

Online Dispute Resolution Platforms (ODR): A Legal and Technical Perspective

María Concepción Rayón Ballesteros¹, José Luis González Ávila²

¹Professor of Law at the Complutense University of Madrid, Registered Mediator at the Ministry of Justice, Doctor of Law and Graduate in Political Sciences and Public Administration; ²Professor in the Department of Computer Science at the University of La Laguna, Civil Servant of the Autonomous Community Government of the Canary Islands, Project Manager for the Administrative Procedures Processing Platform, Tutor in Industrial Engineering at the National University of Distance Education (UNED)

Abstract

Online Dispute Resolution (ODR) platforms have emerged as a crucial tool in the digital age, addressing the need for efficient conflict resolution in e-commerce and cross-border transactions. This paper examines ODR platforms from legal and technical perspectives, exploring their role in modernising alternative dispute resolution (ADR) mechanisms. The paper analyses the legal frameworks governing ODR, including international regulations and national legislation. It also investigates the technical aspects of ODR platforms, such as user interface design, data security, and the integration of artificial intelligence in dispute resolution processes. By synthesising legal and technical insights, this paper contributes to understanding ODR platforms as a multifaceted solution for enhancing access to justice in the digital marketplace. It concludes with recommendations for policymakers, technologists, and legal practitioners to foster the development of effective and equitable ODR systems.

Keywords

ADR • alternative dispute resolution • conflict • consumer protection • mediation, ODR, online dispute resolution

1. Introduction

In the vast and dynamic landscape of digital mediation platforms, the role of technology has evolved from being merely ancillary to becoming the cornerstone of contemporary conflict resolution systems. Incorporating artificial intelligence and other technological advancements has ushered in a new era where interactions between parties are more efficient, secure, and precise. This convergence of mediation and technology has driven a qualitative leap in managing disputes, enabling greater personalisation, automation, and protection of communication processes, all framed within the fundamental principles of privacy and information security.

The development of these platforms, particularly with the integration of artificial intelligence, offers unprecedented capabilities. Not only are the time and resources required for mediation optimised, but AI also opens the door to new forms of predictive analysis based on patterns and precedents stored in vast databases. These platforms are designed to offer increasingly precise and contextualised solutions, capable of anticipating responses and offering proposals tailored to the specifics of each conflict. Through machine learning and big data, these tools provide greater accuracy and foster an environment more conducive to transparency and objectivity.

However, the growing technological sophistication brings with it an ethical and technical imperative: the need to guarantee the inviolability of data. The confidentiality of the parties and the protection of sensitive information must be at the core of any modern mediation platform. To this end, rigorous security systems, such as encryption via SSL/TLS certificates, have been implemented to ensure that all communications are encrypted and secured during every interaction. Likewise, data encryption on servers and hierarchical access management based on user profiles further reinforce information protection, aligning with the strictest international standards, such as those defined by the General Data Protection Regulation (GDPR). These mechanisms, along with the adoption of secure document repositories and archiving systems, form the pillars upon which the integrity and reliability of today's digital mediation platforms rest.¹

¹ Elisavetsky, A., and Marun, M. V. "Transformación digital de la mediación Praxis en Hispanoamérica" [Digital Transformation of Praxis Mediation in Latin America]. *International Journal of Online Dispute Resolution*, 9(1) (2022): 93–99. <https://doi.org/10.5553/IJODR/235250022022009001008>

[†] Corresponding author: María Concepción Rayón Ballesteros

E-mail: mariaconcepcionrayon@gmail.com

Open Access. © 2024 María Concepción Rayón Ballesteros, José Luis González Ávila, published by Sciendo
 This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 License.

2. Conceptual Framework of ODR Platforms

Online Dispute Resolution (ODR) represents a paradigm shift in conflict resolution, leveraging digital technologies to facilitate the settlement of disputes in the virtual realm. Unlike traditional Alternative Dispute Resolution (ADR) mechanisms, which typically involve face-to-face interactions, ODR operates entirely within digital platforms, transcending geographical boundaries and temporal constraints. This innovative approach encompasses a spectrum of methodologies, including online negotiation, mediation, and arbitration, each adapted to the digital context. ODR platforms often incorporate sophisticated technologies such as artificial intelligence algorithms for case assessment, blockchain for secure record-keeping, and natural language processing for communication facilitation. From a legal perspective, ODR platforms occupy a unique position within national and international legal frameworks, necessitating careful consideration of jurisdictional issues and the enforceability of outcomes.² The UNCITRAL Technical Notes on ODR³ provide a foundational framework for developing and implementing ODR systems, addressing key aspects such as impartiality, transparency, and due process in the digital sphere. ODR is a “mechanism for resolving disputes through electronic communications and other information and communication technology”. The Technical Notes aim to foster the development of ODR and assist ODR administrators, platforms, neutrals, and parties involved in ODR proceedings. They are intended for use in cross-border, low-value sales, or service contracts concluded using electronic communications. The Technical Notes reflect approaches to ODR systems that embody impartiality, independence, efficiency, effectiveness, due process, fairness, accountability, and transparency. They outline a multi-stage ODR process, including negotiation, facilitated settlement, and a final stage (which may include arbitration).⁴ The Technical Notes emphasise the role of technology, particularly the use of an ODR platform for all communications during proceedings.

