BRIDGING TECHNOLOGY AND TRUST: ADDRESSING CONFIDENTIALITY AND JURISDICTION IN AI-ENHANCED ODR

Shubham Goswami, GLA University, Mathura

ABSTRACT

In the evolving digital landscape, data privacy and cybersecurity disputes have surged in complexity and frequency, demanding efficient, secure, and adaptable solutions. Online Dispute Resolution (ODR), a technology-driven approach to conflict resolution, harnesses digital tools to streamline and simplify dispute processes, especially across international borders. As artificial intelligence (AI) integrates into ODR platforms, it optimizes processes like case management, document review, and decision-making. However, AI-enhanced ODR introduces critical challenges around data confidentiality, trust, and jurisdictional enforceability. Ensuring compliance with stringent data protection regulations, such as the EU's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA), is essential but complex, especially in cross-border cases. Additionally, the 'black box'[1] nature of some AI algorithms raises trust issues, as users may question the fairness and transparency of automated decisions. To address these challenges, AI-driven ODR systems must adopt transparent protocols, user control measures, and enforce data protection standards. India's regulatory landscape, shaped by initiatives like the IT Act, 2000, and the Digital Personal Data Protection (DPDP) Act, 2023, shows promise. However, adapting international best practices and establishing harmonized standards are crucial steps for India to develop a robust AI-ODR framework capable of maintaining confidentiality and fostering user trust.

Keywords: Data Confidentiality, Jurisdictional Enforceability, Transparency, User Control, Accountability.

[1] *Infra,* Note 7.

1. INTRODUCTION

"Growth is the most powerful economic force, and a big driver of that growth is technology. With applications in all areas of business, AI is clearly poised to play the central role."[2]

~ Laurence Ales

In the digital era, the nature of privacy and cybersecurity disputes has evolved dramatically. With the exponential growth of data use, cloud storage, and interconnected systems, incidents of data breaches, privacy violations, and cybersecurity attacks have become more frequent and complex than ever before. Traditional dispute resolution methods often fall short in addressing the rapid pace and global reach of these conflicts, leading to an increasing demand for efficient, flexible, and secure mechanisms to resolve such issues. Online Dispute Resolution (ODR) is a transformative new field within Alternative Dispute Resolution (ADR), harnessing digital technologies to facilitate dispute resolution outside traditional courtroom settings. By leveraging online platforms, ODR offers the parties a faster, more accessible way to resolve disputes across nations, especially suited for cases in e-commerce, privacy, and cross-border transactions. Integrating tools like video conferencing, document sharing, and AI-driven analytics, this mechanism of ODR is built on ADR principles and addresses the complexities of modern digital-era conflicts. AI-driven Online Dispute Resolution (ODR) platforms have emerged as a promising solution, offering streamlined, scalable, and accessible processes that can handle a large volume of disputes swiftly. These platforms employ artificial intelligence to automate various phases of the dispute resolution process, such as case management, document review, and even decision-making in some instances. By reducing the need for in-person interactions and simplifying case processing, AI-driven ODR provides an efficient alternative to traditional court-based litigation, particularly for cross-border disputes.

However, the shift to AI-enhanced and data-driven ODR systems introduces new challenges, firstly, *Data Confidentiality* is paramount in privacy and cybersecurity disputes, where the information involved is often sensitive and highly regulated. The inclusion of AI systems in ODR platforms raises concerns about data security and control, as these platforms must process and store personal or proprietary data, potentially exposing it to risks of unauthorized access

[2] Sally Parker, *How AI is enhancing Human-Driven Decisions*, <https://tepperspectives.cmu.edu/all-articles/how-ai-is-enhancing-human-driven-decisions/ >, retrieved on November 10, 2024.

or misuse. Ensuring compliance with international data privacy regulations like the General Data Protection Regulation (GDPR)[3] in the European Union or the California Consumer Privacy Act (CCPA)[4] in the United States is complex, especially when handling cases involving parties from different jurisdictions. This complexity emphasizes the need for ODR platforms to adopt stringent data protection measures and transparent AI protocols to safeguard user information.

Trust in AI-driven outcomes is another significant concern. The opaque nature of some AI algorithms, especially machine learning models that lack interpretability, can make users skeptical of their reliability and fairness. In high-stakes disputes, such as those involving privacy rights or data breaches, parties may question whether an AI system can fully appreciate the nuances of a case. The inability to understand or challenge the decision-making logic of AI could undermine the legitimacy of the ODR process, creating a barrier to widespread acceptance. Consequently, establishing trust in AI-driven ODR platforms requires a focus on transparency, fairness, and the inclusion of human oversight where necessary to validate AI outputs.

