Recibido: 30 mayo 2018
Aceptado: 3 septiembre 2018

Arbitraje, vol. XI, nº 2, 2018, pp. 499–518

Retos que presenta la computación en la nube para la resolución extrajudicial de conflictos *

Antonio MERCHÁN MURILLO **

Sumario: I. Introducción. II. Las ODR y la tecnología empleada. 1. Plataformas de ODR. 2. Necesidades de interoperabilidad y normalización de la tecnología. III. Factores a tener en cuenta en el uso de las plataformas de ODR. 1. El administrador de las ODR. 2. Acceso a la plataforma. 3. Identificación de las partes. 4. Protección de los datos. 5. Ejecutividad de las ODR. 6. Ley aplicable. IV. Conclusión.

Resumen: Retos que presenta la computación en la nube para la resolución extrajudicial de conflictos

En este artículo analizamos los retos que presenta la computación en nube para la resolución de litigios online (ODR). Para ello, estudiamos variables tales como la tecnología empleada, el acceso a la plataforma, la identidad de las partes, el aseguramiento sobre la naturaleza de los datos a transferir, las garantías relativas al cumplimiento por parte de terceros de los requisitos de seguridad, la confidencialidad, la protección de datos, así como, las cuestiones sobre la ley aplicable en caso de infracción.

Palabras clave: RESOLUCIÓN DE CONFLICTOS EN LÍNEA– COMPUTACIÓN EN NUBE – CONFIANZA.

Abstract: Challenges of Cloud Computing for Dispute Resolution

This article discusses the challenges posed by cloud computing for online dispute resolution (ODR). For this, it analyzes factors such as the technology used, access to the platform, the identity of the parties, assurance about the nature of the data to be transferred, guarantees regarding compliance by third parties of the security requirements, confidentiality, data protection, as well as issues on the law applicable in case of infringements

Keywords: ONLINE DISPUTE RESOLUTION – CLOUD COMPUTING – TRUST.

I. Introducción

El comercio electrónico va unido a la aparición de conflictos de alcance transfronterizo, implicando transacciones, de mayor o menor valor, de bie-

* Comunicación presentada en el Congreso Internacional "Estrategias actuales en materia de Mediación y Arbitraje comercial", que tuvo lugar en la Universidad de Alcalá el 24 abril 2018.

** Abogado y Doctor en Derecho. Profesor de Derecho internacional privado. Universidad Pablo de Olavide

ISSN 1888–5373
DOI 10.19194arbitrajeraci.11.02.07

nes específicos de Internet y condicionadas por la configuración de la red. Las peculiares características de los conflictos surgidos en el ámbito del comercio electrónico, unido al potencial de las vías electrónicas para la rápida y eficaz resolución de controversias, contribuyen a la importancia atribuida al empleo de mecanismos extrajudiciales en un entorno electrónico.

La creación de estos mecanismos de solución de controversias, desarrollados en línea y configurados como una alternativa voluntaria, no excluyente del ejercicio de acciones ante tribunales estatales, reviste especial importancia en relación con las transacciones típicas de comercio electrónico; en particular, en situaciones transfronterizas donde no existen mecanismos de arbitraje, en sentido propio, disponibles, al menos, en sistemas tan restrictivos como el español[1].

Reconociendo el valor del arbitraje, como medio para solucionar controversias, nacidas de las relaciones comerciales internacionales y el desarrollo de las tecnologías de la comunicación, resulta fundamental, para que los consumidores y las empresas dispongan de instrumentos para resolver los litigios, sobre todo, si las partes se encuentran en jurisdicciones diferentes.

Hoy en día, las tecnologías tienen una función cada vez más central en la resolución de litigios y podrían contribuir a ofrecer una alternativa verosímil al procedimiento judicial, como ya de *facto* se hace; porque, entre otras cosas, mejora el acceso a esos mecanismos, agiliza el proceso y ofrece a las partes un mayor control del procedimiento de resolución[2].

