dispersed structure adequately addresses cybersecurity obligations, AI governance, user protection, and platform accountability remains underexplored. This study examines whether India requires a dedicated regulatory framework for ODR.

² Ethan Katsh & Janet Rifkin, *Online Dispute Resolution: Resolving Conflicts in Cyberspace* 12–15 (Jossey-Bass 2001).

³ Pablo Cortés, *Online Dispute Resolution for Consumers in the European Union* 25–30 (Routledge 2010).

⁴ NITI Aayog, *Designing the Future of Dispute Resolution: The ODR Policy Plan for India* 8–12 (2021).

⁵ Agami, NITI Aayog & Omidyar Network India, *The ODR Handbook: Unlocking ODR for the Nation* 5–8 (2021).

⁶ Agami, *Enabling an Online Dispute Resolution Ecosystem*, Agami, [Agami ODR Mission](#) (last visited June 8, 2026).

THESIS STATEMENT

This paper argues that while existing ADR laws provide a legal foundation for Online Dispute Resolution in India, they are inadequate to regulate the technological and institutional dimensions of the ODR ecosystem. A dedicated regulatory framework is required to preserve the substantive role of existing ADR laws while establishing comprehensive standards for the governance of digital dispute resolution platforms.

RESEARCH METHODOLOGY

This paper adopts a doctrinal and comparative methodology. The doctrinal component systematically analyses primary legal sources, the *Arbitration and Conciliation Act, 1996*, the *Mediation Act, 2023*, the *Information Technology Act, 2000*, and the *Digital Personal Data Protection Act, 2023*, along with subordinate legislation, sectoral regulatory frameworks, judicial decisions, and policy documents such as the reports of **NITI Aayog**, in order to evaluate the adequacy of the existing framework and identify its regulatory gaps.

The comparative component examines institutional responses to ODR in the European Union, Canada, and China, alongside the normative standards articulated by the *United Nations Commission on International Trade Law*; not to transplant foreign models, but to draw contextually relevant lessons for an Indian framework. The study relies on secondary literature and publicly available primary sources and does not involve empirical research.

1. UNDERSTANDING ONLINE DISPUTE RESOLUTION

1.1 INTRODUCTION TO ONLINE DISPUTE RESOLUTION

The digitisation of commerce and communication has reshaped both the nature of disputes and the manner of their resolution, and ODR emerged as an innovative response incorporating technology into the traditional methods of ADR.⁷ Initially developed for disputes arising from online transactions, it evolved into a wider system applicable across sectors.⁸ Unlike traditional ADR, ODR uses digital platforms allowing parties to communicate, exchange documents, participate in hearings, and reach settlements without

⁷ Ethan Katsh & Janet Rifkin, *Online Dispute Resolution: Resolving Conflicts in Cyberspace* 1–15 (Jossey-Bass 2001).

⁸ NITI Aayog, *Designing the Future of Dispute Resolution: The ODR Policy Plan for India* 8–12 (2021).

physical presence.

1.2 EVOLUTION OF ODR

ODR emerged in the late 1990s alongside the growth of the internet and e-commerce, offering an alternative where the cost and delay of litigation made traditional mechanisms unsuitable for low-value, high-volume online disputes. Early systems focused on consumer and e-commerce matters; ODR is now used in commercial, banking, insurance, employment, consumer, and cross-border disputes. The COVID-19 pandemic further accelerated the adoption of virtual hearings, demonstrating the capability of technology-enabled dispute resolution at scale.

1.3 TYPES OF ODR

- **Online Negotiation**

It is the simplest form of ODR, enabling parties to communicate directly through digital platforms and negotiate mutually acceptable settlements without a neutral third party.

- **Online Mediation**

It involves a neutral mediator who assists parties towards a voluntary settlement through virtual meetings and digital communication tools, facilitating dialogue without imposing a binding decision.

- **Online Arbitration**

It incorporates technology into arbitral proceedings through electronic filing, virtual hearings, digital evidence submission, and online delivery of awards, while remaining legally grounded in arbitration law.

