Global Journal of Researches in Engineering: F
Electrical and Electronics Engineering
Volume 20 Issue 5 Version 1.0 Year 2020
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

From the Theory and Design of an Electronic Dispute Resolution Platform in the Field of Consumer Affairs to its Effective Implementation under European and Spanish Law

By Oscar Daniel Franco Conforti
Universitat Oberta de Catalunya

Introduction- In the field of dispute resolution by electronic means, it is possible to find a wide range of expressions (i.e, distance dispute resolution, online dispute resolution, electronic dispute resolution, and a long etcetera) that situation is due to the rich Spanish language allows to create in an attempt to reproduce the essence of the idea of Online Dispute Resolution (ODR) from the Common Law.

ODRs are a set of methodologies through which a conflict can be resolved through the use of information and communication technology (ICTs), which is thus incorporated as a "fourth part" into the traditional tripartite models of conflict resolution (Katsh and Rifkin 2001).

GJRE-F Classification: *FOR Code: 290903p*

Strictly as per the compliance and regulations of:

From the Theory and Design of an Electronic Dispute Resolution Platform in the Field of Consumer Affairs to its Effective Implementation under European and Spanish Law

Oscar Daniel Franco Conforti

I. Introduction

In the field of dispute resolution by electronic means, it is possible to find a wide range of expressions (i.e, distance dispute resolution, online dispute resolution, electronic dispute resolution, and a long etcetera) that situation is due to the rich Spanish language allows to create in an attempt to reproduce the essence of the idea of *Online Dispute Resolution* (ODR) from the *Common Law*.

ODRs are a set of methodologies through which a conflict can be resolved through the use of information and communication technology (ICTs), which is thus incorporated as a "fourth part" into the traditional tripartite models of conflict resolution (Katsh and Rifkin 2001).

To be more specific, an ODR will be the result of the sum: methodology of conflict resolution plus the technological tools (e-mail, chat, SMS, videoconference, etc.) applied to a specific case, by the parties and the conflict operator (when there is one) who will help them in trying to achieve resolution of the case by themselves (or not) (Comfort 2013).

Two early conclusions can be drawn from this idea and concept of ODRs: (a) the technological tools are transversal and functional to all methods of conflict resolution and, (b) there is no equivalence between the technological tool and the method of conflict resolution applied in the specific case (Conforti 2013, 2017).

Among the possible origins of the ODR are, on the one hand, the theory of the transfer of the methodologies of *alternative* dispute resolution (ADR) from the face-to-face to the virtual scenario promoted by professionals in the field of law who, aware of the opportunities offered by the new communication technologies, decided to take these methods (negotiation, mediation, arbitration, etc.) to the cybernetic environment; and, on the other hand, with the theory that focuses on economic transactions carried out through the Internet, wherein the absence of ways to resolve conflicts derived from purchases and sales that were made in this new scenario (for example, in portals such as Amazon®, eBay® or PayPal® —the undisputed promoters of these methods of conflict resolution derived from their commercial activity—) activated the need to respond to unsatisfied consumers. Their origin should not mislead us, ADR and ODR are not equivalent. There are at least three reasons to argue that there is no correspondence between them: Firstly, because ODR procedures may not necessarily satisfy the "alternative" requirement of ADRs, since the form of ODR includes so-called virtual courts or *cyber courts*; secondly, because the technological component of ODR makes it possible to create different or non-existent procedures in ADRs (Generalitat de Catalunya Departament de Justicia 2009) and, thirdly, because the dialogue and creativity required for an ODR process differs from that of ADR processes since here "*Dialogue is a direct, face-to-face meeting process which should not be confused with endless the orisation and speculation.*" (Bohm 2012) and creativity seeks to avoid "*self-feeding confusion*" (Conforti 2015).

The scientific literature in relation to ODR is truly abundant, however, that does not happen in the pragmatic scenario where there is hardly any literature that explains how to resolve in practice the various issues raised by ODRs, in relation to guaranteeing the identity of the parties, electronic signatures, security, privacy, confidentiality, and data protection, among others.

Perhaps part of the explanation for this disparity in developments is that *a priori,* not all ODR need secure, private, and confidential communications. If this were not the case, B2C (*Business to Consumer)* e-commerce would probably not exist, or at least not in its current development. However, it is no less true that today communications on the Internet have greatly improved in terms of security, privacy and confidentiality; practically all communications can use secure servers (Https) and be encrypted, with various certificates and levels of security.

Author: Senior researcher at the Galtung Institute Spain (IG-Spain). Doctor in Law and Professor of Negotiation in the Law and Political Science Departments of the Universitat Oberta de Catalunya (UOC). Honorary Professor in the Department of Criminal Law at the Universidad Autónoma de México (UNAM).
e-mails: franco.conforti@gmail.com, https://orcid.org/0000-0001-6596-1046

Secure, private, and confidential communications are only indispensable when required by the parties to the dispute or by law.

Possibly the Law is the other part of the explanation.

The ODR comes from the *common law* legal system where the legal regulation that has been made of them is —in accordance with tradition in that legal system— almost nil. However, in our legal system of continental law, there is an abundant legal regulation to which we must pay attention, among other things, for the sake of legal security.

Thus, for example, in Spain when we speak of mediation by electronic means, the Law establishes the obligation to avoid impersonation by guaranteeing the identity of the participants in the mediation process (Law 5/2012 art.24.1).