En esta situación, surgen las ODR (*Online Dispute Resolution*), permitiendo que las partes en un procedimiento de ADR puedan resolver cualquier disputa online de principio a fin. Las ODR eliminan nuestra limitación física, proporcionando un entorno en línea productivo, en el que resolver cualquier tipo conflicto.

Con las ODR se observa el potencial de la tecnología para dar respuesta a las necesidades de comercio electrónico en crecimiento, día tras día, explicándose así la necesidad de aparición de plataformas informáticas dispuestas a ofrecer servicios de resolución de conflictos en línea, siendo los primeros intentos a través del Grupo de Trabajo III de la CNUDMI/UNCITRAL; a partir de 2010, se ha ocupado de la solución de controversias por vía informática surgidas a raíz de operaciones transfronterizas de comercio electrónico, incluidas las operaciones entre empresas y entre empresas y consumidores. En el ámbito europeo, se ha adoptado el Reglamento 524/2013, del Parlamento Europeo y del Consejo, de 21 de mayo, sobre resolución de litigios en línea en materia de consumo y la Directiva 2013/11/UE, del Parlamento Europeo y del Consejo, de 21 de mayo, sobre resolución alternativa de litigios

[1] P.A De Miguel Asensio, *Derecho Privado de Internet*, 5ª ed., Madrid, Civitas/Thomsom Reuters, 2015, pp. 971.

[2] Comisión Europea: *Comunicación relativa a la mejora del acceso de los consumidores a mecanismos alternativos de solución de litigios (COM/2001/0161 final)*, Bruselas, 4 abril 2001. Disponible en: http://eur–lex.europa.eu/legal–content/ES/TXT/?uri=CELEX:52001DC0161 (última visita: 5/5/2018).

en materia de consumo, con la que se pretende dar respuesta a la necesidad de desarrollo del mercado interior del comercio en línea.

Dicho lo anterior, debe tenerse en cuenta que las ODR pueden ayudar a resolver una situación, que se plantea en relación con las operaciones transfronterizas de comercio electrónico, debido a que el sistema judicial tradicional no ofrece una solución adecuada, para las controversias derivadas del comercio electrónico transfronterizo. Motivo por lo que las ODR deberían ser una vía sencilla, rápida y eficiente para que pudiera utilizarse en el "mundo real", y no debería entrañar gastos, demoras ni cargas desproporcionadas en relación con el valor económico del objeto del litigio.

No obstante, a pesar de los principios sobre los que se sustentan de equidad, la transparencia, el respeto de las garantías procesales y la rendición de cuentas, se plantean retos con relación a los problemas propios que en este entorno se producen.

II. Las ODR y la tecnología empleada

Las ODR son un "mecanismo para resolver controversias facilitado mediante el empleo de las comunicaciones electrónicas y demás tecnologías de la información y las comunicaciones"[3]. Ese proceso puede implementarse de maneras diferentes por los distintos administradores, y puede evolucionar con el tiempo[4].

Nótese como se vale de esta vía electrónica de comunicación para facilitar la solución de controversias, mediante el recurso a los servicios de uno o más terceros llamados a resolverla, por medio de una decisión, que podrá ser o no ser vinculante para las partes.

El aspecto tecnológico es crucial para la efectividad del proceso. Cada forma de ODR puede utilizar un sistema tecnológico diferente, individualizando el curso de un proceso dado. De la misma manera, pueden tomarse diferentes formas, desde una plataforma de Internet completamente automatizada, utilizando un portal basado en el chat electrónico o la videoconferencia (tipo Skype) o hasta el uso exclusivo de métodos como correo electrónico[5]. La primera opción constituye un sistema a través del cual se analizan las posibilidades de solución de controversias con el mediador de forma directa. La segunda opción se utiliza, por ejemplo, en la mediación dentro de un sistema de ofertas presentadas, en la que las partes acuerdan una cantidad aceptable para todas, sin la necesidad de reunirse directamente.

---

[3] Cnudmi/Uncitral: *Notas técnicas de la CNUDMI sobre la solución de controversias en línea*, Naciones Unidas, Nueva York, 2017, p. 4.