1.4 FEATURES & IMPORTANCE OF ODR

Several characteristics distinguish ODR from traditional mechanisms. It reduces the costs of travel, infrastructure, and procedural formality; improves accessibility by allowing participation irrespective of location; promotes efficiency through faster communication and case management; and offers the adaptability to handle large volumes of disputes simultaneously.

ODR has accordingly gained prominence in insurance claims, employment disputes, and small commercial matters where speed and cost-efficiency are essential. Banks use it for

loan and recovery disputes, fintech companies for digital payment and lending disputes, and e-commerce platforms for consumer grievances.⁹

2. EXISTING LEGAL SYSTEM GOVERNING ODR

2.1 ARBITRATION AND CONCILIATION ACT, 1996

The *Arbitration and Conciliation Act, 1996* is the principal legal basis for ODR in India. Founded on party autonomy and procedural flexibility, it permits parties to determine the procedure governing arbitral proceedings, and although enacted before modern ODR platforms emerged, its provisions are broad enough to accommodate technology-enabled mechanisms.¹⁰ Judicial acceptance of virtual hearings has further strengthened the validity of online arbitration.¹¹

The Act, however, regulates arbitration as a dispute resolution mechanism, not the digital platforms through which it is conducted. It is silent on platform governance, cybersecurity obligations, accreditation of service providers, algorithmic transparency, and AI-assisted decision-making. It validates online arbitration without regulating the broader technological ecosystem of ODR.

2.2 MEDIATION ACT, 2023

The *Mediation Act, 2023* gave statutory recognition to mediation and expressly permits the use of electronic means for conducting proceedings, providing legal support for online mediation and improving accessibility for parties in different geographical regions.¹²

The Act nevertheless focuses on mediation procedure and settlement outcomes. It establishes no standards for online mediation platforms, technological infrastructure, confidentiality protocols in digital environments, or user protection, leaving important governance concerns outside its scope.

2.3 INFORMATION TECHNOLOGY ACT, 2000

The *Information Technology Act, 2000* provides an essential supporting framework by

⁹ Pablo Cortés, *Online Dispute Resolution for Consumers in the European Union* 45–53 (Routledge 2010).

¹⁰ Arbitration and Conciliation Act, No. 26 of 1996, §§ 19, 20, India Code (1996).

¹¹ *State of Maharashtra v. Praful B. Desai*, (2003) 4 SCC 601.

¹² Mediation Act, No. 32 of 2023, § 30, India Code (2023).

granting legal recognition to electronic records, electronic contracts, digital signatures, and electronic communications.¹³ The validity of electronic agreements, online submissions, digital evidence, and virtual communication in ODR proceedings depends largely on this recognition, which underpins the digital infrastructure on which ODR platforms operate.

The Act was enacted to regulate electronic commerce and cyber activities generally, not dispute resolution. It therefore does not address accreditation of ODR platforms, dispute resolution standards, procedural safeguards for digital proceedings, or accountability mechanisms for technology providers.

2.4 DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Data is among the most important components of the ODR ecosystem: platforms routinely process personal information, financial records, contractual documents, and other confidential material generated during proceedings.¹⁴ The ***Digital Personal Data Protection Act, 2023*** accordingly assumes particular importance, establishing obligations on lawful processing, consent, data security, and the rights of data principals.¹⁵

The legislation does not, however, address the concerns specific to ODR. Confidentiality of proceedings, cross-border transfer of dispute-related data, retention of sensitive records, AI-assisted systems, and automated decision-making remain largely unaddressed. It provides a general framework for data protection, not a specialised regulatory mechanism for ODR platforms.

2.5 INSTITUTIONAL & POLICY SUPPORT FOR ODR

Beyond statutory recognition, ODR in India has been shaped by policy initiatives. The **NITI Aayog Report**¹⁶ and the initiatives of **Agami**¹⁷ have promoted awareness of technology-enabled dispute resolution, highlighted its capacity to improve access to justice and address judicial backlog, and encouraged adoption across banking, fintech, e-commerce, and consumer protection.