II. Issues Raised by the ODR

Confidentiality, privacy, the identity of the parties, electronic signature, and data protection are undoubtedly the first issues on the agenda when it comes to resolving disputes by electronic means.

From a practical point of view, the challenge must be understood at multiple levels, ranging from avoiding the distortion of the conflict resolution methodology in question to the imperative of compliance with the rules of law, to the technical requirements and guarantees to be met by ODR platforms.

Unlike in *Common Law,* where Ethan Katsh acknowledged that "[...] *we have neglected to design systems to deal with disputes that may arise.*" (Katsh 2014), we in the Continental Law must focus on ensuring legal certainty through the design of ODR platforms that take into account the specificity of this modality of work (Sourdin 2007, Conforti 2018).

There is no doubt that there are more than four parties to an ODR. We are talking about the natural or legal persons that have some degree of connection with the ODR process, which is known as a "fifth party" (Lodder 2010, 79), and I would even go so far as to say that it would be appropriate to split a "sixth party", I am referring to the internet service provider.

It is appropriate to open a brief parenthesis to point out, without going into detail, that as regards access to the Internet, in a way, the United Nations General Assembly (UN) closed the debate that, in the field of the Law on New Technologies, existed when it considered access to the Internet as a Human Right.

There is no need for new human rights standards for the internet because the principles and doctrines in current international law apply in all areas. The same international laws and standards that already exist must be applied in the same way to online media.

By applying this human rights-based approach to facilitating access to the Internet, it is the State's obligation to close the multiple forms of the existing digital divide, by promoting digital literacy, by facilitating access to online information - as an important tool for promoting the right to education - and in the resolution of conflicts by electronic means - which is of particular interest to us -, etc. (United Nations 2016).

Table 1: Parties at ODR Own elaboration

Part 1, 2 and 3	Part 4	Part 5	Part 6
Parties to the Conflict	E-mail	Service Provider or ODR Platform (ODRS)	Internet Service Provider
Conflict Operator	Virtual Meeting		
	Provider of ICT tools		

It is clear that while the "fourth part" participates in the ODR process, both the "fifth part" and the "sixth part", which I have just introduced in the table, are not directly involved in the ODR process. It follows that the legal consequences for both are necessarily different.

We must note the need to address the issue of ODR or ODRS (*Online Dispute Resolution Supplier)* platform suppliers, also ODRs. But before we continue, I think it is appropriate to return to at least one of the early conclusions drawn *above* and to point out that the issue deserves preliminary clarification.

A videoconference is not an ODR (Conforti 2013, 2015, 2020) (ADR *Institute of Canada* 2020).

a) Videoconferencing is an ICT (Cloud Computing) tool

A videoconference is a communication established through the Internet in which image and sound are transmitted. People in a video conference can see and hear each other through their computers or devices in real-time (synchronously).

The videoconference is carried out in the cloud over the Internet by a service provider who makes certain *software* available to end-users which may (or may not) need to be downloaded to the customer's computer or mobile device.

This means that the responsibility for managing the key infrastructure, such as storage, security, and

operational features, falls directly on the shoulders of the cloud-based video conferencing service provider. As a general rule, in the free versions, these services are focused solely on production without the additional responsibility of managing the critical ICT infrastructure they offer; in the paid versions, the videoconferencing service provider will assume different levels of responsibility (the specific contract conditions for each of them must be consulted).

Applications such as Zoom, Microsoft Teams, Webex, etc., provide virtualisation solutions over the Internet, only support synchronous communication, and lack the full menu of an ODR that is typical of ODRS platforms.

A videoconference alone, i.e. without an electronic file, without proof of identity, electronic signature, etc., does nothing to actively help the operator of the conflict and the parties to reach a resolution.

b) ODRs are the result of the sum of ICT tools and conflict resolution methodologies

As I explained *above,* ICT tools are in the cloud (*Cloud Computing*) and, when added to conflict resolution methodologies, in the form of ODR platforms, they form a new category or model of *Cloud Computing* service.

ODR's can be developed (in whole or in part) in the cloud, which is why they are included in the *Cloud Computing* category, which can generate some degree of confusion and erroneous assimilation with videoconferencing, however, the differences are notorious.

ODRs provide a space to develop, execute, and manage a wide range of processes. They eliminate the complexity that comes with building and managing all the infrastructure needed to develop and launch protocols for electronic dispute resolution (i.e. for electronic mediation).

By using these developments companies and consumers avoid having to worry about the diversity of devices, operating systems, storage, security, data protection, as the ODRS platform will take care of all this.

ODR platforms are online dispute resolution programs that offer the full range of ODR tools: electronic filing, case management, synchronous and asynchronous communication, reports, etc., using certain *hardware* and *software* ICT tools that have been specially designed and created to develop ODR processes.

On the other hand, ODRS platforms should provide a way to guarantee the confidentiality and privacy of the mediation process and certainty about the identity of the participants, digital signature and personal data protection.

Confusing a videoconference with an ODR platform has led some Justice departments to use software applications and programs that, due to multiple security failures, have been classified as unsafe —i.e: Zoom— (National Cryptologic Centre). The issue is not only a technical problem, because it is also a legal one since different levels of legal protection are being generated for the same rights.