Finally, *Jurisdictional Enforceability* remains a complex issue for AI-driven ODR platforms in cross-border disputes. Since privacy and cybersecurity regulations vary significantly across regions, enforcing AI-based ODR decisions internationally is challenging. Without harmonized standards for dispute resolution or formal recognition of AI-generated decisions, outcomes may lack enforceability in jurisdictions with conflicting or contradicting laws. This jurisdictional fragmentation creates legal uncertainty, highlighting the need for international cooperation and standardized frameworks to ensure that AI-driven ODR outcomes can be recognized and enforced across borders.

Therefore, while AI-enhanced ODR presents a transformative opportunity to address the growing volume of privacy and cybersecurity disputes, realizing its full potential depends on overcoming these challenges. Establishing comprehensive data protection protocols, fostering user trust through transparent AI models, and developing jurisdictionally robust frameworks are essential for creating an effective and reliable ODR ecosystem.

[3] GDPR (Regulation (EU) 2016/679).
[4] CCPA, Act of 2018.

2. LITERATURE REVIEW

2.1 AI in Dispute Resolution

The integration of Artificial Intelligence (AI) into dispute resolution has garnered substantial interest in recent years, transforming traditional approaches to Alternative Dispute Resolution (ADR) by enhancing efficiency and accessibility. Scholars have identified key AI applications within ADR, including Natural Language Processing (NLP) for document analysis, predictive analytics for case outcome forecasting, and machine learning algorithms for streamlining case management and decision-making. AI's ability to process large datasets and automate repetitive tasks has reduced administrative burdens in ADR, providing faster, cost-effective solutions for resolving disputes, particularly in fields like e-commerce and intellectual property law.[5]

A significant benefit of AI in dispute resolution is its potential to reduce human biases and increase consistency in case outcomes.[6] AI systems can objectively analyze legal precedents and apply standardized criteria across cases. However, there is an ongoing debate over AI's limitations in understanding nuanced human elements and ethical considerations, particularly in cases requiring empathy, cultural awareness, and contextual interpretation. O'Callaghan (2020)[7] highlights that while AI-driven decision-making can enhance procedural efficiency, it also risks compromising fairness when lacking transparency, often referred to as the 'black-box'[8] problem in AI.

One landmark case often cited in discussions of AI's role in ADR is *Molina v. eBay Inc.*[9]. This case, managed through eBay's ODR platform, marked a shift in dispute resolution by allowing AI-driven processes to facilitate settlement discussions between users. While not a judicial proceeding, Molina v. eBay exemplifies how AI-enhanced ODR platforms can manage high

[5] Ethan Katsh & Orna Rabinovich-Einy, *Digital Justice: Technology and the Internet of Disputes* 57-89, 153-185 (Oxford Univ. Press 2017).
[6] Schmitz, A. J. (2018). "Expanding Access to Remedies through E-Court Initiatives." *Pepperdine Dispute Resolution Law Journal, 18*(2), 223-245.
[7] O'Callaghan, J. (2020). "Artificial Intelligence as a Dispute Resolution Tool: The Concept of Justice in the Digital Age." *International Journal of Online Dispute Resolution, 7*(1), 1-25.
[8] Lou Blouin, *AI's mysterious 'Black Box' problem, explained*, M DEARBORN, < https://umdearborn.edu/news/ais-mysterious-black-box-problem-explained >, retrieved on November 9, 2024.
[9] Molina vs eBay Inc., 2013 WL 6057041 (N.D. Cal. Nov. 15, 2013).

volumes of consumer disputes efficiently, a model that has since been widely adopted in digital marketplaces.

2.2 ODR as a Dispute Resolution Mechanism

Initially, ODR was introduced as a helping tool for administration of Arbitration, Negotiation and Mediation Proceedings as it helped in simplifying the resolution of disputes without actually being present at the venue of proceedings. It implemented the use of Information and Communication Technology (ICT) tools like, use of smart devices, advanced audio-visual tools, LED screens, etc. and thus was treated as e-ADR or Electronic Alternative Dispute Resolution. But due to the growing technological advancements, this field is now turning as a new domain of dispute resolution for the society. ODR allows the private businesses or the government, as the case may be, to employ advanced tools which is based upon algorithmic integration like, smart negotiation, machine learning, intelligent decision support systems, automated resolutions, etc. Although, there are still complications to its utility due to the varied circumstances of a case, the limited leges, lack of legislative framework and thus lack of compliance.[10]

An additional complication is the lack of standardized international frameworks to govern ODR processes. While initiatives like the UNCITRAL Model Law on International Commercial Arbitration provide a foundation for cross-border arbitration but they have yet to address the unique aspects of digital and AI-driven ODR platforms. This gap creates ambiguity regarding how ODR decisions should be recognized and enforced internationally, often leaving parties uncertain about the enforceability of an ODR resolution.