¹³ Information Technology Act, No. 21 of 2000, §§ 4, 5, 10A, India Code (2000).

¹⁴ Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

¹⁵ Digital Personal Data Protection Act, No. 22 of 2023, §§ 4–13, India Code (2023).

¹⁶ NITI Aayog, *Designing the Future of Dispute Resolution: The ODR Policy Plan for India* 8–20 (2021).

¹⁷ Agami, NITI Aayog & Omidyar Network India, *The ODR Handbook: Unlocking ODR for the Nation* 12–25 (2021).

Policy initiatives are, however, advisory rather than binding. They facilitate growth and innovation but cannot independently ensure uniform standards of governance, accountability, and compliance across ODR platforms.

2.6 SECTOR-SPECIFIC REGULATION: THE RBI & CONSUMER PROTECTION FRAMEWORKS

A significant, though sector-specific, development has emerged from the financial sector. In August 2020 the **Reserve Bank of India (RBI)** introduced a framework titled ***Online Dispute Resolution (ODR) System for Digital Payments***, directing all authorised Payment System Operators to implement a transparent, rule-based, system-driven ODR mechanism for disputes arising from failed digital transactions.¹⁸ Participating entities were required to operationalise the system by 1 January 2021, and the framework expressly contemplated progressive automation with minimal manual intervention.¹⁹

The framework is notable for three reasons. First, unlike the statutes discussed above, it does not merely recognize ODR, instead it mandates it, making ODR a compulsory component of the digital-payments grievance-redress architecture. Second, it prescribes concrete operational standards, including resolution timelines and transparency. Third, it shows that Indian regulators are already willing to impose binding ODR obligations within their domains.

Yet the framework also illustrates the fragmentation this paper identifies. Its mandate is confined to failed digital-payment transactions and does not extend to ODR platforms operating in e-commerce, insurance, employment, or general commercial disputes. The result is a regulator-by-regulator approach in which each authority prescribes standards for its own domain, with no common baseline for accreditation, cybersecurity, confidentiality, or algorithmic accountability.

A comparable impetus is visible in consumer protection. The ***Consumer Protection Act, 2019*** recognised e-commerce transactions and strengthened institutional oversight, while the ***Consumer Protection (E-Commerce) Rules, 2020*** imposed grievance-redress

¹⁸ Reserve Bank of India, Online Dispute Resolution (ODR) System for Digital Payments, RBI/2020-21/21, DPSS.CO.PD No.116/02.12.004/2020-21 (Aug. 6, 2020).

¹⁹ Id. (requiring authorized Payment System Operators to implement the ODR system by January 1, 2021).

obligations on e-commerce entities.²⁰ The e-Daakhil portal reinforces these measures by enabling consumers to file and pursue complaints online before the consumer commissions, embedding elements of ODR within the statutory consumer-protection machinery.²¹

Alongside these measures, a growing ecosystem of private ODR service providers has emerged. Platforms such as **SAMA**, **CADRE**, **CORD**, and **Presolv360** administer negotiation, mediation, and arbitration for banks, financial institutions, and e-commerce companies.²² The coexistence of binding sectoral mandates, statutory consumer-protection mechanisms, and an expanding private-platform market illustrates both the momentum behind ODR and the absence of any common regulatory baseline governing these diverse actors.

3. REGULATORY CHALLENGES IN THE ODR ECOSYSTEM

3.1 DATA PRIVACY & CONFIDENTIALITY CONCERNS

One of the most significant challenges in ODR is the protection of sensitive information. Unlike conventional processes, ODR platforms operate entirely through digital infrastructure and routinely process large volumes of personal, financial, commercial, and contractual data, as parties disclose confidential information, settlement proposals, business records, and private communications during proceedings.

This increases the risk of unauthorised access, data breaches, and misuse. Although the **Digital Personal Data Protection Act, 2023** establishes a general framework, it does not address the confidentiality requirements exclusive to dispute resolution, leaving data retention, storage practices, cross-border transfer, and the protection of confidential settlement discussions uncertain, with consequences for user trust and the credibility of ODR platforms.