In the attempt to justify the comparison between a videoconference and an ODR platform, it is based (mainly, but not exclusively) on the lack of economic resources to face the implementation of safe *software* and *hardware* applications, and on the urgent need to allocate these economic resources to manage the health emergency caused by the COVID19 Pandemic.

The most immediate consequence of this confusion (fuelled by the videoconference operators themselves, such as Zoom, WhatsApp, Microsoft Teams) is an increase in the digital divide between citizens who receive "access to justice" and later "justice" services in the absence of technical, intellectual, ethical and legal security conditions (National Security Agency USA 2020) and those consumers who use ODR platforms that are in line with Spanish and European legislation.

In addition, "different levels of legal protection are being created for the same rights".

Let's look at some tables that will help avoid confusion regarding the meaning of some terms that are used as synonyms when in fact they are not.

Table 2: Comparison of Web conferencing, Videoconferencing, and Telepresence

	WEBCONFERENCE	VIDEOCONFERENCE	TELEPRESENCE
Desktop software	Yes	Yes	Yes
Hardware	No	No	Yes
Variety of cameras and microphones simultaneously	No	No	Yes
Bandwidth or connectivity requirements	Under	Medium	High

Video image quality, sound, and interactivity	Low image quality (flicker, pixelation), interfering audio, and limited interactivity	High-quality HD video and sound, unlimited interactivity	*High-end* codecs and large displays with Full HD or UHD 4K resolutions, Unlimited interactivity
Access from multiple devices (device compatibility)	Yes *Bring Your Own Device* (BYOD)	Yes *Bring Your Own Device* (BYOD)	No

Own elaboration

Table 3: Comparison between Videoconference and ODR Platform

	VIDEOCONFERENCE	ODR PLATFORM
Software	YES	YES
Hardware	No	YES
Responsibility in the management of critical ICT infrastructure	No	YES
Asynchronous communication	No	YES
Security: end-to-end encryption and data protection	No	YES
Electronic file (direct access to hearings, calendar, time-stamping, recordings, a record of performances, statistical reports, notes)	No	YES
Electronic signature level 2 multifactor	No	YES
Online support within the platform	No	YES

Own elaboration

III. The Fifth Part, the ODR'S

The appearance on the stage of the ODRS responds to this practical approach pursued by this article. In other words, it is a question of establishing: (1) how they should respond and, (2) how they respond to the issues of "confidentiality, privacy, the identity of the parties, electronic signature, and data protection", the ODRS platforms in our legal framework, that is the Continental Law.

a) How should ODRS platforms respond?

Without prejudice to what has been said *above* regarding how the ODRS platforms should respond in relation to Law 5/2012, of 6 July, on mediation in civil and commercial matters; Regulatory Decree 980/2013, of 13 December, which develops certain aspects of Law 5/2012, of 6 July, on mediation in civil and commercial matters; Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations; Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the Guarantee of Digital Rights. It should be noted that the body of law at the European level in relation to the resolution of online consumer disputes is made up of Directive 2013/11/EU and Regulation (EU) No 524/2013, both of the European Parliament and of the Council, of 21 May 2013, on the resolution of online consumer disputes (hereinafter the Directive) (de la Rosa 2020).

The Directive seeks to protect the consumer and has therefore created a way for the out-of-court settlement of disputes on-line through a dispute resolution process which, according to recital 12, is an On-Line Dispute Resolution (ODR).

From a procedural point of view, this ODR excludes negotiation between the parties (argument 23 and Art. 2 e.) and technically, it could be said that it is a facilitation process in which the facilitator can suggest or impose a solution that is binding on the parties.

The principles of this ODR are: the technical quality of the dispute settlement operator (expertise), independence and impartiality, transparency, efficiency and speed, accessibility to the ODR, fairness (not justice), freedom of choice, legality (through the rule of

law), data protection, secure exchange of information and comprehensive, easily accessible and understandable information for the consumer.

Pragmatically, any trader with a website should include an advertisement (similar to cookies) with a text such as: "*The European Commission provides consumers with an online dispute resolution platform for consumer issues which you can access from here: http://ec.europa.eu/consumers/odr*". The same announcement should be made in the e-mails with offers of these on-line services.

The trader must inform the consumer of the alternative dispute resolution body to which he has adhered. The entities do not necessarily have to be registered on the EU platform. In this case, the announcement could be similar to the following: "*We have joined the XXXX online dispute resolution service, you can access it here: XXXX or opt for the ODRS provided by the European Commission to consumers which can be accessed from here: http://ec.europa.eu/consumers/odr*" (Conforti 2016a).

Furthermore, the trader must bear in mind that he is the person responsible for the processing of personal data and must exercise due diligence to ensure, at all times, that the information is processed in accordance with the provisions of Law 3/2018 and the EU's general data protection regulation 2016/679 (GDPR).

To benefit from its advantages, the merchant can opt for an ODR service that uses the cloud to host sensitive information, however, he must bear in mind (as I mentioned earlier than now) that the law places the responsibility on him since it is the merchant who has taken the decision to use such services in the cloud; and therefore it must be he who, in the eyes of the Spanish Data Protection Agency (AEPD,) ensures adequate and secure processing.

The trader is responsible for the file, and as such, the guarantor of the fundamental rights of its customers for the protection of their personal data. When deciding to contract cloud services, in addition to the technical and economic advantages, traders must have a legal assessment that allows them to identify the suitability of the services they intend to contract or join in order to prevent sanctions from the AEPD. To do this, it will be essential to have experts to advise on ODRS platforms.