3. Technical Infrastructure of ODR Platforms

The technical infrastructure of Online Dispute Resolution (ODR) platforms stands as a fundamental pillar for the effective functioning of these systems, which aim to provide alternative solutions to traditional judicial proceedings tailored to the demands of the digital age. In this context, a structure is required that not only meets the requirements of efficiency, security, and accessibility but is also capable of integrating cutting-edge technologies that enable the dynamic and automated management of disputes. These platforms have become highly complex scenarios, where not only technological demands converge but also user expectations, as individuals seek a swift and fair resolution of their conflicts without needing to submit to conventional courts' rigidity.

To achieve this goal, ODR systems must incorporate a sophisticated technological architecture that allows for precise information exchange and decision-making management. In this regard, the integration of expert systems plays a crucial role. These systems must be capable of processing and managing the requests of the parties involved in a dispute, acting as autonomous mediators that facilitate dialogue and promote rapprochement between opposing positions. The mediation of requests is one of the most relevant competencies of these platforms, as by attempting to bridge the gap between the divergent positions of the parties, the possibilities of reaching a mutually satisfactory solution are optimised.

In this regard, the ability of ODR platforms to bring positions closer cannot rely exclusively on human intervention. While mediators and arbitrators play a fundamental role, the scale at which these platforms operate and the volume of disputes they handle necessitate that automated technological solutions take on a significant part of the mediation process. This is where expert systems come into play, providing analyses based on historical data, behavioural patterns, and prior outcomes, all to suggest resolution pathways tailored to the particular circumstances of each conflict. These systems evaluate the merits of opposing positions and offer recommendations to maximise the potential for consensus among the parties.

Another crucial aspect of the technical infrastructure of ODR platforms is the integration of blockchain⁵ and smart contracts, emerging technologies that promise to revolutionise how these platforms manage and execute decisions. With its ability to

² Markovnikov Zunko, I. “Implementation of the ODR (ON line Dispute resolution) Platform according to the regulation (EU) no 524/2013 On line dispute resolution for consumer disputes,” Economic and Social Development, Book of Proceedings (Sep 1/Sep 2, 2016): 264 y 265.

³ The UNCITRAL Technical Notes on Online Dispute Resolution (ODR) are a non-binding, descriptive document adopted by the United Nations Commission on International Trade Law (UNCITRAL) in 2016. These Technical Notes guide implementing ODR systems for cross-border e-commerce disputes, particularly those involving low-value sales or service contracts. These notes are available at this link: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/v1700382_english_technical_notes_on_odr.pdf

⁴ Montesinos García, A., and Barona Vilar, S. *Arbitraje y nuevas tecnologías [Arbitration and New Technologies]* (1. ed). Thomson Civitas. (2007).

⁵ De Filippi, P., and Hassan, S. “Blockchain Technology as a Regulatory Technology: From Code to Law.” *First Monday*, 21(12) (2016) <https://doi.org/10.5210/fm.v21i12.7113>

immutably record all transactions and decisions, blockchain adds transparency and trust to the process. Smart contracts, on the other hand, allow for the automatic execution of agreements once the agreed conditions are met, thereby eliminating the need for manual intervention and significantly reducing resolution times.⁶

Nevertheless, the implementation of these technologies also presents certain technical challenges. One of the most significant is the interoperability between different legal systems, especially in cross-border disputes, where differences in data protection regulations and privacy laws can lead to complications. The need to comply with regulations such as the General Data Protection Regulation (GDPR)⁷ in Europe requires ODR platforms to manage personal data efficiently and securely, ensuring compliance with applicable laws in each jurisdiction.

In this context, using an expert system facilitates the mediation of requests and plays a fundamental role in data protection. These systems can act as guardians of information, constantly monitoring data flows and ensuring that the highest standards of security and privacy are upheld. Moreover, expert systems can detect anomalous patterns in user behaviour or data flow, enabling them to identify and mitigate potential security vulnerabilities before they escalate into serious issues.

Finally, it is important to note that the success of ODR platforms depends on their capacity to evolve and adapt to the technical challenges that arise over time. The technical infrastructure of these platforms must undergo constant review and improvement to ensure that it keeps pace with the latest technologies and remains relevant in an ever-changing legal and technological landscape. Implementing expert systems and automating mediation are the first steps in a continuous evolution towards smarter, more secure, and efficient platforms. The ODR systems of the future will not only resolve disputes more quickly and efficiently. Still, they will also be capable of anticipating conflicts and offering proactive solutions based on data analysis and artificial intelligence.

3.1. Technological Components

The technical infrastructure of Online Dispute Resolution (ODR) platforms cannot be merely limited to integrating technologies that ensure efficiency, security, and accessibility; it must be conceived as a deeply collaborative ecosystem that promotes fluid interaction among its various components and users. Adopting a technical architecture grounded in microservices is imperative to achieve this ideal. These enable greater modularity and scalability and facilitate collaborative environments where different parties can participate synergistically, optimising the management of the conflict itself and the user experience.

These artificial intelligence tools can, for example, guide users in the proper formulation of their requests or in structuring their arguments, which becomes crucial when parties do not have legal representation. Simultaneously, artificial intelligence can offer legislative suggestions based on the laws applicable to the specific case, personalising responses and ensuring that users understand their rights and the limits of potential resolutions.