3.2 CYBERSECURITY RISKS

²⁰ Consumer Protection Act, No. 35 of 2019, India Code (2019); Consumer Protection (E-Commerce) Rules, 2020, G.S.R. 462(E) (India).

²¹ National Consumer Disputes Redressal Commission, e-Daakhil Portal, <https://edaakhil.nic.in>.

²² See NITI Aayog, Designing the Future of Dispute Resolution: The ODR Policy Plan for India (2021) (documenting India's emerging private ODR ecosystem).

Because proceedings are conducted online, cybersecurity is a fundamental requirement rather than a supplementary concern. ODR platforms may be vulnerable to hacking, phishing, unauthorised access, data manipulation, or system failure, and a breach can compromise confidential documents, disrupt proceedings, and undermine confidence in the process.

While existing cyber laws provide general safeguards, no uniform cybersecurity standards apply specifically to ODR platforms. The protection offered by different providers may therefore vary significantly, creating uncertainty for users and raising questions of accountability in the event of a security failure.

3.3 PLATFORM ACCOUNTABILITY

ODR depends upon private technology platforms. Unlike courts and tribunals, its proceedings are often administered by digital service providers that manage communication, document exchange, case management, and virtual hearings. Despite performing functions that directly influence the process, no comprehensive framework governs their accountability, and operational standards, transparency obligations, grievance redressal, and quality control remain largely unanswered.

If a platform fails to protect user data, suffers repeated technical failures, or adopts unfair practices, no specialised institution monitors compliance or enforces standards. The absence of a dedicated regulatory authority compounds the problem.

3.4 ARTIFICIAL INTELLIGENCE & AUTOMATED DECISION-MAKING

AI is increasingly used within ODR platforms for case management, document review, dispute categorisation, predictive analytics, and settlement recommendations, with real potential to improve efficiency and reduce administrative burdens.

Reliance upon AI nevertheless raises concerns of transparency, fairness, and accountability. Algorithmic systems may operate through processes users do not fully understand, making it difficult for parties to see how outcomes or recommendations are generated. Concerns about algorithmic bias have also attracted attention: systems trained on incomplete or biased data may produce outcomes that unintentionally disadvantage

certain users. The absence of clear regulatory standards governing AI-assisted dispute resolution leaves responsibility and oversight uncertain.

3.5 DIGITAL DIVIDE & ACCESSIBILITY

Although ODR is praised for improving access to justice, its effectiveness depends upon access to technology. Significant sections of the population continue to face barriers of internet connectivity, digital literacy, language, and access to devices.

For technologically proficient users ODR may simplify dispute resolution considerably; for those in rural areas, elderly persons, and users with limited digital skills, it may impede effective participation. As ODR becomes integrated into the justice system, accessibility must remain a central consideration of any regulatory framework, so that technological innovation does not create new barriers to justice.

3.6 JURISDICTIONAL & ENFORCEMENT ISSUES

ODR frequently involves parties located in different cities, states, or countries. While technology enables disputes to be resolved across geographical boundaries, it complicates the determination of applicable law, the identification of the appropriate forum, and the enforcement of outcomes, difficulties to which cross-border disputes are particularly vulnerable.

Although arbitration and mediation law provide certain enforcement mechanisms, the increasing digitalisation of dispute resolution requires greater clarity on the jurisdictional rules applicable to ODR proceedings; the absence of specialised guidance contributes to legal uncertainty.

3.7 ABSENCE OF A DEDICATED REGULATORY AUTHORITY

No body currently formulates uniform standards for ODR platforms, monitors compliance, accredits service providers, establishes cybersecurity requirements, supervises AI-assisted systems, or addresses user grievances. Governance remains dispersed across multiple laws and institutions, which may in time weaken user confidence and produce inconsistent compliance.

The difficulty, then, is not the absence of legal recognition but the absence of a coherent regulatory structure; one capable of addressing cybersecurity, platform accountability, AI governance, data protection, and accessibility while preserving the benefits of technology-enabled dispute resolution.