The doctrine has identified many possibilities for improving the EU platform while respecting the spirit of European law with regard to it, i.e: a prior system of assisted negotiation could have been implemented (de la Rosa 2017a), the admissibility of compulsory consumer mediation (de la Rosa 2017b), an information alert system by which the consumer is informed of the rate of complaints registered for certain services or products (known as *name and share),* some form of measure could have been established in relation to multiple successive and identical complaints (*repeat players)* (Marcone Lo Presti 2020, 94).

Finally, some concern should be expressed regarding the fact that the submission of complaints, their processing, and transmission raise the question of the accreditation of the identity of the parties since the forms of the EU's RLL platform do not show how this is accredited and certified (Valbuena González 2015).

Paraphrasing Andrés Vázquez López, it can be said that in the scenario of ODR, in addition to the regulatory requirements themselves, the principle of transparency imposes a series of conditions on mediation institutions and dispute operators so that they guarantee it by advertising at least the applicable regulations, the identification of the holder providing the service, the identification of the dispute operator, and the identification of the channels of access to the available services, the information necessary for the correct use of the ODR platform and other ICTs used, specifying the navigation structure in the virtual environment of the digital platform and the different sections available, (general description of the mediation procedures, negotiation protocols used by the institutions or the same conflict operator and estimated timetables for the duration of the procedure, description of the electronic means available for carrying out mediations by this means, methods used for sending and receiving documents and description of the electronic communication methods used in the procedure, seeking to facilitate the interoperability of the systems, languages supported, detailed outline of all the phases of the process used for carrying out mediations by electronic means, cost of the ODR process and its criteria for determination, method of payment and, where appropriate, information on the free nature of the service, and information on the legal consequences of the possible agreement in relation to at least the applicable law, the possibility of obtaining an enforcement order and the competent courts in the event of enforcement or challenge of the agreement). In addition, an indication of how to exercise the rights of access, objection, rectification, and cancellation of personal data, with an indication of the level of protection and the mechanisms used to guarantee the security measures available to computer media in accordance with the applicable legislation on personal data protection (Vázquez López 2020).

It is absolutely understandable that in the emergency situation in which we are living due to the pandemic, a significant number of technological tools appear to be available, although it does not seem that all of them will be useful for online conflict resolution (Hu Wu 2020).

In our case the ODRS has to be designed following the parameters of legal security set by local and European laws, specifically taking into account the fundamental critical points already indicated (i.e.

confidentiality, privacy, identity certification, electronic signature, and data protection).

The ODRS thus become formal out-of-court dispute resolution systems in our legal system. The design of ODR systems will require genuine professionals from at least three distinct areas of expertise, I mean

Conflict management: this is a "conflict operator" who is familiar with the various methods of conflict resolution (negotiation, arbitration, conciliation, mediation, etc.) as this is the only way to be able to differentiate between them.

Legal informatics: because it is about the application of informatics in law and not just about informatics.

Law: because the process will need legal certainty and that must translate into the protection of fundamental rights such as the right to privacy, and the protection of personal data.

The design of an ODR Platform must respond not only to the EU's RGPD and other local and related legislation, but also to the Sustainable Development Goals 16 and 17 adopted by the United Nations and of course to the principles of the European Ethical Charter on the use of artificial intelligence in judicial systems and their environment (where relevant): respect for fundamental rights, non-discrimination, quality and safety, transparency, impartiality, and fairness. All this under the maxim "under user control".

To avoid the dangers of choosing a platform, you must choose one that guarantees: "confidentiality, privacy, the identity of parties and data protection".

"*ODR platforms have to produce a positive change in the people who will use them. On the part of the users, the design of the platform requires specific knowledge that must respect the values of the conflict resolution methodologies that can be applied through it and, at the same time, the fundamental rights of the people who use them.* "(Conforti 2020).

On the other hand, it has to be admitted that the generalisation of ODRS will require a combination of (a) training of conflict operators specialised in the online field and, (b) the continuous improvement of platforms (electronic file and collaborative video conference). Only in this way will it be possible to incorporate ethics and transcend the legal framework.

In particular, and focusing on ODR platforms, we must make it clear that not all technology is innovation, but nor it is all innovation technology.
The two pillars on which an ODR Platform is to be built are *ease-use* and *security*.

The design of an ODR platform should respond to the experience of the different types of users, focusing on the specific needs of each one of them, obtaining, as a result, a useful and simple product to be used, which can also be used in all types of devices.

An ODR platform, to be used in the legal system of continental law, will need to shield and provide citizens, professionals, and institutions with intellectual, legal, ethical, and computer security (Conforti 2016b).

b) How does an ODRS platform respond?

Having already made the distinctions and differentiations between a videoconference and an ODR platform (see *ut supra* point II sections 1 and 2) and laid down the principles on which an ODR platform should be designed (see *ut supra* point III section 1), let us move on to the study of the customer's experience.

The concept of "client" in an ODRS is multiple, it can be either a trader, consumer, the operator of the dispute, or the institution that offers the public the platform of dispute resolution. For the customer's experience to be satisfactory we must bear in mind that it will be directly related to their expectations and the outcome of the process, which in turn will be closely linked to the legal security of the process, i.e. the eventual effective enforcement of the agreement, even if it has to be forced (Conforti 2012).