In an environment where collaboration is key, these platforms must facilitate mediation and constructive dialogue between conflicting parties, helping them to bridge their positions and find common ground. The ability of an expert system to manage requests, analyse the parties' positions, and offer suggestions based on precedents is fundamental to this process. Nevertheless, for mediation to be truly effective, collaborative tools must be integrated to become practically invisible to users, operating intuitively and naturally. In this way, participants can focus on resolving the conflict rather than on technology.

The use of advanced visual technologies, such as AngularJS, allows the platform to have a modern and appealing appearance, enhancing the user experience and making it more accessible, even for those who have no prior experience with digital platforms. However, usability-focused design must prevail beyond the visual, ensuring that the available tools respond promptly to user needs. In this regard, every platform aspect must be designed to provide a coherent and comprehensible experience, with clear navigation and functionalities anticipating user actions, facilitating access to relevant information without requiring extensive or confusing searches.

3.2. Digital interfaces: user accessibility and design.

Furthermore, storing and managing these platforms' data is crucial for their success. With its flexible and scalable structure, MongoDB provides an ideal solution for efficiently managing large volumes of information. The non-relational nature of MongoDB allows data to be stored in a way that enables quick retrieval and manipulation, providing the platform with the agility necessary to respond to the changing demands of users and, more importantly, ensuring the security and confidentiality of information—essential elements in any dispute resolution environment. Integrating databases like MongoDB into the infrastructure of these

⁶ Ustun, E. S., Yuce, M., and 2022 IEEE 24th Conference on Business Informatics (CBI) Amsterdam, Netherlands 2022 June 15 - 2022 June 17. (2022). Smart Legal Contracts & Smarter Dispute Resolution. In 2022 IEEE 24th Conference on Business Informatics (CBI) (Vol. 02, Issue CBI, pp. 111–117). <https://doi.org/10.1109/CBI54897.2022.10056>

⁷ General Data Protection Regulation (EU) 2016/679. <https://gdpr-info.eu/>

platforms ensures that operations, from case registration to document retrieval, are carried out smoothly, allowing users to focus on the mediation process without being burdened by technical concerns.

Moreover, including voice as a primary means of interaction adds a layer of convenience for users. Written communication on these platforms can often feel awkward or inadequate for fully expressing individuals' emotions or concerns regarding their cases. The ability to speak directly to the platform, as if it were a human mediator, not only facilitates the expression of complex thoughts but can also significantly accelerate the communication process. The system would not just listen to the words but interpret them deeply, analysing context and emotional subtext to provide a practical and emotionally comforting response.

3.3 Data processing systems: algorithms, machine learning, and artificial intelligence in decision-making.

Creating a mediation platform of this nature demands a meticulous integration of technologies, which, when combined, transcend the simple function of serving as a mere intermediary for dialectical exchanges between opposing ideas. These platforms must go beyond conventional applications designed to facilitate dialogue. They must be capable of offering added value by providing each user with a space to present their arguments and contextual support that enables a profound understanding of their position.

To achieve this aim, advanced natural language processing (NLP) systems are implemented, not limited to decoding textual content but also allowing for discerning the implicit intentions within users' expressions. This capacity to comprehend discourse is essential in guiding decisions within the complex decision trees that outline the possible pathways to resolution. The ultimate goal of these technologies is not merely to interpret the literal meaning of language but also to capture the nuances that help algorithms make optimal decisions at every stage of the negotiation process.

One of the fundamental aspects is the vectorisation of ideas. For this, it is essential to have an adequate corpus, as only then can models operate effectively. The most efficient platforms are those that specialise in predefined fields, such as labour or family disputes, areas where the nature of the conflicts and the resolution parameters are more clearly defined. By creating a specialised corpus, machine learning algorithms can analyse and compare the current situation to previous cases, identifying patterns and proposing solutions based on similar experiences.

Tools such as TensorFlow and Scikit-learn play a crucial role in this process. They allow for the identification of patterns and the optimisation of predictions regarding possible negotiated outcomes, thereby improving the precision and efficiency of the mediation process. With proper training and a specialised corpus, these algorithms simulate the ability of human mediators to find points of consensus but with exponentially greater speed and analytical capacity.

3.4. Cybersecurity measures: encryption, data protection, and authentication protocols.

Cybersecurity measures constitute one of the fundamental pillars in the design and operation of a digital mediation platform, given the sensitive nature of the interactions that take place within it. Information security takes on central importance, as these platforms manage personal data and the involved parties' intentions, desires, and expectations—confidential elements that must be safeguarded with the utmost care.

From the outset, ensuring the authenticity of the participating identities is imperative. To this end, using digital certificates has become an indispensable practice. These allow for proper authentication, ensuring that each user is indeed who they claim to be, thus minimising the risk of identity theft, one of the greatest dangers in the digital environment. The encryption of communications, both in transit and at rest, is another essential component of this security framework. Platforms must, therefore, operate under a secure protocol such as HTTPS, which, through the use of advanced encryption,⁸ protects data transmission from leaving the user's device until it reaches the platform's servers. Once the server has received the data, it is crucial to apply encryption techniques to ensure unauthorised actors cannot read or tamper with stored information.

Given the confidential and sensitive nature of the data being handled—particularly when it involves negotiations, agreements, and details that may include intimate or strategic aspects of the parties involved—the use of end-to-end encryption (E2EE) emerges as an indispensable standard. This technique ensures that only the parties involved in the communication can access its content, shielding the information from any potential external intrusion. Security protocols such as SSL/TLS⁹ must be implemented to ensure data transmission and storage are conducted under the strictest security conditions.