4. COMPARATIVE PERSPECTIVES ON ODR REGULATION

The regulation of ODR is not a uniquely Indian concern. Several legal systems have already developed dedicated statutory or institutional responses to technology-enabled dispute resolution, and their experience offers lessons for the design of an Indian framework.

- A. The **European Union** was among the first to enact a dedicated instrument for consumer ODR. *Regulation (EU) No 524/2013* established a centralised, publicly operated platform for disputes arising from online transactions.²³ Its fate is equally instructive: owing to persistently low usage, with only a small fraction of complaints ever receiving a trader response, the Union repealed the Regulation through *Regulation (EU) 2024/3228*, and the platform was permanently discontinued on 20 July 2025.²⁴ The European experience shows that regulatory design must be accompanied by mechanisms securing participation and trader engagement; a platform cannot succeed on legal recognition alone.
- B. At the international level, *UNCITRAL* adopted the Technical Notes on Online Dispute Resolution in 2016.²⁵ Though non-binding, they articulate core principles: impartiality, transparency, fairness, and due process; to guide the development of ODR systems for cross-border, low-value, high-volume disputes, and provide a widely accepted normative reference point that an Indian framework could adapt.
- C. **British Columbia** offers a leading example of institutionalised ODR. The Civil Resolution Tribunal, established under the *Civil Resolution Tribunal Act, 2012*, is widely regarded as **Canada's first online tribunal**.²⁶ Operational since 2016 for strata disputes and 2017 for small claims, it conducts the entire process online, combining

²³ Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on Online Dispute Resolution for Consumer Disputes, 2013 O.J. (L 165) 1.

²⁴ Regulation (EU) 2024/3228 of the European Parliament and of the Council of 19 December 2024 repealing Regulation (EU) No 524/2013; the ODR platform was permanently discontinued on 20 July 2025.

²⁵ UNCITRAL, Technical Notes on Online Dispute Resolution (2016).

²⁶ Civil Resolution Tribunal Act, S.B.C. 2012, c. 25 (Can. B.C.).

guided self-help tools, negotiation, facilitation, and binding adjudication.²⁷ Crucially, it is a public institution embedded within the justice system, demonstrating that ODR can be delivered through a dedicated statutory body rather than left to private platforms.

D. **China** has adopted a distinctive model through specialised Internet Courts. The Hangzhou Internet Court, inaugurated in August 2017, was the world's first, followed by the Beijing and Guangzhou courts in 2018.²⁸ They adjudicate internet-related disputes, such as e-commerce, online lending, digital intellectual property entirely through online proceedings and have pioneered blockchain-based evidence authentication. While reflecting a particular institutional context, the model illustrates the feasibility of purpose-built, technology-centred adjudicatory institutions.

Three insights follow. Dedicated statutory and institutional frameworks for ODR are feasible and increasingly common. Their success depends not only on legal recognition but on sustained user trust, participation, and procedural safeguards, as the closure of the EU platform demonstrates. And instruments such as the UNCITRAL Technical Notes offer a ready normative foundation on which India could build. Together they reinforce the case for a coordinated framework supported by an independent authority, rather than continued reliance on a fragmented body of general legislation.

5. TOWARDS A DEDICATED REGULATORY FRAMEWORK FOR ODR IN INDIA

The question is not whether ODR is legally valid, but whether the current framework is institutionally equipped to govern an increasingly technology-driven ecosystem. The answer appears to be in the negative.

A dedicated framework must first address data governance. ODR proceedings involve highly sensitive information, and although general data protection legislation provides a foundation, ODR presents concerns requiring specialised safeguards. Regulatory standards should prescribe clear obligations on the collection, storage, retention, transfer, and deletion of dispute-related data.

²⁷ Civil Resolution Tribunal (B.C.) (strata claims from July 13, 2016; small claims from June 1, 2017).

²⁸ See Provisions of the Supreme People's Court on Several Issues Concerning the Trial of Cases by Internet Courts (2018) (China); the Hangzhou Internet Court was established on Aug. 18, 2017.