Following Milagros Sanz Parrilla, let's see how the ODR platform of the company Acuerdo Justo SL responds, within our legal framework, to the questions of "confidentiality, privacy, the identity of the parties, electronic signature and data protection". This is the first Spanish platform created in 2008. "*This service has been developed with the collaboration of the Family Mediation Centre of Catalonia of the Department of Justice of the Generalitat de Catalunya and is based in Barcelona*" (Sanz Parrilla 2011, 449-450).

Completely redesigned, the platform has been able to maintain the two hallmarks mentioned *above,* i.e.*ease-use* and *security*. The ODR's Acuerdo Justo platform has updated its image following a modern design respecting the maxims in the design and creation that are recognized.
The design is adaptable to the customer's needs.

It can be installed on local servers, runs on any PC system, is compatible with all modern computers and browsers.

The *framework* under which the platform is programmed, as well as the rest of modern *frameworks,* are based on the ES2015 standard of Javascript (ES6), which is the current standard of modern browsers.

The platform automates a large part of the process of registration and creation of the electronic file of the ODR process.

It applies artificial intelligence in the computer architecture necessary to raise the level of security of the identification of the parties and their electronic signatures in the mediation minutes and agreements to multi-factor [(taking it to level 2 multi-factor inspired by the European directive PSD2 which is the one they apply, for example, European banks and shops to provide greater security to their customers through

enhanced authentication which consists of asking the consumer for two of these three elements: something he has (e.g. his ID card or a bank card), something he knows (the card's PIN), or something he is (the fingerprint or the iris)].

The platform has technical support for non-users and users at two different levels of assistance that even allows video calls from the platform itself to be assisted by an expert in parallel and outside the session that the professional may be carried out synchronously.

With regard to security (the identity of the parties, confidentiality, privacy, and data protection), the platform works with encryption: (a) *secure socket layer* (SSL), (b) *transport layer security* (TLS), and (c) *hypertext transfer protocol secure (*HTTPS), which I will explain later.

Encryption or encoding is the process of making sensitive information unreadable. Once encrypted, the information can only be read by applying a key. It is a security measure that is used to store or transfer sensitive information that should not be accessible to third parties. The platform uses 128-bit SSL security certificates and/or higher, which are distinguished by having the highest encryption capacity in the industry.

Deciphering such encryption could only be done by means of brute-force calculation, which consists of entering all possible variables in a message until the correct one appears. Decoding a 128-bit key, by means of brute-force calculation, would take the attacker a minimum of 149,745,258,842,898 years (Martínez de la Torre, 2016).

1. The platform works on a *secure socket layer* (SSL), i.e. a cryptographic protocol (a set of rules to follow related to security, applying cryptography) used to make secure connections between a client (such as an Internet browser) and a server (such as a computer visiting web pages).
2. It also uses *transport layer security* (TLS), which is a protocol that provides data encryption and application authentication between client and server, and is very useful and necessary, especially when sending messages over insecure networks, such as e-mail.
3. In addition to the hypertext *transfer protocol secure (*HTTPS), which is an internet communication protocol that protects the integrity and confidentiality of user data between their computers and the website. Because users expect a secure and private online experience, the adoption of the HTTPS protocol to protect connections to web sites is the most common and is well known to all users.

Regard to data protection [in accordance with the data protection regulations of Organic Law 15/1999, replaced on 6 December 2018 by the Organic Law on the Protection of Personal Data and the guarantee of digital rights, in accordance with the European regulations of the General Regulations on Data Protection (RGPD), in force since 25 May 2016 and applicable from 25 May 2018], with the differentiation between digital and electronic signatures referring to encrypted coding (and *clickwrap)*, to the use of synchronous or asynchronous systems that can be guaranteed by certification bodies, such as, for example, the notarial online certifications currently performed, as well as services related to PKI (public key infrastructure) and time stamping (*timestamping) and* qualified electronic signatures, are issued in accordance with the requirements of Law 59/2003 of 19 December on Electronic Signatures and Law 5/2012 on Mediation] (Vázquez López 2020) the session that starts in end-to-end SSL encrypted mode.

The login part of the tool is handled with the Cisco Webex Meetings APIs. The password is passed through HTTPS with the certificate created by *LetsEncrypt* for the website, furthermore, it is not stored on the server, it is only stored in the *cookies to* refresh the *token,* thus providing a smooth platform experience for the user.

The password is sent using AES 256 encryption.

SQL database. The MySQL database table is protected with a username and password. And everything is hosted on *Google Cloud Server.* The *Compute Engine*'s control plane exposes its API via GFE, so it takes advantage of infrastructure security features such a denial of service protection (DoS) and centrally managed SSL/TLS support. Customers can obtain similar protections for applications running on their *Compute Engine* virtual machines by choosing to use the optional *Google Cloud Load Balancer* service which is based on GFE and can mitigate many types of DoS attacks.

End-user authentication to the *Compute Engine* control plane API is done through Google's centralised identity service that provides security features such as hijacking detection. Authorisation is done using the central *Cloud* IAM service.

Each virtual machine (VM) runs with an associated virtual machine manager (VMM) service instance. The infrastructure provides these services under two identities. One identity is used by the VMM service instance for its own calls and the other identity is used for the calls that the VMM makes on behalf of the customer's VM. This allows the platform to further segment the trust placed in the calls coming from the VMM.

Compute Engine persistent drives are encrypted at rest using keys protected by the central infrastructure key management system. This allows for automated rotation and central auditing of access to these keys.