[4] Cnudmi/Uncitral: *A/CN.9/WG.III/XXXII/CRP.3 – Solución de controversias en línea en las operaciones transfronterizas de comercio electrónico. Documento presentado por Colombia y los Estados Unidos de América*, Viena, 30 de noviembre a 4 diciembre 2015, p. 6.

[5] K. Mania, "Online Dispute Resolution: The Future of Justice", *Int'l Comp. Jurisp.*, vol. 1, 2015, pp. 76–86.

Con lo anterior, puede comprobarse que las ODR requieren de un intermediario de base tecnológica que determine un sistema que permita generar, enviar, recibir, almacenar, intercambiar o procesar de algún otro modo las comunicaciones; es decir, una plataforma que, como es lógico, debe administrarse y coordinarse por el administrador ODR; también se podría encomendar la administración de la plataforma ODR a una entidad separada de ésta[6]. Lo que nos lleva a la computación en la nube o *cloud computing* y, así, a identificar una serie de cuestiones relacionadas con el diseño de los sistemas, su desarrollo y funcionamiento; al favorecimiento de la interoperabilidad y normalización de la plataforma, para permitir adaptarse al medio y a los procesos de intercambio de datos.

1. Plataformas de ODR

Como hemos comentado, hablar de plataformas de ODR es hablar de computación en la nube o *cloud computing* que, de un modo general, puede definirse como los servicios informáticos (por ejemplo, el almacenamiento y el procesamiento de datos) por Internet[7] o lo que es lo mismo, el almacenamiento, tratamiento y utilización de datos en ordenadores a distancia a los que se tiene acceso a través de Internet[8]; es decir, la computación en nube permite la disponibilidad de capacidad informática en todas partes y para cualquier persona.

Debemos tener claro, que hablamos de un modelo que permite acceso de red ubicuo, conveniente y bajo demanda a un conjunto de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios), que pueden aprovisionarse y liberarse rápidamente, con un mínimo esfuerzo de gestión o interacción por parte del proveedor de servicios.

La computación en la nube tiene la capacidad de implementar a varios modelos y marcos. La clasificación más común es el modelo de servicios de software, plataforma e infraestructura con software como servicio (SaaS), plataforma como servicio (PaaS) e infraestructura como servicio (IaaS)[9]. Estos servicios difieren según su flexibilidad y nivel de optimización.

Dentro de la clasificación anterior, puede decirse que la mayoría de las plataformas serán del modelo de SaaS, otorgando a las partes la capacidad

---

[6] Cnudmi/Uncitral: *A/CN.9/WG.III/WP.140 – Solución de controversias en línea en las operaciones transfronterizas de comercio electrónico. Proyecto de documento final con principios y elementos de un proceso ODR*, Nueva York, 29 de febrero a 4 marzo 2016, p. 27.

[7] Cnudmi/Uncitral: *Labor prevista y posible labor futura: parte cuarta Propuesta del Gobierno del Canadá: posible labor futura en materia de comercio electrónico: cuestiones jurídicas que afectan a la informática "en la nube"*, Nueva York, 7 a 18 julio 2014, p. 2.

[8] Comisión Europea: *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Liberar el potencial de la computación en nube en Europa (SWD (2012) 271 final) COM (2012) 529 final*, Bruselas, 27 septiembre 2012, p. 2.

[9] B. Shojaiemehra Amir, M. Rahmania Nooruldeen y N. Qader, "Cloud computing service negotiation: A systematic review", *Computer Standards & Interfaces*, vol., 2018, pp, 196–206.

de utilizar las aplicaciones del proveedor que se ejecutan en una infraestructura de nube[10]. Los consumidores no administran ni controlan la infraestructura en la que se ejecutan las aplicaciones[11]. Las aplicaciones son accesibles desde varios dispositivos cliente a través de una interfaz de cliente delgada, como un navegador web (*v.gr*., correo electrónico basado en la web), o una interfaz de programa. El modelo SaaS también suele estar estandarizado, pero su configuración, eficiencia y escalabilidad pueden variar. La facilidad con la que se pueden comprar las aplicaciones SaaS ha hecho que este modelo particular de servicio en la nube sea la forma más ampliamente adoptada.