8 Scholz, L., and Müller, S. "Encryption in Online Dispute Resolution Platforms: Ensuring Data Confidentiality." *International Journal of Law and Information Technology*, 27(4) (2019): 277-299. <https://doi.org/10.1093/ijlit/eay020>

9 Reddy, K. P., and Jain, P. "TLS/SSL Encryption in Online Platforms: Enhancing Secure Data Transmission." *Journal of Cybersecurity Research and Practice*, 12(2), (2021) 45-58. <https://doi.org/10.1007/s10207-020-00499-w>

Upon the conclusion of a negotiation or mediation process, it becomes necessary to precisely identify the nature of the data processed. Data protection regulations, such as the General Data Protection Regulation (GDPR), distinguish between different types of information and grant special status to medical, financial, or employment data. Each category entails specific obligations regarding its handling, retention, and deletion. Once the process is concluded, the platform must determine whether the data should be archived, deleted, or retained under certain conditions. In many cases, it is recommended to transfer the data to a specialised archiving system, such as Speria, to ensure that, while the information is preserved, it is not accessible without the necessary controls and restrictions, thereby preventing unauthorised future access.

In sum, a digital mediation platform must incorporate a robust cybersecurity architecture that guarantees data confidentiality, integrity, and availability in compliance with applicable regulations, with particular emphasis on preserving the trust of the involved parties.

3.5. Blockchain and smart contracts in ODR: how they function and their benefits for transparency and enforcement.

Using technologies such as blockchain introduces unparalleled security to systems and decentralises data distribution, granting each party involved an independent module that operates autonomously. This distribution model provides each actor greater control and participation within the network, as each node holds a copy of the information, thereby eliminating reliance on a single centralised entity. In this way, the integrity and availability of data are guaranteed within a secure and decentralised environment.

Additionally, blockchain platforms offer highly advanced infrastructure for creating and deploying networks and smart contracts without building a chain from scratch. Among these platforms, several stand out as particularly influential:

Ethereum is among the most prestigious platforms for developing smart contracts and decentralised applications (dApps). It stands as a paradigm of innovation. Using the Solidity programming language, Ethereum enables the creation of self-executing and transparent smart contracts, thereby revolutionising the automation of complex transactions.

On the other hand, Hyperledger Fabric, a private blockchain framework designed by the Linux Foundation and geared towards enterprise solutions, offers a modular approach that allows for tailored configurations. This feature makes it an extremely versatile tool, adaptable to various corporate needs.

Concorda, developed specifically for the financial industry, offers a unique privacy solution, making it especially suitable for consortia that require discretion in their operations. Meanwhile, Quorum, a platform derived from Ethereum, has been primarily adopted by companies in the financial sector seeking greater privacy in their decentralised applications.

Specialised tools have been developed in the realm of blockchain node and network management to facilitate the monitoring and administration of these distributed networks. Geth (Go-Ethereum), an Ethereum implementation written in Go, allows the execution of full or light nodes on the Ethereum network, enabling dApp development and mining. Parity, another Ethereum implementation developed in Rust, stands out for being fast and lightweight, optimising node management in environments where efficiency is crucial.

For networks based on Hyperledger Fabric, Hyperledger Explorer offers a powerful visualisation tool that monitors blocks, transactions, and nodes, providing a comprehensive view of the network's functionality. Infura, in turn, removes the need to manage one's own nodes, offering simplified access to Ethereum's node infrastructure. Thus, it facilitates the development of decentralised applications without incurring the costs and complexities of managing the infrastructure.

Likewise, testing and auditing tools are fundamental to ensuring the security and functionality of blockchains and smart contracts. MythX, an automated auditing tool for Solidity contracts, detects common vulnerabilities and prevents risks before deployment on the network. With its symbolic analysis engine, Manticore offers an exhaustive testing method for Ethereum contracts, identifying potential security flaws. Similarly, Securify, an automatic auditing platform developed by the University of Zurich, strengthens security through an in-depth analysis of smart contracts.

Finally, blockchain explorers are essential tools for real-time activity visualisation within these distributed networks. Etherscan is, without a doubt, the most widely used explorer for monitoring transactions, contracts, and data on the Ethereum network. Similarly, Blockchain.info allows for exploring the Bitcoin blockchain, offering a direct window into the visualisation of transactions, blocks, and addresses. Blockchair, a multi-blockchain explorer, supports networks such as Bitcoin and Ethereum, providing a unified and comprehensive view of several blockchains.

3.6. Key Technical Challenges

The primary technical challenges faced by online mediation platforms are not solely centred around the development of more advanced technologies but also involve the need for broader adoption, transforming them into priority tools for conflict resolution and alleviating the burden on traditional judicial systems. To achieve this, such platforms must be recognised as

initial mediation tools and mechanisms whose rigour and seriousness endow them with an almost probative status in cases where mediation efforts fail. In other words, their capacity to manage disputes should be sufficiently robust to serve as a weighty reference within judicial or extrajudicial frameworks.

However, this shift in interaction also presents certain risks that cannot be ignored. Written language, lacking the nuances of verbal communication, is more susceptible to misunderstandings and misinterpretations, which could exacerbate tensions or escalate conflicts that, in essence, the platform is designed to resolve. Therefore, one of the most significant challenges lies in refining the algorithms of these platforms so that they may soften the language used, adapting it to the specific context of the mediation in progress. This “malleability” of discourse would allow the interpretation of words in a way that fosters mutual understanding, creating an environment more conducive to reconciliation.