Cybersecurity must occupy a similarly central position, since the integrity of proceedings depends upon the security of the platforms conducting them. ODR platforms should be required to comply with minimum cybersecurity standards, undertake regular security audits, and maintain effective incident-response mechanisms.

The framework must further ensure that innovation does not undermine access to justice. Given persistent challenges of digital literacy, internet access, and language diversity, regulatory standards should promote multilingual interfaces, accessible platform design, and user-centric procedures capable of accommodating individuals from diverse socio-economic backgrounds. The success of ODR should be measured not by technological sophistication but by its capacity to make dispute resolution more inclusive.

This depends on an appropriate balance between innovation and regulation. Excessive regulation may discourage technological development, while insufficient regulation weakens public trust and creates governance gaps. The objective should be an environment that encourages innovation while ensuring accountability, transparency, security, and procedural fairness.

6. PROPOSED ODR REGULATORY AUTHORITY IN INDIA

6.1 STRUCTURE OF THE PROPOSED AUTHORITY

The proposed ODR Regulatory Authority should be established through dedicated legislation enacted by Parliament, functioning as an independent statutory body responsible for supervision rather than adjudication. Its purpose would not be to interfere with the outcome of disputes, but to regulate the systems, platforms, and technological processes through which disputes are resolved.

To ensure balanced governance, the Authority should consist of experts from diverse fields. The composition may include:

- A Chairperson possessing substantial experience in dispute resolution or judicial administration;
- An ADR expert with specialization in arbitration and mediation;
- A technology expert with knowledge of digital platforms and cybersecurity;
- A data protection expert;
- An Artificial Intelligence specialist; and

- A representative nominated by the Central Government.

Such a multidisciplinary structure would enable the Authority to address both legal and technological concerns associated with ODR.

6.2 FUNCTIONS OF THE AUTHORITY

The primary responsibility of the Authority should be to regulate and promote the responsible growth of ODR in India. Its functions may include:

a) ACCREDITATION OF ODR PLATFORMS

The Authority should establish accreditation standards for ODR service providers, compliance with prescribed technological, procedural, and ethical standards being mandatory. Accreditation would give parties a means of evaluating the reliability, security, and competence of platforms, strengthening accountability and contributing to the professionalisation of the ecosystem.²⁹

b) REGULATORY OVERSIGHT

The Authority should monitor compliance with applicable regulations and ensure that ODR platforms operate in accordance with prescribed standards.

c) USER PROTECTION

The Authority should provide guidelines aimed at safeguarding user rights, ensuring procedural fairness, and protecting confidential information.

d) AWARENESS AND CAPACITY BUILDING

The Authority should promote awareness regarding ODR among legal professionals, businesses, consumers, and public institutions.

e) POLICY DEVELOPMENT

The Authority should continuously assess emerging technological developments and recommend policy reforms necessary for the effective governance of ODR.

²⁹ Colin Rule, *Online Dispute Resolution for Business* 137–145 (Jossey-Bass 2002).

6.3 REGULATORY POWERS OF THE AUTHORITY

For effective enforcement, the Authority should be vested with appropriate regulatory powers. These powers may include:

- Grant, suspend, or revoke accreditation of ODR platforms;
- Conduct compliance audits and inspections;
- Issue directions and regulatory guidelines;
- Investigate complaints against service providers;
- Require disclosure of relevant information from ODR platforms; and
- Impose penalties for violations of prescribed standards.

6.4 REGULATION OF ARTIFICIAL INTELLIGENCE IN ODR

The integration of AI into dispute resolution necessitates specialised oversight. While AI can improve efficiency through automated case management, document review, and settlement recommendations, it raises concerns of transparency, accountability, and algorithmic bias.

The proposed Authority should formulate guidelines governing the use of AI within ODR platforms. These guidelines should require:

- Disclosure whenever AI tools are utilized during dispute resolution proceedings;
- Meaningful human oversight over AI-assisted processes;
- Periodic audits of algorithmic systems;
- Transparency regarding AI-generated recommendations; and
- Measures to identify and mitigate algorithmic bias.