No obstante, también podrá darse el modelo PaaS, que es una extensión de SaaS, no será el administrador quien tiene el control sobre las aplicaciones instaladas y, en algunos casos, la configuración del entorno de alojamiento[12]. Por consiguiente, no administran ni controlan la infraestructura de la nube central, como servidores, sistemas operativos o almacenamiento.

Asimismo, la plataforma o foro facilitado por el proveedor de servicios ODR, será accesible al público en general[13], como pudiera ser un sitio en Internet (plataforma abierta o pública) o una plataforma de acceso limitado o restringido, como sería el caso de un sistema interno de gestión de archivos informáticos o Intranet (plataforma cerrada o privada)[14].

2. Necesidades de interoperabilidad y normalización de la tecnología

La Unión Europea ha reconocido el potencial de las ODR, al igual que el potencial del *cloud computing*[15], determinando problemas claves y los pasos

---

[10] Un ejemplo, la encontramos en la plataforma para la Resolución de litigios en línea creada a través del Reglamento 524/2013 del Parlamento Europeo y del Consejo, de 21 mayo 2013, sobre resolución de litigios en línea para los litigios de los consumidores y por el que se modifican el Reglamento 2006/2004 y la Directiva 2009/22/CE (Reglamento sobre la RLL de los consumidores). La plataforma se encuentra disponible en: "http://eur–lex.europa.eu/legal–content/EN/TXT/?qid=1426859531321&uri=CELEX%3A32013R0524" (última visita 12/04/2018).

[11] National Institute of Standards and Technology (nist), U.S. Departament of Commerce, *The NIST Definition of Cloud Computing – Recommendations of the National Institute of Standards and Technology*, septiembre, 2011, p. 3.

[12] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica y M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing", *Electrical Engineering and Computer Sciences University of California at Berkeley*, febrero, 2009. Disponible en: "https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS–2009–28.pdf" (Última visita: 24/5/2018).

[13] Cnudmi/Uncitral: *A/CN.9/WG.III/WP.105 – Solución por vía informática de controversias surgidas en el marco de operaciones de comercio electrónico transfronterizas*, Viena, 13 a 17 diciembre 2010, p. 11.

[14] En relación los tipos de cloud computing, *vid.* L. Joyanes Aguilar, "Computación en la nube (Notas para una estrategia española en cloud computing)", *Revista del instituto español de estudios estratégicos*, nº 0, 2012.

[15] Comisión Europea: *Comunicación de la Comisión al Parlamento Europeo, al Consejo, Al Comité Económico y Social Europeo y al Comité de las Regiones: Liberar el potencial de la computación en nube en Europa*, COM (2012) 529 f*inal*, Bruselas, 27 septiembre 2012, p. 18.

necesarios que deben tomarse para eliminar cualquier barrera, para su desarrollo. En este sentido, destaca la necesidad de normalización de las TIC, especialmente en el ámbito de la ODR, tratando de definir desarrollar, mejorar, poner en práctica, mantener y fomentar servicios y herramientas, normas y especificaciones interoperables[16].

Como denominador común, un problema a todas las infraestructuras, la falta de interoperabilidad. En este sentido, como ha recalcado la Comisión Europea, en varias ocasiones, el mayor obstáculo a la interoperabilidad suele ser la falta de una estructura normalizada de los datos, por lo que debe considerarse como una cuestión necesaria la posibilidad de definir los datos de referencia que se requieren en los servicios transfronterizos.

Por ello, además del desarrollo de una normalización oficial internacional y de la UE, es necesario adoptar medidas para respaldar las especificaciones técnicas, en materia de TIC, elaboradas por otros organismos de normalización y las buenas prácticas generalmente aceptadas, que se utilizan de hecho con mayor frecuencia[17]. Igualmente, debe considerarse esencial que se desarrollen procedimientos, para garantizar que las necesidades de los usuarios finales de las normas se conocen en el momento de elaborar los planes de normalización[18]. En este sentido, debe tenerse en cuenta que las referencias a la tecnología aparecen, a veces, de manera casi imperceptible en cualquier Ley. Con frecuencia, las normas técnicas se incorporan al ordenamiento jurídico, evolucionando hacia normas jurídicas; que, al final, llegan a limitar la aplicación de otras, que en la mayoría de los casos están relacionadas con aquellas[19].