3.7. Data privacy concerns, particularly in cross-border disputes (GDPR and international privacy laws).

Data privacy concerns, especially in cross-border disputes, become critical when managing sensitive information across different jurisdictions.¹⁰ The European Union’s General Data Protection Regulation (GDPR) and international privacy laws provide the regulatory framework that outlines the requirements and safeguards to ensure that personal information is maintained under strict conditions of security and confidentiality. In this context, using digital certificates such as SSL/TLS emerges as a fundamental pillar in protecting communications and verifying the identities of the involved parties.

An SSL/TLS certificate is a digital artefact with a dual purpose: verifying the identity of the systems interacting within a network and establishing an encrypted communication channel through the Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocol. This mechanism ensures that the connections between the parties within a mediation platform occur in a secure environment, shielded against potential privacy breaches. Each party involved in the mediation signs their communications using the digital certificate, ensuring the authenticity of the transmitted messages and the integrity of the exchanged data. This is essential for preserving the confidentiality of information and protecting the intentions and decisions integral to the dispute resolution process.

In the field of certification, issuing authorities play a crucial role in guaranteeing the reliability of the credentials used. In Spain, the *Fábrica Nacional de Moneda y Timbre* is the leading certifying authority¹¹ responsible for issuing digital certificates, including the eDNI, which allow for secure identification of users in the digital environment. Similarly, in other European countries, such as Germany, *Bundesdruckerei* serves as the responsible institution; in the United Kingdom, the key certifying authority is *Digidentity*, and in France, entities like *Certinomis* and *DocuSign France* perform equivalent functions. These certifying organisations ensure that a rigorous identity verification and authentication standard backs each interaction between parties involved in digital mediation.

Spain’s legal framework concerning data protection is particularly stringent. In addition to the GDPR, the *Esquema Nacional de Interoperabilidad* (ENI) is implemented, which sets forth a series of guidelines and standards to ensure that data can be shared between different communities and organisations securely and lawfully. This scheme, aligned with the recommendations of the European Union, particularly with the European Interoperability Framework, ensures that the data exchanged in mediation processes and other sensitive contexts comply with the most demanding legal and technical requirements, both nationally and across Europe.

The ENI envisions data interoperability within a pan-European context,¹² taking into account the diverse regulations and policies of member states. This interoperability not only refers to the ability of systems to exchange data but also to the protection and security level that such data require, according to the category of information and national and international standards. Additionally, the ENI establishes links with various European instruments that ensure cooperation and the reuse of essential components, such as communication networks and interoperability services, thus ensuring a secure and cohesive ecosystem across the continent.

The technical aspects of secure communication rely on public and private key cryptography. The web server provides the browser with a public key within the SSL/TLS certificate, which allows information to be encrypted before sending. The server, in turn, is the only entity possessing the private key necessary to decrypt the received data. This asymmetric key exchange ensures that only authorised systems can access the information, protecting it against any possible interception.

10 Andrade, N., Oliveira, F., and Cardoso, A. “Data Protection Challenges in Cross-Border Online Dispute Resolution.” *Journal of Internet Law*, 22(3) (2018): 15-24.

11 Roßnagel, H., and Zibuschka, J. “Digital Identities and the Law: A European Perspective on Authentication and Certification.” *Information Security Journal: A Global Perspective*, 26(1) (2017): 1-13. <https://doi.org/10.1080/19393555.2016.1264909>

12 Borgesius, F. Z., and González, C. “The General Data Protection Regulation in the European Union: Innovations and Limitations.” *Computer Law & Security Review*, 32(1) (2016): 2-12. <https://doi.org/10.1016/j.clsr.2015.12.007>

Authentication is another key element in this process. When the server sends the public key from the SSL/TLS certificate to the browser, the latter verifies the certificate's authenticity through a trusted third party. In this way, the browser can confirm that the server it is communicating with is legitimate and not a malicious source seeking to intercept or manipulate the data. This process ensures communications confidentiality and interactions reliability within a digital environment.

3.8. Security vulnerabilities: how platforms can ensure data integrity and confidentiality.

Once cases have been concluded, their accessibility should be drastically restricted. To this end, a robust archival system, such as Speria, should be employed to seal the cases, rendering them inaccessible from the platform once they are closed. This measure is vital to prevent potential data leaks after the cases have been finalised, safeguarding the data and ensuring it cannot be manipulated or accessed without explicit authorisation.

As for the underlying infrastructure, the network on which these platforms operate must be protected by the most advanced server security systems. The platform must be equipped to repel any attempted attack or unauthorised infiltration from firewalls to intrusion detection systems. If the data managed is particularly sensitive or the platform belongs to a closed organisation, using a VPN (Virtual Private Network) would be an additional effective strategy to enhance protection. This private network would encapsulate all data traffic, ensuring the information is neither visible nor accessible from external networks.

Finally, to proactively address any vulnerabilities that may arise throughout the platform's development and operation, the implementation of a continuous integration¹³ system is indispensable. This system should be accompanied by a suite of security tests designed to constantly evaluate the system's stability and robustness against potential failures. Integration and unit testing would allow for detecting and correcting any emerging vulnerabilities, ensuring that the platform operates within the highest security standards.