The *Compute Engine* is accessed using SSH from the Google cloud platform and finally, the platform uses the traffic from the *Nginx Open Source* server to

control and filter the traffic to the server allowing only https type connections.

The ODR Acuerdo Justo platform is a native Spanish speaker, which is worth highlighting because there is no such thing as a fair agreement in the market. Already available in English, it is intuitive and designed to meet the most stringent specific ODR needs. In addition to reinforcing security in the IT environment and data protection in the digital environment, it guarantees legal certainty in accordance with the European Union's international standards of quality and regulations, from an approach that is in keeping with the intellectual, legal, ethical, and IT security that it is intended to protect.

According to the website's explanations, the ODR Fair Settlement platform will allow the operator to settle disputes:

1. Planning remote sessions from your own platform.
2. Launch the connection of conflict operators to the sessions from that platform.
3. To adapt the communication of the meeting room to the consumers in a totally personalized way and suitable for all types of mobile devices.
4. Access to the statistics and recordings of the sessions from the platform.
5. To have a collaborative environment on the platform that allows operators, with a single click, to access an expert on the ODR subject in question, via chat and video conference.
6. An Expert can add other people to the videoconference session if additional support is needed. This interface is embedded in the platform, it will not be necessary to open a new application (it is done through a *widget*).
7. The *widget* may have an associated *bot which will* allow the expert to be assigned to the user's query.
8. From the point of view of user administration, the platform will also be able to automate the management of licenses associated with users (registration, deletion, etc.).
9. Legal informatics: because it is about the application of informatics in law and not just about informatics.

Sticking to Spanish and European law we can say that the regulations on the computer and legal security are implemented in the ODR platform of Acuerdo Justo.

In other words, to the question *Can ODR processes be carried out with sufficient guarantees of computer and legal security?* the answer is: Yes, at the Acuerdo Justo ODR Platform, it is possible.

Table 4: Comparison between Zoom, Webex (videoconference), and Acuerdo Justo (ODR platform) [1]

ZOOM	WEBEX	ACUERDO JUSTO
—	Security • end-to-end encryption • data protection	Security • end-to-end encryption • data protection
—	—	Electronic file • direct access to audiences • calendar • time-stamping • recordings • record of proceedings • Statistical reports • notes
—	—	Electronic signature • level 2 multifactor
—	—	Online support • by video call within the platform • provided by specialists of recognized experience

Source: Conforti, 2020. [1] Zoom, Webex, and Acuerdo Justo ODR Platform are registered trademarks. The table has been compiled from public information and is available at Google Play Store, Apple App Store, Company Websites, *US Department of Homeland Security CISA Cyber+Infrastruture,* and *National Security Agency USA* reports, cited in the bibliography.

"*Legal, technological, intellectual, and ethical security is a necessity for citizens that we must guarantee from public and private services alike. In it, the ethics of responsibility and conversion co-exist; however, the ethics of responsibility cannot be waived, because only in this way will we achieve authentic justice.*"(Conforti 2020).

IV. Conclusion

Due to the current global circumstances, it is well known for all the reasons for being on the Internet. It is no longer a question of if you arenot on the Internet, you do not exist, but of something much deeper, such as our Democracy.

Reaching citizens through the Internet is a necessity for every State that claims to be in the vanguard.

At least this is clear from Agenda 2030 and the Sustainable Development Goals, in particular ODS 16.

Finally, I propose to take up again the reflections on the obligation of the State to provide "efficient protection". The efficient protection of people's rights does not necessarily refer to the legal system, which also refers to a much broader idea that remodels the concept of Justice by expanding it, *a priori* —but not only— to the area of consumption, which is the subject of this paper.

We speak not only of "effective judicial protection" but also of "effective guardianship", that is, the application of alternative methods of conflict resolution in various fields, such as consumer affairs.

Thus, the need arises to remodel the concept of Justice towards the new paradigm of "Open Justice". Open Justice consists of a series of mechanisms that accredit "to" and "before" the citizenry "in" and "the" fulfilment of its procedures.

The "efficiency" of the Open Justice paradigm requires a transformation that consists of moving —naturally and smoothly— from "access to Justice" to "access to The Justice". Both systems of "protection of rights" coexisting on an equal footing.

One of the greatest challenges facing the Justice system when faced with the inclusion of technology as a means of materialising both judicial and extrajudicial processes is, almost naturally, the concern for programming and applying artificial intelligence algorithms to the sector on the one hand, and intellectual, legal, ethical and computer security on the other.

The traditional arguments of cost reduction, time-saving, incorporating specialised trends, providing resources to citizens in relation to judicial protection, are still valid, however, are not the main reasons why it is advisable to use an ODR platform in the consumer field.

We must bear in mind that ODRS, among other things, seek to overcome the barrier of distance; however, we must not lose sight of the fact that identity accreditation systems and electronic and digital signature certificates are often incompatible between one state and another, which ultimately creates a problem and prevents, *a priori,* their development.

It is no less true that the potential violation of confidentiality or security is not substantially greater in the virtual mode than in the face-to-face one. Therefore, until ICTs allow us to do so, the doctrine favours a minimum regulation that enables self-regulation in these matters, making it clear that this does not mean that anything is worthwhile since as I have mentioned *ut supra,* we must take as a starting point the State's obligation to provide "efficient protection" (Vilalta 2017).