La lectura de las normas técnicas, en materia de interoperabilidad, permite observar el grado de precisión técnica al que se llega, imposible de alcanzar a través de las normas jurídicas, que les dan amparo[20]. La complejidad técnica y la permanente evolución justifican, plenamente, el recurso a las

---

[16] Comisión Europea: *Marco Europeo de Interoperabilidad – Estrategia de aplicación COM/2017/0134 final*, Bruselas, 23 marzo 2017. Disponible en: http://eur–lex.europa.eu/legal–content/ES/TXT/?uri=COM%3A2017%3A134%3AFIN (última visita: 24/5/2018).

[17] Comité Económico y Social Europeo: *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones — Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora,* COM (2016) 410 final, DO de 10.3.2017, p. 4, "https://eur–lex.europa.eu/legal–content/ES/TXT/?uri=CELEX:52016AE4559" (última visita: 23/05/2018).

[18] Debe tenerse en cuenta por normalización las especificaciones técnicas sobre una materia determinada, tal como resulte de los trabajos preparatorios y hayan sido difundido para obtener comentarios al respecto o informar al público, y cuya adopción se contemple de acuerdo con el procedimiento de normalización correspondiente, en el sentido recogido por el Reglamento 1025/2012, de 25 octubre 2012, sobre normalización, que deja lugar para las especificaciones internacionales basadas en el consenso (art. 10 del Reglamento).

[19] A. Cerrillo Martínez, *A las puertas de la administración digital,* Madrid, Instituto Nacional de Administración Pública (INAP), 2016, p. 42.

[20] A. Merchán Murillo, *Firma Electrónica: Funciones y Problemática (Especial referencia al reglamento (UE) nº 910/2014, relativo a la identificación electrónica por la que se deroga la directiva 199/93/CE de firma electrónica)*, Pamplona, Thomson Reuters – Aranzadi, 2016, p. 123 –126.

normas técnicas para fijar estos aspectos, que, por otro lado, tienen un gran impacto en el desarrollo de cualquier aplicación.

Con lo anterior, nos referimos a la necesidad de crear marcos de interoperabilidad, para los sistemas de información; pues, estos resultan de vital importancia, para permitir la consecución del objetivo de permitir integrar la prestación y administración de servicios, en una ventanilla única[21] (o portal electrónico) y, así, garantizar que todos los procedimientos y trámites relativos al acceso a una actividad de servicios y a su ejercicio se puedan realizar fácilmente, a distancia y/o por vía electrónica, tal y como estableció en su día la Directiva 2006/123/CE, de 12 diciembre 2006, relativa a los servicios en el mercado interior.

No debe olvidarse que la plataforma de ODR aparece como una plataforma de resolución de litigios en línea, que opera a modo de ventanilla única, mediante la intervención de una serie de entidades vinculadas, que ofrecen medios de resolución alternativa, con garantía de calidad[22].

Para garantizar que el punto de contacto único funcione como verdadero centro de administración, para la Resolución de litigios en línea, debe permitir el acceso a los ciudadanos y a las empresas, creando un servicio transfronterizo esencial, que se corresponda con necesidades definidas, conforme al fin que se pretende para las ODR, respetando el principio de neutralidad tecnológica.

Solo de esta manera, se puede determinar un sistema jurídico específico, que permita a los actores actuantes comunicarse, intercambiar información, ofrecer y usar servicios en tiempo real. Por ello, las normas y/o actuaciones que los Estados realicen, deben cumplir con determinados componentes técnicos normalizados, que permitirán una solución al transporte seguro de datos, al desarrollo y al mantenimiento de los componentes específicos nacionales necesarios.