Such safeguards would enable responsible innovation while preserving procedural fairness and public confidence in dispute resolution systems.³⁰

6.5 BENEFITS OF PROPOSED AUTHORITY

A dedicated Authority would create uniform standards across the country, build user confidence through compliance with data protection and cybersecurity requirements, improve accountability through continuous oversight, and facilitate responsible adoption

³⁰ Orna Rabinovich-Einy & Ethan Katsh, *Artificial Intelligence and Dispute Resolution: Opportunities and Challenges*, 21 *Cardozo J. Conflict Resol.* 297, 310–322 (2020).

of emerging technologies. It would function not merely as a regulator but as an institution fostering trust, legitimacy, and long-term growth within the ODR ecosystem.³¹

6.6 RELATIONSHIP WITH EXISTING REGULATORY BODIES

A dedicated ODR authority would not operate in a vacuum. Several bodies already exercise mandates that intersect with ODR, and the proposed authority must complement rather than duplicate them. The **Arbitration Council of India**, envisaged under **Part IA of the Arbitration and Conciliation Act, 1996**, is empowered to grade arbitral institutions and accredit arbitrators, yet it remains unconstituted several years after its statutory introduction, and its mandate is in any event confined to arbitration rather than the wider technological ecosystem of ODR.³² The **Data Protection Board of India**, operational following the notification of the **Digital Personal Data Protection Rules, 2025**, adjudicates data-protection grievances but does not regulate dispute-resolution platforms as such.³³

The proposed authority should therefore be conceived as a coordinating and standard-setting body working alongside these institutions and sectoral regulators such as the **Reserve Bank of India**, the **Securities and Exchange Board of India**, and the **Insurance Regulatory and Development Authority of India**. Its focus should be limited to the technological and institutional dimensions of ODR platforms; accreditation, cybersecurity, algorithmic accountability, and user protection; leaving substantive arbitration, mediation, and data-protection matters to the existing statutory regimes. A clear explanation of jurisdiction, supported by mechanisms for inter-regulatory cooperation, would prevent duplication and conflict.

6.7 ANTICIPATING OBJECTIONS

The proposal is not immune to objection. It may be argued that ODR in India remains at a growing stage, and that premature or heavy-handed regulation could restrain innovation, deter new applicants, and impose disproportionate compliance costs on smaller platforms.

³¹ Colin Rule, *Online Dispute Resolution for Business* 145–160 (Jossey-Bass 2002).

³² Arbitration and Conciliation Act, No. 26 of 1996, §§ 43A–43M (Part IA, inserted by the Arbitration and Conciliation (Amendment) Act, 2019); the Arbitration Council of India has not yet been constituted.

³³ Digital Personal Data Protection Act, No. 22 of 2023, §§ 18–26, India Code (2023); Digital Personal Data Protection Rules, 2025 (notified Nov. 14, 2025).

Indian policy discourse has for this reason generally favored a phased, largely industry-led approach.³⁴

These concerns are legitimate but not critical. The purpose of the proposed framework is not to over-regulate but to establish a minimum baseline of accountability, accreditation, cybersecurity, confidentiality & transparency calibrated to the size and risk profile of different platforms. A responsive, light-touch model incorporating co-regulation and self-regulatory standards developed in consultation with industry can secure user trust without suppressing innovation. The European experience suggests that the greater risk lies not in regulation as such, but in frameworks that fail to sustain participation and confidence.

7. CONCLUSION

ODR represents the future of dispute resolution, but its long-term legitimacy will depend not only upon technological innovation but upon effective governance. India's existing legal framework provides a foundation for ODR, yet remains insufficient to regulate the technological and institutional challenges of digital dispute resolution. A dedicated framework supported by an independent ODR Regulatory Authority can bridge this gap by ensuring accountability, transparency, user protection, and public trust, enabling India to harness the benefits of technology while preserving the fundamental principles of fairness and access to justice.