As for the application of artificial intelligence in-justice (predictive justice), there is no doubt about its value; however, we owe it to ourselves to reflect deeply on the programming of the algorithms, because it is not the same to construct them under the parameters of Chinese society as one constructed in Abu Dhabi or another based on the idiosyncrasies of Spanish society.

With regard to the issues of "confidentiality, privacy, the identity of the parties, electronic signature and data protection", it has become clear that in our legal context there is at least one platform that has overcome all the difficulties of intellectual, legal, ethical and IT security and provides a practical solution that has been in operation since 2008.

Bibliography

1. ADR Institute of Canada. *Task Force Recommends ODR Platforms to the ADR*. Institute of Canada https://www.mediate.com/articles/Platforms.cfm. 2020.
2. D. Bohm. *About the Dialogue.* Kairos. Barcelona. 2012.
3. National Cryptology Centre. *The use of Zoom and its implications for security and privacy Recommendations and good practices.* Available on the Internet: https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/abstract/215-abstract-el-uso-de-zoom-y-sus-implicaciones-para-la-seguridad-y-privacidad-recomendaciones-y-buenas-practicas/file. Visited 12/10/2020.
4. Cybersecurity & Infraestructure Security Agency. *Guidance for Securing Video Conferencing*. Official website of the Department of Homeland Security. https://www.cisa.gov/publication/guidance-securing-video-conferencing
5. O. D. F. Conforti. “ODR and restorative justice online: clarifying Concepts due to its legal implication”, in *International Journal of Advanced Research*. Int. J. Adv. Res. 6(1), 850-857. ISSN: 2320-5407. Article DOI: 10.21474/IJAR01/6293. Jan, 18, 2018.
6. _____. “From e-Mediation to On-line Restorative Justice in Criminal Law”, in *American Journal of Engineering and Technology Management*. Vol. 2, No. 5, 2017, pp. 56-63. doi: 10.11648/j.ajetm.20170205.11, Nov, 2, 2017.
7. _____. Overview on mediation and enforcement of agreement Portugal and Spain (UE). *Ponencia en III International Congress on Mediation and Arbitration. Centro de Administração e Politicas*

Publicas, Unidades de Investigação do Instituto Superior. Lisboa. Portugal. 2012.

8. _____. *Pequeño Manual de Mediación Electrónica*, 2da Ed., Acuerdo Justo. Alicante. 2013.
9. _____. Mediación on-line: de dónde venimos, dónde estamos y a dónde vamos. *InDret Revista para el Análisis del Derecho*, nº 4, Sección Doctrina Procesal. 2015.
10. _____."Compliance en resolución de liti gios en línea en materia de consumo." Diario La Ley, nº 8877, de 7 de junio de 2016. Editorial La Ley. 2016a.
11. _____. Report on the feasibility of an alectronic mediation platform for the European Union, in Lorenzo M. Bujosa Vadell (dir) Almudena Gallardo Rodríguez (coord). *Electronic Mediation and e-Mediator: Proposal for the European Union*. EMEDU PROJECT. Editorial Comares SL. Granada. 2016b.
12. _____. "Mediación Electrónica ¿Qué peligros encierra la elección de la Plataforma?" *Editorial Jurídica Sepin*, 22 septiembre, 2020a. https://blog.sepin.es/2020/09/mediacion-electronica-peligros-eleccion-plataforma/
13. _____. "Aprendiendo a mediar online." *Ponencia y Taller invitado, Semana de la Mediación 2020*, 9 a 13 de Noviembre, Monterrey, NL, México; y "La mediación electrónica en la era de las videoconferencias. El fin no justifica los medios" *Encuentro de mediadores 2020*. Colegio de Abogados de la Pcia. de Córdoba, Argentina. 2020b.
14. Directiva 2013/11/UE del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativa a la resolución alternativa de litigios en materia de consumo y por la que se modifica el Reglamento (CE) n o 2006/2004 y la Directiva 2009/22/CE. (Directiva sobre resolución alternativa de litigios en materia de consumo).
15. España. Decreto Reglamentario 980/2013, de 13 de diciembre, por el que se desarrollan determinados aspectos de la Ley 5/2012, de 6 de julio, de mediación en asuntos civiles y mercantiles. «BOE» núm. 310, de 27/12/2013. https://www.boe.es/eli/es/rd/2013/12/13/980/con
16. _____. Ley Orgánica 15/1999, de 13 de diciembre de protección de datos personales. BOE, Jefatura del Estado, Madrid, 14 dic. 1999. Sección I, n. 298, p. 43088-43099.
17. _____. Ley 34/2002, de 11 de julio, de servicios de la Sociedad de la información y de comercio electrónico. BOE, Jefatura del Estado, Madrid, 12 jul. 2002. Sección I, n. 166, p. 25388-25403.
18. _____. Ley 59/2003, de 19 de diciembre de Firma electrónica. BOE, Jefatura del Estado, Madrid, 20 dic. 2003. Sección I, n. 304, p. 45329-45343.
19. _____. Ley 5/2012, de 6 de julio, de mediación en asuntos civiles y mercantiles. «BOE» núm. 162, de 7 de julio de 2012, páginas 49224 a 49242 (19 págs.) https://www.boe.es/eli/es/l/2012/07/06/5
20. _____. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. «BOE» núm. 236, de 02/10/2015. https://www.boe.es/eli/es/l/2015/10/01/39/con
21. _____. Ley 7/2017, de 2 de noviembre, por la que se incorpora al ordenamiento jurídico español la Directiva 2013/11/UE, del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativa a la resolución alternativa de litigios en materia de consumo. (2017).
22. _____. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. «BOE» núm. 294, de 06/ 12/ 2018 https://www.boe.es/eli/es/lo/2018/12/05/3/con
23. Reglamento (UE) No. 524/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, sobre resolución de litigios en línea en materia de consumo y por el que se modifica el Reglamento (CE) n o 2006/2004 y la Directiva 2009/22/CE.
24. F. Esteban de la Rosa. "Régimen de las reclamaciones de consumo transfronterizas en el nuevo derecho europeo de resolución alternativa y en línea de litigios de consumo". *Revista Española de Derecho Internacional* Sección ESTUDIOS Vol. 69/1, enero-junio 2017, Madrid, pp. 109-137 http://dx.doi.org/10.17103/redi.69.1.2017.1.04© 2017 Asociación de Profesores de Derecho Internacional y Relaciones Internacionales ISSN: 0034-9380; E-ISSN: 2387-1253." (2017a).
25. _____. «La vertebración del régimen español de la mediación de consumo en el marco del Derecho europeo». En: Aura Esther VILALTA (coord.). «Mediación sectorial y digitalización». IDP. Revista de Internet, Derecho y Política. N.º 25, págs. 17-31. UOC [Fecha de consulta: 08/10/2020] http://dx.doi.org/10.7238/idp.v0i25.3092 (2017b).
26. _____. "Los retos del nuevo marco Europeo para el Sistema Español de Arbitraje de Consumo". *Revista de Derecho Privado*, Núm. 5, septiembre-octubre 2020. Págs. 67-81.
27. F. Valbuena González. "La plataforma europea de resolución de litigios en línea (ODR) en materia de consumo". *Revista de Derecho Comunitario Europeo*, 52, 987-1016. doi: http://dx.doi.org/10.18042/cepc/rdce.52.05. 2015.
28. Generalitat de Catalunya Departament de Justícia, Centre d`Estudis Jurídics i Formació Especializada. *Materiales del Libro Blanco de la Mediación en Cataluña*. Pompeu Casanovas, Leonardo Díaz, Juame Magre, Marta Poblet. 2009.
29. C. Hu Wu. "No toda tecnología es innovación". *A definitivas*. https://adefinitivas.com/adefinitivas-