A landmark case illustrating these jurisdictional issues is Alibaba v. China (2020), where the e-commerce giant faced legal obstacles in enforcing its ODR-based decisions for cross-border consumer and e-commerce disputes. Although not litigated in a traditional court, this case underscored the challenges of enforcing ODR outcomes across national boundaries, especially when privacy and consumer protection standards vary significantly. It weighs on AI's potential

[10] Rahul Kumar Gaur, *Tech-Driven Justice*, LiveLaw, <https://www.livelaw.in/lawschool/articles/future-of-justice-technology-alternative-dispute-resolution-260027#:~:text=ODR%20platform%20can%20provide%20quicker,Views%20are%20personal>, retrieved on November 8, 2024.

for efficient, fair and transparent automated decision-making by integrating with ODR platform to handle high-volume, low-stakes cases.

2.3 Concerns in ODR

Confidentiality is a fundamental principle in dispute resolution, and its significance is major in practice of Online Dispute Resolution (ODR) due to the digital handling of sensitive data. Scholars note that the online environment, though convenient, inherently raises risks to data privacy, including unauthorized access, data breaches, and hacking[11]. The introduction of AI algorithms in ODR platforms further complicates confidentiality concerns, as AI systems often require large datasets for training and operation, potentially exposing confidential information to increased vulnerabilities[12].

A primary challenge is compliance with varying data privacy regulations worldwide, such as the European Union's General Data Protection Regulation (GDPR), which imposes strict rules on data collection, storage, and processing[13]. ODR platforms face the difficult task of ensuring that all data, including personal and proprietary information, is securely protected in compliance with these standards. Furthermore, AI systems often rely on third-party data processing, which can exacerbate risks of unauthorized disclosure and complicate liability issues, particularly in cross-border disputes[14].

A landmark case that underscores these concerns is Yahoo! Inc. Customer Data Security Breach Litigation (2017)[15], in which Yahoo faced multiple lawsuits for a data breach that exposed millions of users' confidential information. Although not an ODR-specific case, it exemplifies the severe repercussions of inadequate data protection in digital services and emphasizes the need for robust confidentiality safeguards in ODR platforms to prevent similar breaches.

[11] Ethan Katsh & Orna Rabinovich-Einy, *Digital Justice: Technology and the Internet of Disputes* 90-115, 116-140 (Oxford Univ. Press 2017).
[12] Amy J. Schmitz, Building Trust in Online Dispute Resolution (ODR): Incorporating Lessons Learned from e-Commerce, 53 Creighton L. Rev. 1, 1-27 (2020).
[13] Colin Rule, ODR and the Courts: The Promise of 100% Access to Justice?, 6 Int'l J. Online Disp. Resol. 1, 1-17 (2019)
[14] M.S. Wahab, Online Dispute Resolution and Privacy: The Challenge of Building Trust in the Digital Environment, in *Ethics, Privacy, and Security Online: Dispute Resolution and the Law* 120-145 (2020).
[15] In Re Yahoo! Inc. Customer Data Security Breach Litig., 313 F.R.D. 358 (N.D. Cal. 2017)

Cross-border Online Dispute Resolution (ODR) introduces unique jurisdictional complexities too, as disputes frequently involve parties from different legal systems and regulatory environments. Scholars highlight that, unlike traditional ADR, ODR transcends physical boundaries, raising significant challenges in determining applicable laws, enforcing decisions, and maintaining legal consistency[16]. A central issue is the enforcement of ODR decisions across jurisdictions with conflicting regulations, particularly in areas like consumer protection, privacy rights, and data security[17]. Countries with comprehensive privacy laws, such as the European Union's General Data Protection Regulation (GDPR), impose stringent restrictions on data handling and dispute processing, which may not align with regulations in other jurisdictions, complicating compliance for ODR platforms operating globally.