III. Factores a tener en cuenta en el uso de las plataformas de ODR

En síntesis, un arbitraje online debe, ante todo, sustentarse en factores tales como el aseguramiento sobre la naturaleza de los datos a transferir, el país de origen, el país receptor, la razón por la cual se procesan los datos y las medidas de seguridad vigentes, para la transferencia y el procesamiento de los datos personales en juego.

---

[21] UN/CEFACT: *Recommendation and Guidelines on Establishing a Single Window to Enhance the Efficient Exchange of Information between Trade and Government, Recommendation No. 33*, Nueva York, 2005, pp. 3 y 4, "http://www.unece.org/fileadmin/DAM/cefact/recommendations/rec33/rec33_trd352e.pdf" (última visita: 10/5/2018).

[22] M.B. Aige Mut, "Aproximación a los diferentes mecanismos alternativos de resolución de conflictos: especial referencia a la nueva plataforma europea para resolución de litigios", *Diario La Ley*, nº 8732, abril, 2016, p. 5.

Las ODR se desarrollan en la nube, a través de lo que hoy conocemos como *cloud computing*, realizándose el acceso a todos los procesos y documentación asociada a este[23], a través de la nube. Este hecho permite sugerir normas específicas y estándares legales, con miras a asegurar la confianza (fe en la autenticidad) en el intercambio internacional de documentos y datos electrónicos entre partes (sujetos) que interactúan electrónicamente.

En este contexto, observamos cuestiones ventajosas, las partes implicadas en un procedimiento arbitral podrán presentar sus documentos y alegaciones a través de la nube, así como la información será consultable desde cualquier lugar, en cualquier momento y desde cualquier dispositivo fijo o móvil, por parte de los usuarios, previamente autorizados como los árbitros y los miembros de las partes en conflicto, realizándose una apuesta por la digitalización de los expedientes y la implementación de la política de papel cero haciéndola realmente efectiva, en consonancia con las tendencias de la Justicia moderna.

Lo anterior, nos permite comprobar que se está produciendo la modificación del actual régimen de arbitraje internacional, para acomodarlo a las nuevas tecnologías de la información y de las comunicaciones y su aplicación a las formas tradicionales del arbitraje. Sin embargo, a pesar de esta tendencia, nos podemos encontrar con problemas, propios de este entorno.

1. El administrador de las ODR

Las ODR requieren un intermediario de base tecnológica. De esta forma, un proceso ODR no se puede sustanciar con la participación, únicamente, de las partes en la controversia y un decisor neutral; es decir, sin un administrador. Por el contrario, para que pueda usarse la tecnología, a fin de facilitar la solución de una controversia, un proceso ODR debe contar con un sistema que permita generar, enviar, recibir, almacenar, intercambiar o procesar, de algún otro modo, las comunicaciones[24].

Se suele recurrir, como regla general, a la subcontratación y la externalización de los servicios estratificados de computación en la nube[25]. Las condiciones estándares de los proveedores pueden reservarle, expresamente, al proveedor el derecho a recurrir a terceros, para prestar al cliente los servicios de computación en la nube, o este derecho puede resultar implícito, debido a la propia naturaleza de los servicios que han de prestarse. En cualquier caso, al proveedor le interesa conservar la mayor flexibilidad posible en ese sentido.

---

[23] *Vid*., *v.gr*., que el Tribunal Arbitral de Barcelona (TAB) da acceso a todos sus procesos y documentación asociada a través de la nube con el objetivo de lograr una mayor simplificación administrativa y un ahorro relevante de costes en la partida de papel.

[24] Cnudmi/Uncitral: *A/CN.9/WG.III/XXXII/CRP.3 – Solución de controversias en línea en las operaciones transfronterizas de comercio electrónico. Documento presentado por Colombia y los Estados Unidos de Amérc*a, Viena, 30 de noviembre a 4 diciembre 2015, p. 6.

[25] Cnudmi/Uncitral: *A/CN.9/WG. IV/WP.148 – Aspectos contractuales de la computación en la nube*, Nueva York, 16 a 20 abril 2018, p. 26.