internacional/no-toda-tecnologia-es-innovacion/, 2020.
30. E. Katsh y J. Rifkin. *Online Dispute Resolution: Resolving Conflicts in Cyberspace*. San Francisco: Jossey-Bass. 2001.
31. E. Katsh. Foreword to the book *Electronic Mediation Handbook*. Franco Conforti. 2014. Acuerdo Justo. España.
32. R. Lodder y J. Zeleznikow. *Enhanced Dispute Resolution Through the Use of Information Technology*. Cambridge University Press. New York. 2010.
33. R. Marcon Lo Presti. *Justicia Digital para el consumidor. Ideas, dilemas y premisas del ODR de consumo en el espacio U.E y Chile*. Santiago de Chile. Editorial Demokratia. 2020.
34. J. Martínez de la Torre. *Cifrado de clave privada: AES.* Grado en Matemática Computacional. Estancia en Prácticas y Proyecto Final de Grado Universitat Jaume I. 3710/2016.
35. Naciones Unidas. Asamblea General. Consejo de Derechos Humanos. 32o período de sesiones. Tema 3 del programa. Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo. 27 de junio 2016.
36. https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_32_L20.pdf
37. National Security Agency. Cybersecurity Information. *Selecting and Safely Using Collaboration Services for Telework*. Update Report. 14/08/2020. https://media.defense.gov/2020/Aug/14/2002477670/-1/-1/0/CSI_%20SELECTING_AND_USING_COLLABORATION_SERVICES_SECURELY_SHORT_20200814.PDF .
38. Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content. Brussels, 9.12.2015 COM(2015) 634 final 2015/0287 (COD).
39. Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods. Brussels, 9.12.2015 COM(2015) 653 final 2015/0288 (COD).
40. M. Sanz Parrilla. "El uso de medios Electrónicos en la Mediación", en Helena Soleto, Muñoz. *Mediación y Resolución de Conflictos: técnicas y ámbitos*. Tecnos Madrid. 2011. pp. 449-450.
41. T. Sourdin. "Accrediting Mediators. The New National Mediation Accreditation Scheme". Australia. September 2007. Available at SSRN: https://ssrn.com/abstract=1134622 or http://dx.doi.org/ 10.2139/ssrn.1134622. 2007.
42. Vázquez López. "¿Se puede Mediar Online con suficientes garantías de seguridad informática y jurídica?" *Blog eMediador.eu* https://www.emediador.eu/Blog/Entries/2020/9/se-puede-mediar-online-con-suficientes-garantas-de-seguridad-informtica-y-jurdica.html 14/09/2020.
43. E. Vilalta. "Análisis crítico del procedimiento simplificado de mediación en línea para reclamaciones de cantidad de la ley 5/2012, de mediación civil y mercantil". *Revista de Internet, Derecho y Política.* UOC. IDP N.º 25 (Septiembre, 2017) I ISSN 1699-8154.