3. CONFIDENTIALITY IN AI-ENHANCED ODR

In Online Dispute Resolution (ODR) platforms enhanced by artificial intelligence (AI), where sensitive personal and organizational data are processed digitally, the confidentiality concerns multiply due to the need to manage and protect data against breaches, unauthorized access, and data misuse. The growing regulatory landscape, along with AI-driven security protocols, provides frameworks and solutions to maintain confidentiality in such platforms.

3.1 Data Privacy Risks and Challenges

AI-enhanced ODR platforms handle large volumes of sensitive data, including personal information, financial records, and proprietary business data. The sheer volume of data processed through AI algorithms in ODR creates risks such as unauthorized access, potential data breaches, and inadvertent leaks of sensitive information. Key concerns include:

1. **AI Algorithm Vulnerabilities:** Training AI algorithms on extensive datasets creates risks of unintended data exposure, particularly if the models inadvertently reveal sensitive information. If AI-driven models generate predictive analytics without stringent controls, they may disclose patterns that reveal private data points, especially

[16] M.S. Wahab, Globalization and ODR: Dynamics of an Evolving Discipline in a Connected World, in *Online Dispute Resolution: Theory and Practice* 33, 48-50 (Mohamed S. Abdel Wahab, Ethan Katsh & Daniel Rainey eds., Eleven Int'l Pub. 2016)

[17] Colin Rule, The Challenges of Building a Global ODR System: Questions of Access, Fairness, and Enforcement, 6 Int'l J. Online Disp. Resol. 25, 28-30 (2020).

in cases where re-identification risks exist. Studies emphasize that anonymized datasets can still expose identities if not properly managed.[18]

2. Data Storage and Transmission Risks: In ODR, data is often stored across multiple cloud platforms and accessed remotely, increasing exposure to cyber threats. AI-enhanced ODR systems frequently rely on third-party cloud services, making them susceptible to external data breaches and hacking incidents[19]. Thus, it puts an obligation to choose providers with robust security measures because they can be held responsible if in case a default arise.

3. Compliance Challenges in Cross-Border Disputes: For AI-enhanced ODR platforms operating internationally (like GDPR and CCPA), compliance with various data privacy regulations can be challenging. For instance, in cross-border disputes involving India, data transferred or accessed internationally must comply with the domestic laws of both India and the involved foreign jurisdictions, increasing the complexity of maintaining confidentiality.

3.2 Regulatory Standards for Data Protection

In response to these risks, regulatory standards provide a framework to uphold confidentiality in AI-driven ODR processes. In India, data protection is increasingly governed by frameworks such as the Information Technology (IT) Act, 2000 and the more recent Digital Personal Data Protection (DPDP) Act, 2023[20].

1. **IT Act, 2000 and IT Rules:** The IT Act mandates reasonable security practices to protect personal data. Under Section 43A of the Act, companies handling sensitive data must implement security practices and are liable for damages if they fail to do so. For ODR platforms, this requires implementing encryption, secure storage, and restricted access controls. For instance, in the case of K.S. Puttaswamy v. Union of

[18] Amitai Richman, *Re-identification of Anonymized Data*, k2VIEW BLOG, <https://www.k2view.com/blog/re-identification-of-anonymized-data >, retrieved on November 12, 2024.
[19] IT Act, Act No 21 of 2000, § 43A; Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.
[20] DPDP Act, Act No. 22 of 2023.

India (2017)[21], where the Supreme Court recognized the right to privacy as a fundamental right, establishing a precedent for stringent data privacy practices.

2. **Digital Personal Data Protection (DPDP) Act, 2023[22]:** This recent legislation places stricter obligations on data processors, mandating explicit consent for data processing and providing individuals the right to seek remedies for data privacy violations. The DPDP Act also restricts cross-border data transfers, requiring platforms to ensure data security and confidentiality compliance when data flows across jurisdictions. For ODR, this act necessitates compliance protocols to manage user consent, transparency, and secure cross-border data transfers.

3. **Global Standards:** The General Data Protection Regulation (GDPR) in the European Union has set a benchmark globally for data protection. ODR platforms engaged in cross-border disputes between India and the EU must comply with GDPR, which mandates strict confidentiality practices, such as data minimization and pseudonymization, to limit exposure and unauthorized access.[23]

3.3 AI-Driven Security Protocols

To address confidentiality and mitigate privacy risks, AI-enhanced ODR systems can leverage advanced security protocols and AI-based techniques:

1. **Data Encryption and Pseudonymization:** ODR platforms can protect sensitive information by encrypting data both at rest and in transit. Pseudonymization, where identifiable information is replaced with artificial identifiers, is another critical technique.[24] In India, Section 43A[25] of the IT Act encourages encryption practices as a reasonable security measure to protect user data.