De esta forma, se debe contemplar quién es el administrador ODR y de la plataforma ODR, que deberá adoptar y aplicar medidas de confidencialidad adecuadas, para garantizar la seguridad del proceso. También, habrá que garantizar la autenticidad de las comunicaciones y la identidad de las partes, así como la identificación de la institución arbitral, que gestionará electrónicamente la causa sometida a arbitraje.

Dicho lo cual, debemos tener en cuenta situaciones de transparencia[26], siendo aconsejable que se dé a conocer toda relación contractual, que pueda existir entre el administrador de servicios ODR y un determinado proveedor, para que los usuarios del servicio estén informados de cualquier posible problema que pudiera surgir. Hablamos de una situación en la que una de las partes (el proveedor) proporciona a otra (el administrador de las ODR) un servicio de computación en la nube para unos usuarios finales (las partes litigantes).

Hay que tener en cuenta que a las partes le interesa, sobre todo, obtener garantías relativas al cumplimiento, por parte de terceros de los requisitos de seguridad, de la confidencialidad, la protección de datos, la ausencia de conflictos de intereses y el riesgo de incumplimiento del contrato por el proveedor, ante posibles incumplimientos por él o por terceros[27].

2. Acceso a la plataforma

La identidad electrónica, en la computación en nube, es una identificación que se compone de información almacenada y transmitida a los distintos usuarios de ésta. Pensemos que la identidad es un elemento fundamental, que va a vincular la información con su propietario y, por tanto, con el buen manejo efectivo y seguro de los datos específicos que dan entrada a la nube. De esta forma, nos encontramos ante una forma diferente de realizar transacciones. Situando la identidad electrónica a un nivel sin precedentes de importancia personal, comercial y legal.

No debe olvidarse que, en el contexto de la computación en la nube, hablamos, en la mayoría de los casos, de datos transfronterizos, por lo que debe tenerse en cuenta la necesidad de establecer métodos seguros de autenticación electrónica para las transacciones por Internet y para el desarrollo del mercado único digital. Los servicios de computación en nube convierten en necesaria la autenticación fiable de la identidad del usuario, para garantizar la confianza y dinamizar el uso de los servicios[28]. En este ámbito se han realizado marcos normativos para permitir una autenticación y autorización fia-

[26] Cnudmi/Uncitral: *A/CN.9/WG.III/WP.138 – Solución de controversias en línea en las operaciones transfronterizas de comercio electrónico*, Viena, 30 de noviembre a 4 diciembre 2015, p. 2.

[27] Cnudmi/Uncitral: *A/CN.9/WG. IV/WP.148 – Aspectos contractuales de la computación en la nube*, Nueva York, 16 a 20 abril 2018, pp. 25.

[28] Un procedimiento único de apertura de sesión simplifica requerirá el uso de un conjunto de servicios y métodos de autenticación más complejos y fiables que el de una simple contraseña de creación propia para potenciar la confianza en el conjunto de proveedores de que se trate.

bles en la nube, a través de los Reglamentos 910/2014 del Parlamento Europeo y del Consejo, de 23 julio 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y el Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 abril 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

En cualquier caso, todos los esquemas de identidad electrónica dependen de dos procesos: primero, autenticación de identidad y, posteriormente, autenticación/verificación de identidad[29]. Cuando se autentica, la identidad se registra en el sistema y luego se puede usar para realizar transacciones. Ésta se verifica en el momento de cada transacción, desde dentro de la propia nube.

De la información registrada en ese momento, surge la información de identificación tal y como si fuera la firma, que se usa para vincular a un individuo de manera inseparable.

Con lo anterior, observamos, que dentro de la nube se producirán dos elementos que se unirán para facilitar la identidad de la persona que se sitúa dentro de la nube. Estos dos elementos fundamentalmente son: la identidad fijada al individuo y otra fijada a la propia transacción que se realiza[30]. La primera, será la que identifique a las partes y, por tanto, tendrá un efecto directo sobre la formación y sobre la exigibilidad del contrato, determinando así su capacidad para obligarse contractualmente; suele ser suficiente con incluir el nombre de dicha persona jurídica, su forma legal, su número de inscripción en el registro (si procede) y su domicilio social o dirección de negocio, junto con la mención de sus documentos fundacionales. La segunda, sería la parte más sustancial de la información de la transacción y que se actualiza continuamente, en función de las transacciones que realice en la nube.