4. Legal Issues in the Regulation of ODR Platforms

The regulatory framework governing Online Dispute Resolution (ODR) platforms exhibits specific characteristics and poses a series of challenges, which this paper will elucidate in due course. The ensuing analysis will address the distinctive features of ODR platform regulation and examine the consequent legal and practical implications that arise therefrom.

4.1. Enforceability and Recognition

The legal validity and enforceability of ODR outcomes vary significantly across jurisdictions. While mediated settlements may be enforceable as contracts in most legal systems, their status as directly enforceable instruments akin to court judgments is not universally recognised. The UNCITRAL Model Law on International Commercial Mediation and International Settlement Agreements Resulting from Mediation (2018) aims to address this issue by providing a framework for enforcing international settlement agreements.

The UNCITRAL Model Law on Electronic Commerce and the United Nations Convention on the Use of Electronic Communications in International Contracts generally support the recognition of electronic signatures and e-agreements in ODR contexts. However, the legal status of e-arbitration awards remains contentious, particularly in light of the formal requirements stipulated in the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards.

4.2. Procedural Safeguards

Robust review mechanisms are essential to ensure the integrity and fairness of ODR outcomes. These may include: judicial review of ODR decisions, particularly in cases involving mandatory law or public policy considerations; internal appeal processes within ODR platforms, subject to clear and transparent procedural rules; compliance with due process standards, including the right to be heard and equality of arms, adapted to the digital environment; transparency requirements for ODR providers regarding their decision-making processes and potential conflicts of interest.

Developing international standards for ODR procedural fairness, potentially through instruments such as the UNCITRAL Technical Notes on ODR, is crucial for fostering trust in and recognising ODR outcomes across jurisdictions.

¹³ Nolte, F., and Berg, P. "Implementing Continuous Integration for Cybersecurity in Cloud-based Platforms." *Journal of Software Engineering and Applications*, 13(6) (2020): 291-306. <https://doi.org/10.4236/jsea.2020.136020>

4.3. Jurisdictional Complexities

Determining applicable law in cross-border disputes resolved through ODR platforms presents significant challenges. The principle of party autonomy in the choice of law clauses may be constrained by mandatory rules of the forum or by the overriding mandatory provisions of third countries. In the absence of an express choice, conflict of laws rules become paramount, with the potential application of the “closest connection” test or the law of the characteristic performer’s habitual residence.

Jurisdictional challenges are further exacerbated in the ODR context due to the virtual nature of proceedings. The traditional bases for asserting jurisdiction, such as the defendant’s domicile or the place of performance, may be inadequate or indeterminate in cyberspace. Consequently, the Brussels I Recast Regulation and the Hague Convention on Choice of Court Agreements may provide insufficient guidance for ODR-specific scenarios.

4.4. Applicable Law in Cross-Border Disputes

The determination of applicable law in ODR contexts remains a complex issue. The principle of party autonomy, allowing parties to choose the governing law, is generally respected but may be limited by mandatory rules of the forum (*lex fori*), Overriding mandatory provisions of third countries, and public policy considerations.

Without party choice, courts or ODR platforms may resort to the Rome I Regulation (for contractual obligations in the EU), the “closest connection” test, or the law of the characteristic performer’s habitual residence. These traditional conflict-of-law rules may require adaptation to suit the unique nature of online transactions and disputes.

4.5. Jurisdictional Challenges

The virtual nature of ODR complicates jurisdictional assertions. Traditional bases for jurisdiction include the defendant’s domicile (*actor sequitur forum rei*), place of performance, and place of the harmful event (for torts). This may be difficult to establish in cyberspace. The Brussels I Recast Regulation and the Hague Convention on Choice of Court Agreements¹⁴ provide some guidance but may not fully address ODR-specific scenarios. Courts and legislators are grappling with new jurisdictional concepts, such as Virtual presence, Targeting of online activities and Effects doctrine in the digital realm.

5. Comparative Analysis of ODR Regulatory Frameworks: European Union, United States of America and Asian countries

The European Union, United States, and Asian countries have taken different approaches to Online Dispute Resolution (ODR), each reflecting their unique legal systems, technological landscapes, and consumer protection priorities. Here’s an analysis of ODR developments in these regions:

The EU has taken a proactive approach to ODR through the ODR Regulation¹⁵ (Regulation 524/2013), which works in tandem with the ADR Directive (Directive 2013/11/EU). The ODR Regulation established a pan-European ODR platform to facilitate the resolution of disputes arising from online transactions.¹⁶ Key features include covering contractual disputes from online sales or service contracts between EU consumers and traders;¹⁷ Online traders must inform consumers about the ODR platform and provide a link to it on their websites; the platform offers translation services to facilitate cross-border dispute resolution.¹⁸

The United States of America’s approach to ODR is more decentralised, with initiatives at both federal and state levels and significant involvement from private sector platforms. No comprehensive federal ODR legislation exists, but agencies like the Federal Trade Commission (FTC)¹⁹ guide e-commerce dispute resolution. Several states have implemented court-connected ODR programs, particularly for small claims and family law matters. Examples include Utah’s ODR pilot program for small

¹⁴ Convention of 30 June 2005 on Choice of Court Agreements, <https://www.hcch.net/en/instruments/conventions/full-text/?cid=98>

¹⁵ Regulation (EU) 524/2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR) <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0001:0012:EN:PDF#:~:text=This%20Regulation%20aims%20to%20create,have%20arisen%20from%20online%20transactions.>

¹⁶ The European ODR platform is a centralized hub connecting consumers, traders, and ADR entities. Its efficacy can be assessed through several metrics: since its launch in 2016, the platform has received hundreds of thousands of complaints, indicating growing awareness and utilization; the platform has been particularly effective in addressing language barriers and jurisdictional issues in cross-border disputes despite its potential, the platform faces issues such as low trader engagement and limited consumer awareness in some Member States. The European Commission has proposed repealing the ODR Regulation and replacing the ODR platform with a more streamlined digital tool as part of a broader reform of the consumer ADR framework.