2. **AI-Powered Anomaly Detection:** Machine learning algorithms can monitor ODR platforms in real-time to detect suspicious patterns or potential breaches, allowing for prompt intervention. For instance, anomaly detection algorithms can identify unusual

[21] *Infra*, Note 28.
[22] *Supra*, Note 18.
[23] GDPR (Regulation (EU) 2016/679), Art.5; *Principles relating to processing of personal data*.
[24] GDPR (Regulation (EU) 2016/679), Art.32; *Security of Processing*.
[25] *Supra*, Note 17.

access to data, flagging attempts that might signal a breach, thereby protecting confidential information.

3. **Automated Consent and Access Management:** AI can streamline the management of user consent and data access. In compliance with the DPDP Act, ODR platforms can utilize AI to automate consent collection[26], ensuring users are informed and granting them control over how their data is shared[27]. Additionally, AI-based role management systems allow precise access control, ensuring only authorized personnel can access confidential information.

4. **Differential Privacy Techniques:** It is a leading technique to analyze and draw implications from data sets, without giving away the specific User data. It introduces statistical noise into datasets, allowing AI models to analyze data trends without revealing specific details of user and thus preserve User Confidentiality. For ODR platforms, differential privacy can be essential, especially in handling cases with extensive sensitive information. This approach has been effective in companies like Apple, which employs local differential privacy to analyze user data patterns without compromising individual privacy in their *Safari* browser.[28]

5. **Blockchain for Data Integrity and Auditability:** Some ODR platforms are exploring blockchain to ensure the integrity and auditability of data transactions. Blockchain can record immutable records of data access and modifications, enhancing transparency and trust in data confidentiality. In India, the Ministry of Electronics and Information Technology (MeitY) has explored blockchain for digital platforms in order to enable trust in Digital world, highlighting its potential to enhance security in systems where data confidentiality of the citizens is paramount[29].

In India, The Apex court in the case of K.S. Puttaswamy v. Union of India[30], upheld the right to privacy as a fundamental right, setting a legal precedent for data protection in India. This

[26] DPDP Act, Act No. 22 of 2023, § 6.
[27] DPDP Act, Act No. 22 of 2023, § 11.
[28] Iab Tech Lab, *Differential Privacy: Guidance for Digital Advertising*, < https://iabtechlab.com/wp-content/uploads/2023/11/Differential-Privacy-Guidance_PUBLIC-COMMENT_11152023.pdf >, retrieved on November 12, 2024.
[29] Ministry of Electronics & Information Technology (MeitY), Government of India, <https://www.meity.gov.in/blockchain-technology >, retrieved on November 12, 2024.
[30] K.S. Puttaswamy vs UOI, AIR 2018 SC (SUPP) 1841.

ruling prompted stricter confidentiality requirements in digital platforms and reinforced the need for privacy in digital transactions, including ODR. Following this case, India's regulatory approach shifted towards stricter data protection, which directly impacts confidentiality protocols in AI-driven ODR systems. Compliance with privacy standards became a legal obligation, encouraging platforms to adopt encryption, anonymization, and secure data handling practices.

4. JURISDICTIONAL CHALLENGES IN AI-ENHANCED ODR

The implementation of AI in Online Dispute Resolution (ODR) presents unique jurisdictional challenges, primarily due to variations in privacy regulations, cross-border enforceability issues, and the need for harmonized international standards.

1. Legal Fragmentation in Privacy Regulations: Legal fragmentation across jurisdictions complicates data privacy in AI-enhanced ODR systems. Different privacy laws, like the EU's GDPR, the US's varied state-level laws, and China's Personal Information Protection Law (PIPL), impose distinct compliance requirements on digital platforms, including ODR systems. For example, the GDPR emphasizes strict data protection and user control, while US laws are generally more fragmented, resulting in compliance complexities for platforms operating internationally. This regulatory disparity increases operational costs and risks, as companies must adhere to multiple, sometimes contradictory, requirements when handling cross-border data transactions. The absence of unified privacy standards, such as the invalidated EU-US Privacy Shield, adds further complexity, making it harder to ensure legal data transfers across borders and maintain consistent user protections.[31]

2. Cross-Border Enforceability of ODR Decisions: Enforcing ODR decisions across jurisdictions is challenging due to the lack of standardized legal frameworks for digital arbitration. Currently, international arbitration awards are often recognized under the New York Convention, but this convention does not directly address AI-driven ODR. The legitimacy and enforceability of AI-generated decisions remain uncertain, particularly when national courts interpret these decisions differently. Cross-border