RECOMMENDATIONS

- i. A dedicated ODR Regulatory Authority should be established through parliamentary legislation. A uniform accreditation framework should be introduced for ODR service providers.
- ii. Sector-specific cybersecurity and confidentiality standards should be developed for ODR platforms.
- iii. Comprehensive guidelines governing AI-assisted dispute resolution should be formulated.
- iv. Mechanisms ensuring transparency and platform accountability should be implemented.
- v. Multilingual and accessible ODR systems should be promoted to reduce digital exclusion.

³⁴ See NITI Aayog, Designing the Future of Dispute Resolution: The ODR Policy Plan for India (2021).

- vi. Continuous stakeholder consultation should be encouraged to ensure adaptive and technology-responsive regulation.

BIBLIOGRAPHY

Books

1. Cortés, Pablo. *Online Dispute Resolution for Consumers in the European Union*. Routledge, 2010.
2. Katsh, Ethan & Janet Rifkin. *Online Dispute Resolution: Resolving Conflicts in Cyberspace*. Jossey-Bass, 2001.
3. Rule, Colin. *Online Dispute Resolution for Business: B2B, E-Commerce, Consumer, Employment, Insurance, and Other Commercial Conflicts*. Jossey-Bass, 2002.

Journal Articles

1. Katsh, Ethan & Orna Rabinovich-Einy, "Artificial Intelligence and Dispute Resolution: Opportunities and Challenges," 21 *Cardozo Journal of Conflict Resolution* 297 (2020).
2. Katsh, Ethan & Orna Rabinovich-Einy, "Digital Justice: Reshaping Boundaries in an Online Dispute Resolution Environment," 1 *International Journal of Online Dispute Resolution* 5 (2014).
3. Cortés, Pablo, "The Future of Online Dispute Resolution," 21 *Computer Law & Security Review* 76 (2005).
4. Rule, Colin, "Making Peace on eBay: Resolving Disputes in the World's Largest Marketplace," 28 *University of Toledo Law Review* 1 (2007).

Reports and Policy Documents

1. Agami, NITI Aayog & Omidyar Network India, *The ODR Handbook: Unlocking ODR for the Nation* (2021).
2. NITI Aayog, *Designing the Future of Dispute Resolution: The ODR Policy Plan for India* (2021).
3. NITI Aayog, *Online Dispute Resolution: Shifting from Disputes to Resolution* (2020).
4. Reserve Bank of India, Online Dispute Resolution (ODR) System for Digital Payments, RBI/2020-21/21 (Aug. 6, 2020).

National Judicial Data Grid, Department of Justice, Government of India,
<https://njdg.ecourts.gov.in.Statutes>

1. Arbitration and Conciliation Act, No. 26 of 1996, India Code (1996).

2. Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
3. Information Technology Act, No. 21 of 2000, India Code (2000).
4. Mediation Act, No. 32 of 2023, India Code (2023).
5. Consumer Protection Act, No. 35 of 2019, India Code (2019).
6. Consumer Protection (E-Commerce) Rules, 2020, G.S.R. 462(E) (India).
7. Digital Personal Data Protection Rules, 2025 (India).

International Instruments

1. Regulation (EU) No. 524/2013 of the European Parliament and of the Council of 21 May 2013 on Online Dispute Resolution for Consumer Disputes, 2013 O.J. (L 165) 1.
2. UNCITRAL Model Law on International Commercial Arbitration, 1985 (as amended in 2006).
3. UNCITRAL Technical Notes on Online Dispute Resolution, 2016.
4. Regulation (EU) 2024/3228 of the European Parliament and of the Council of 19 December 2024 repealing Regulation (EU) No 524/2013.
5. Civil Resolution Tribunal Act, S.B.C. 2012, c. 25 (Canada, British Columbia).
6. Provisions of the Supreme People's Court on Several Issues Concerning the Trial of Cases by Internet Courts, 2018 (China).

Cases

1. State of Maharashtra v. Praful B. Desai, (2003) 4 SCC 601.
2. Trimex International FZE Ltd. v. Vedanta Aluminium Ltd., (2010) 3 SCC 1.
3. Shakti Bhog Foods Ltd. v. Kola Shipping Ltd., (2009) 2 SCC 134.