¹⁷ [https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/753200/EPRS_BRI\(2024\)753200_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/753200/EPRS_BRI(2024)753200_EN.pdf)

¹⁸ https://www.eumonitor.eu/9353000/1/j4nvhd3hydzq_j9vvik7m1c3gyxp/vm7enjjcd8wr

¹⁹ Federal Trade Commission (FTC) Guidance on e-commerce dispute resolution <https://www.ftc.gov/system/files/documents/plain-language/alt067-electronic-commerce-selling-internationally-guide-businesses.pdf>

claims and Michigan's MI-Resolve platform for civil disputes. eBay's Resolution Center handles millions of disputes annually, using automated negotiation and human intervention. PayPal's dispute resolution system offers a streamlined process for resolving transaction-related disputes.

The regulatory approach is largely sector-specific, with different rules for financial services, e-commerce, and other industries. The American Bar Association has issued ethical guidelines for lawyers participating in ODR.

Asian countries, particularly China and India, have rapidly developed ODR systems despite their unique challenges.

China has established specialised Internet Courts in Hangzhou, Beijing, and Guangzhou, which extensively use ODR technologies. Alibaba's Consumer Protection Platform handles millions of e-commerce disputes annually. The Supreme People's Court has issued guidelines on using ODR in the judicial system.

The Indian government has launched the e-Courts project to digitise court processes, which includes ODR components. Platforms like SAMA have emerged to provide ODR services for commercial and consumer disputes. The Indian Arbitration and Conciliation Act has been amended to facilitate online arbitration.

In conclusion, while the EU has taken a centralised, regulatory approach to ODR, the U.S. system is more decentralised with significant private sector involvement. Asian countries rapidly adopt ODR, often leapfrogging traditional systems, but face infrastructure and legal framework challenges. As ODR continues to evolve, these different approaches offer valuable insights for developing effective cross-border dispute resolution mechanisms in the digital age.

6. Challenges and Future Perspectives

One of the principal challenges to effectively implementing Online Dispute Resolution (ODR) platforms lies in the regulatory fragmentation across jurisdictions. The lack of uniform regulations governing ODR systems results in inconsistencies that can undermine the effectiveness and trust of users in these platforms. Various countries and regions have developed disparate legal frameworks that address resolving online disputes, potentially leading to jurisdictional conflicts and difficulties in enforcing decisions. Such fragmentation necessitates a comprehensive understanding of international law and often requires harmonisation efforts to ensure that ODR platforms operate efficiently and fairly across borders.

Additionally, the implementation of ODR platforms faces significant technical challenges, including issues related to digital literacy and access to technology. For a substantial segment of the population, limited digital skills and lack of access to necessary technological tools can impede the effective use of ODR services, thus restricting their potential benefits to a narrower user base. Ethical concerns also arise with the increasing integration of artificial intelligence (AI) and machine-based decision-making within ODR systems. Questions about AI algorithms' transparency, accountability, and fairness are critical, as these technologies can significantly influence the outcomes of disputes. Ensuring that these AI systems adhere to ethical standards and do not perpetuate biases or infringe on the parties' rights is paramount for maintaining the integrity and fairness of ODR platforms.

International law reform is critical to better accommodate Online Dispute Resolution (ODR) as it becomes increasingly prevalent across global jurisdictions. To address the diverse and sometimes conflicting legal standards currently complicating ODR practices, international legal bodies and governments may need to consider adopting more unified legal frameworks. These reforms would aim to standardise procedures and enforceability of ODR outcomes, thereby enhancing the effectiveness and acceptance of ODR systems worldwide. Such legal harmonisation would mitigate jurisdictional discrepancies and facilitate smoother cross-border dispute resolutions, ultimately fostering a more cohesive global legal environment for ODR.

Furthermore, the role of emerging technologies such as artificial intelligence (AI) and blockchain is poised to significantly shape the future landscape of ODR. AI technologies can automate dispute resolution processes, increasing efficiency and potentially reducing the need for human arbitrators in certain conflicts. This automation, however, raises important questions regarding the transparency and fairness of AI-driven decisions, necessitating rigorous standards and ethical guidelines. On the other hand, blockchain technology promises to create immutable records of disputes and resolutions, enhancing transparency and trust in ODR platforms. By leveraging these technologies, ODR platforms can improve their operational efficiencies and enhance the security and reliability of the dispute resolution processes, setting a new standard for managing and resolving conflicts in the digital age.

7. Conclusions

Digital mediation platforms have solidified their position as an essential pillar in contemporary conflict resolution processes, and their permanence in the legal and technological landscape appears inevitable. Their ability to provide sustainable, efficient solutions tailored to the involved parties' needs ensures their longevity and enhances their relevance in an increasingly digitised environment. The integration of artificial intelligence has experienced a significant boom, transforming these platforms into tools not just for mediation but also for analysis and foresight.