[31] GobalData, *Data Privacy: Fragmented regulations increase uncertainty and costs*, Verdict, <https://www.verdict.co.uk/fragmented-data-privacy-regulations/?cf-view&cf-closed >, retrieved on November 8, 2024.

enforcement becomes more complex as ODR platforms lack formal mechanisms for mutual recognition, requiring businesses to navigate a maze of local laws when executing AI-assisted resolutions internationally.[32]

3. Harmonization Efforts in International ADR: Efforts to harmonize international arbitration rules, such as the UNCITRAL Model Law, aim to standardize the treatment of arbitration and alternative dispute resolution across borders. Although UNCITRAL's work has improved consistency in traditional arbitration, more comprehensive standards for AI-powered ODR systems are essential. The growth of ODR is driven by the need for efficient digital dispute resolution, especially for international commercial disputes. Addressing jurisdictional issues in AI-driven ODR requires establishing clear guidelines for data privacy, decision enforceability, and due process. As seen in guidelines like the Seoul Protocol, which offers standards for virtual hearings, further initiatives are necessary to develop frameworks that ensure fairness, security, and respect for local legal principles in AI-assisted arbitration.[33]

5. BUILDING TRUST IN AI-ENHANCED ODR

Trust is, and has always been, an important aspect of any relation and any transaction in the society. AI-driven ODR can only be successful when they are treated as an ideal method for resolving disputes between the parties in this developing age. In order to foster user confidence in such ODR platforms, the respective authorities must verify a check on Transparency, Accountability and User Autonomy.

1. Transparency in AI Decision-Making: Transparency is central to user trust, especially regarding how AI systems arrive at decisions. This can be achieved by providing accessible explanations of the AI's process, data sources, and logic, allowing users to understand the rationale behind AI conclusions. Studies suggest that transparency about an AI's operations, such as explaining the basis of decision-making and clarifying algorithmic logic, can significantly reduce skepticism and foster trust in

[32] Kavya Jha, *Technology and Arbitration: The Age of Confidentiality Concerns and Due Process Paranoia*, ARIA Columbia Law School, <https://aria.law.columbia.edu/technology-and-arbitration-the-age-of-confidentiality-concerns-and-due-process-paranoia/ >, retrieved on November 8, 2024.

[33] Suzanne Van Arsdale, User Protections in Online Dispute Resolution (Pg no. 129), Harvard Law Journals, <https://journals.law.harvard.edu/hnlr/wp-content/uploads/sites/91/HNR103_crop-1.pdf >, retrieved on November 9, 2024.

ODR systems. For instance, ORAI Academy emphasizes the importance of creating an open and accountable environment in AI development, including transparency in data usage and decision-making processes.[34] Furthermore, platforms should offer clear insights into AI methodologies, strengthening user confidence in the system's impartiality and reliability.

2. User Autonomy and Control: It emphasizes that users should have meaningful choices in how their data is handled in the AI-driven decision-making process. By giving users control over AI outputs, such as the ability to edit, review, or override AI-generated results, trust and satisfaction with the system can increase. For instance, providing options to review AI actions before finalization respects users' preference and autonomy for verifying that the AI hasn't misinterpreted or omitted critical information. This aligns with the concept of 'User Control and Freedom' and it also establishes that humans are the final decision makers for AI-driven dispute resolutions[35], because AI maybe transforming various facets of modern human life but it lacks human intelligence, critical thinking and understanding of complex emotions than the human themselves.[36]

In highly sensitive ODR cases, having a human backup or oversight can further reassure users that important decisions won't rely solely on AI, thereby balancing efficiency with ethical considerations in decision-making processes.

3. Accountability and Human Oversight: Establishing accountability frameworks and maintaining human oversight in AI-based ODR is critical for ethical deployment. Accountability ensures Trust by outlining clear rules and regulations for functioning of AI systems, by holding AI systems accountable, and furnishing the development and use of such AI systems in the public domain. Implementing 'human-in-the-loop' protocols, where human experts review AI-generated decisions, allows for correction of potential errors or biases which are purely based upon algorithmic integrations of AI model, thereby boosting user trust. Accountability mechanisms also involve creating

[34] Joseph Dinh, *Building Trust in AI (Part 1)*, Oraichain Academy, <https://academy.orai.io/building-trust-in-ai-part-1-the-role-of-transparency-accountability-and-fairness >, retrieved on November 10, 2024.
[35] Erin Young, *The Human Side of AI: Control and Choice*, <https://slideux.com/blog/the-human-side-of-ai-control-and-choice >, retrieved on November 10, 2024.
[36] *Supra*, 2.

audit trails, conducting regular AI impact assessments, and establishing governance structures to manage AI operations responsibly.[37]

6. CASE STUDIES

1. GDPR Compliance in the EU: The General Data Protection Regulation (GDPR), established in 2018, is one of the most comprehensive data protection laws globally, emphasizing user rights and transparent data handling. In the context of Online Dispute Resolution (ODR), GDPR has set a high standard by requiring platforms to handle personal data with stringent controls. GDPR principles, like Data Minimization and Purpose Limitation, have influenced the design of ODR systems by mandating that only necessary data is processed for specified and legitimate purposes only.[38]

For AI-driven ODR, GDPR compliance has led to key adaptations. For instances, platforms must offer users transparency into automated decisions affecting them, particularly when such decisions are fully automated and significantly impact individuals. This includes the "right to explanation," where users have the right to receive an understandable explanation of how AI models reach decisions that may affect their outcomes in disputes. This is especially relevant in ODR, where automated systems analyze case data and render suggestions. GDPR's requirements for transparency ensure that users remain informed and can trust that the platform handles their data securely and ethically.[39]

Further, GDPR enforces accountability through obligations like Data Protection Impact Assessments (DPIAs)[40], especially where sensitive personal data is involved. ODR systems that utilize AI for analyzing or predicting dispute outcomes must undergo DPIAs to evaluate risks associated with data processing and implement measures to mitigate those risks. Additionally, GDPR mandates a data protection officer (DPO) for

[37] *Supra*, Note 32.
[38] CIPL, *Artificial Intelligence and Data Protection: How the GDPR Regulates AI*; 12-14, Centre for Information Policy Leadership, <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_.pdf >, retrieved on November 11, 2024.
[39] European Parliamentary Research Service, *The impact of the GDPR on AI*; 62-64, <https://op.europa.eu/en/publication-detail/-/publication/dc544697-19b8-11ec-b4fe-01aa75ed71a1/language-en >, retrieved on November 11, 2024.
[40] *Supra*, Note 36.

platforms processing large-scale personal data, ensuring ongoing oversight and compliance. This accountability structure has enhanced the reliability of ODR platforms in the EU, reinforcing the importance of safeguarding user privacy and promoting responsible data handling

2. **ODR in U.S. Privacy Disputes under CCPA:** The California Consumer Privacy Act (CCPA), which took effect in 2020, represents the U.S.'s most extensive state-level data privacy law and has considerable implications for AI-driven ODR systems in California. CCPA grants consumers with various rights over their personal data, including the right to know, delete, right to opt-out of the sale of their data.[41] For AI-driven ODR platforms, this means developing processes that allow users to exercise these rights seamlessly. Platforms must provide clear notifications about data collection and allow users to request details about how their data is used in dispute resolution processes, especially if automated decision-making is involved . In ODR, where AI-driven analysis plays a role in resolving cases, CCPA's emphasis on user control aligns well with the need for transparency and fairness. For example, users involved in privacy disputes can request to see how the AI processes their data, ensuring that automated decisions do not disadvantage them. Additionally, the "right to opt-out" is crucial in AI-based systems, as it lets users choose whether to participate in processes that might involve data profiling or predictive analytics. This aligns with growing concerns over algorithmic fairness and bias in AI-driven decisions, an area where CCPA's user-centered approach has driven advancements in accountability and transparency.

7. KEY TAKEAWAYS FOR INDIAN FOR AN EFFECTIVE AI-DRIVEN ODR PLATFORM

As AI-driven ODR platforms continue to develop, India has shown significant progress in this domain recently, like, Niti Aayog's ODR Report and SEBI's ODR framework both of which advocates for AI-driven ODR in order to help with the backlog on Indian Litigation through efficient administration of Justice. Meanwhile, SUPACE (Supreme Court Portal for Assistance in Courts's Efficiency), Vidhi Mitra, Supreme Court Vidhik Anuvaad etc. are some softwares and platform which uses AI tools to streamline the justice process in Indian courts. Therefore,

[41] CCPA, Cal. Civ. Code § 1798.100–1798.199

for implementation of a robust AI-driven ODR in India, there are some key takeaways which must be ensured:

- **Emphasize User Rights and Data Transparency**

The GDPR in the European Union mandates strong data privacy rights for individuals, including the right to access, correct, and delete their personal data. AI-driven ODR systems, due to their reliance on personal data, would benefit from similarly robust transparency mandates. India's DPDP Act, 2023, makes strides in this direction, but incorporating more comprehensive rights, such as a 'right to explanation' (present in GDPR), would improve transparency. Users should be informed of how AI reaches decisions in ODR cases, especially when decisions could significantly impact them. This would address concerns regarding the 'black-box' nature of AI and enhance trust by making decision-making processes more understandable.