Using AI-driven processes, such as language analysis, identifying behavioural patterns, and determining causes and effects in disputes, has elevated the effectiveness of mediation, making the outcomes more fruitful and precise. These innovations allow for a deeper understanding of the parties involved and the generation of more tailored and resolute proposals. Moreover, the application of artificial intelligence in collecting and analysing historical data enables the creation of robust statistics, which assist in redirecting conflict situations based on past experiences, creating a feedback loop that enriches the mediation process. In this context, AI-powered digital mediation platforms are here to stay and emerging as key elements in the future of conflict resolution. Thanks to their capacity for continuous learning and growing adaptability, these tools offer a landscape of more transparent, objective mediations grounded in empirical data, marking the dawn of a new era in dispute management.

Future legal developments in Online Dispute Resolution (ODR) are set to incorporate significant reforms in international law aimed at harmonising legal standards across jurisdictions, thereby enhancing the global acceptance and effectiveness of ODR systems. Such reforms would address current discrepancies and facilitate more seamless cross-border dispute resolutions. Additionally, integrating emerging technologies such as artificial intelligence (AI) and blockchain is set to transform ODR practices by automating processes to increase efficiency and create secure, immutable records that enhance transparency and trust. These technologies will streamline dispute resolution and ensure adherence to ethical standards, setting a new precedent for conflict management in the digital era.

References

- Albashrawi, M., and Motiwalla, L. "Big Data Analytics in Online Dispute Resolution: A Future Path." *Journal of Information Systems Applied Research*, 10(4) (2017): 45-54.
- Andrade, N., Oliveira, F., and Cardoso, A. "Data Protection Challenges in Cross-Border Online Dispute Resolution." *Journal of Internet Law*, 22(3) (2018): 15-24.
- Barral Viñals, I., Viola Demestre, I., and Pérez Daudí, V. "El sistema de ADR/ ODR en conflictos de consumo: aproximación crítica y proyección de futuro" [The ADR/ODR System in Consumer Disputes: A Critical Approach and Future Prospects]. *Atelier*, (2019).
- Beatrice Zuffi. "An effective on-line dispute resolution network for enhancing collective redress in Europe: how to handle mass small claims through an integrated approach." *Revista Ítalo-Española de Derecho Procesal*, 1. (2022) <https://doi.org/10.37417/rivitsproc/688>
- Borgesius, F. Z., and González, C. "The General Data Protection Regulation in the European Union: Innovations and Limitations." *Computer Law & Security Review*, 32(1) (2016): 2-12. <https://doi.org/10.1016/j.clsr.2015.12.007>
- De Filippi, P., and Hassan, S. "Blockchain Technology as a Regulatory Technology: From Code to Law." *First Monday*, 21(12) (2016). <https://doi.org/10.5210/fm.v21i12.7113>
- Elisavetsky, A., and Marun, M. V. "Transformación digital de la mediación Praxis en Hispanoamérica" [Digital Transformation of Praxis Mediation in Latin America]. *International Journal of Online Dispute Resolution*, 9(1) (2022): 93-99. <https://doi.org/10.5553/IJODR/235250022022009001008>
- Markovinovik Zunko, I. "Implementation of the ODR (ON line Dispute resolution) Platform according to the regulation (EU) no 524/2013 on On line dispute resolution for consumer disputes," *Economic and Social Development, Book of Proceedings (Sep 1/Sep 2, 2016)*: 264-272.
- Menalo, N. (n.d.). "On-line dispute resolution delivers aid within 72 hours." *Network World Canada*, 10 (18), 8.
- Montesinos García, A., and Barona Vilar, S. "Arbitraje y nuevas tecnologías" [Arbitration and New Technologies] (1. ed). Thomson Civitas (2007).
- Nolte, F., and Berg, P. "Implementing Continuous Integration for Cybersecurity in Cloud-based Platforms." *Journal of Software Engineering and Applications*, 13(6) (2020): 291-306. <https://doi.org/10.4236/jsea.2020.136020>
- Reddy, K. P., and Jain, P. "TLS/SSL Encryption in Online Platforms: Enhancing Secure Data Transmission." *Journal of Cybersecurity Research and Practice*, 12(2) (2021): 45-58. <https://doi.org/10.1007/s10207-020-00499-w>
- Roßnagel, H., and Zibuschka, J. (2017). "Digital Identities and the Law: A European Perspective on Authentication and Certification." *Information Security Journal: A Global Perspective*, 26(1): 1-13. (2017) <https://doi.org/10.1080/19393555.2016.1264909>

- Scholz, L., and Müller, S. "Encryption in Online Dispute Resolution Platforms: Ensuring Data Confidentiality." *International Journal of Law and Information Technology*, 27(4) (2019): 277-299. <https://doi.org/10.1093/ijlit/eay020>
- Ustun, E. S., Yuce, M., and 2022 IEEE 24th Conference on Business Informatics (CBI) Amsterdam, Netherlands 2022 June 15 - 2022 June 17. (2022). Smart Legal Contracts & Smarter Dispute Resolution. In 2022 IEEE 24th Conference on Business Informatics (CBI) (Vol. 02, Issue CBI: 111–117. <https://doi.org/10.1109/CBI54897.2022.10056>