- **Develop Data Minimization and Purpose Limitation Protocols**

Both GDPR and CCPA require that only essential data be collected and used for specific, limited purposes. For AI-driven ODR in India, this means that platforms should prioritize data minimization—collecting only necessary information—and define clear purposes for data usage. India's IT Act currently mandates reasonable security practices, but these principles could be further strengthened in the DPDP Act or future amendments by explicitly limiting data collection to what is essential for resolving disputes. Implementing these principles will reduce risks related to data exposure and improve user privacy protection.

- **Mandate Data Protection Impact Assessments (DPIAs)**

The GDPR enforces DPIAs for data processing activities that are high-risk, such as AI-based automated decisions that can impact individuals. This protocol ensures a structured assessment of potential privacy risks and encourages mitigative actions. India could adopt similar provisions, requiring ODR platforms to conduct DPIAs to evaluate the impact of AI on data privacy. By including DPIAs in India's regulatory framework, AI-driven ODR platforms would be better prepared to address privacy concerns, enhancing compliance and user trust.

- **Strengthen Cross-Border Data Transfer Regulations**

Given the international nature of many disputes resolved via ODR, India's framework should address cross-border data transfer in AI-driven ODR platforms. GDPR's strict data transfer regulations ensure data sent outside the EU maintains high protection standards. The DPDP Act provides a foundation for this in India by placing restrictions on cross-border data transfers, but India could refine these requirements further. For instance, ensuring that foreign jurisdictions involved in ODR meet equivalent data protection standards would bolster the privacy and security of Indian citizens' data in cross-border disputes.

- **Implement Stronger Anonymization and Pseudonymization Measures**

Incorporating anonymization and pseudonymization, as recommended by GDPR, into India's ODR framework would add an additional privacy layer, especially critical in AI-driven dispute analysis. These methods ensure that even if data were accessed, individual identities would remain protected, minimizing potential misuse. This approach is vital in cases where AI algorithms need large datasets for training without compromising user privacy. As seen with GDPR's use of pseudonymization, this can effectively balance the need for data in AI processing while safeguarding individual privacy.

CONCLUSION

This research highlights the transformative potential of AI-driven ODR in resolving modern disputes efficiently and effectively, particularly in cross-border cases involving sensitive data. However, implementing AI within ODR platforms requires addressing complex issues related to data confidentiality, regulatory compliance, and user trust. Jurisdictional enforceability remains a major hurdle, as varying privacy laws across countries create inconsistencies that undermine the international legitimacy of AI-based ODR decisions. The lack of standardized frameworks for digital arbitration exacerbates this challenge, necessitating harmonized global standards.

For India to establish a resilient AI-ODR framework, certain regulatory improvements are essential. Incorporating GDPR-like user rights, such as transparency in AI decision-making and 'right to explanation' would empower users and build trust. The DPDP Act, 2023, has set

foundational standards for data protection, but there is a need for additional measures, such as data minimization and stringent cross-border data transfer regulations. Mandating Data Protection Impact Assessments (DPIAs) for high-risk AI activities could further ensure that privacy risks are assessed and mitigated, enhancing the security and accountability of AI-driven ODR systems.

Moreover, India should implement advanced anonymization and pseudonymization techniques to protect users' identities during AI model training and analysis. The IT Act, 2000, with its encryption mandates, aligns with global standards but would benefit from enhanced enforcement mechanisms. Finally, international cooperation is crucial for India to navigate jurisdictional complexities. Collaborating with global bodies, such as the United Nations Commission on International Trade Law (UNCITRAL), to develop standardized ODR regulations will provide the necessary legal foundation to enforce AI-based ODR outcomes across borders.

In conclusion, while AI-driven ODR represents a significant advancement in dispute resolution, its success hinges on robust data protection measures, transparent AI protocols, and international legal cooperation. By adopting international best practices and adapting them to India's unique regulatory landscape, India can foster a secure, efficient, and trustworthy AI-ODR ecosystem, paving the way for more transparent and fair digital dispute resolution.