Lo importante es, una vez fijados los elementos, cuál sería el que debe obtener mayor o menor protección, teniendo en cuenta la transferibilidad y la seguridad de los datos, la subcontratación y la asignación de riesgos.

3. Identificación de las partes

Tengamos presente que, hoy día, nos hemos acostumbrado a realizar transacciones electrónicas, con carácter comercial o no, sin preguntarnos si los procesos y/o procedimientos electrónicos son suficientemente seguros, basta con que nos brinden un determinado nivel de seguridad, que otorga un cierto nivel de utilidad y "confianza" subyacente[31]. Lo cierto es que se presta muy poca atención a los procesos subyacentes, que recopilan la información

[29] A. Merchán Murillo, *Firma Electrónica...*, *op. cit*., p. 123.

[30] U. Ojiakoab, M. Chipulu, A. Marshall y T. Williams, "An examination of the 'rule of law' and 'justice' implications in Online Dispute Resolution in construction projects", *International Journal of Project Management*, vol. 36, 2018, pp. 301–316.

[31] F.D. Salinas Hinojosa, "Tokens De Seguridad", *Revista de Información, Tecnología y Sociedad*, nº 8, La Paz, junio, 2013.

y los datos utilizados para garantizar, por ejemplo, que somos quienes decimos que somos; pues, cuando una persona se inscribe para utilizar un determinado servicio electrónico, se crea una identidad electrónica. La creación de esta identidad electrónica supone establecer una relación de confianza mutua entre una persona y otra, lo que requiere conjugar estas relaciones bilaterales en un marco de confianza.

Ahora bien, en esta era de phishing, piratería informática, ingeniería social y robo de identidad, la respuesta a la pregunta "¿Quién es usted?" y "¿Cómo puede probarlo?" ha tomado una nueva dimensión. En un entorno en línea, autenticar la identidad de la parte remota es más importante que nunca. Desempeña un papel clave en la lucha contra el fraude de identidad y, además, es esencial para establecer una confianza necesaria que facilite cualquier tipo de transacción electrónica.

En la realidad, constituida por las tecnologías de la información, interesa todo lo relacionado con la identidad y la confidencialidad de sus datos personales, la existencia y validez de sus declaraciones de voluntad, la autoría e integridad de sus mensajes electrónicos y el no rechazo del mensaje en su origen y destino, todo en un marco de seguridad, validez jurídica y, también, en la existencia del documento electrónico, así como su autenticación a través de la firma electrónica.

La importancia de la identidad electrónica es total para garantizar: que la persona, que va a acceder a la plataforma, es quien dice ser, ya que puede probarlo; así como, su capacidad de obrar con libertad de actuación a la hora de firmar el contenido del documento, que, presumiblemente, va a subir a la plataforma. En este sentido, no debemos olvidar, que la firma electrónica no puede garantizar la identidad de la persona ni si se ha utilizado o no con o sin consentimiento[32]. No obstante, si podemos afirmar que las firmas electrónicas pueden ser signos de identidad, porque sabemos que forzosamente son atributos de identidad[33].

En este punto, conviene destacar, que verificar la identidad de una persona o entidad, que, a su vez, busca acceso remoto a un sistema corporativo de computación en nube, que crea una comunicación electrónica o que firma un documento electrónico, es lo que se llama gestión de identidad, que puede ser, bien, proceso de reunión, verificación y validación de información de atributos adecuada acerca de un sujeto concreto (persona física, persona jurídica, dispositivo u otro tipo de entidad) para definir y confirmar su identidad en un contexto específico[34]; bien, el proceso mediante el cual se valida y verifica información suficiente como para confirmar la identidad alegada por la entidad; o bien, el proceso mediante el cual la autoridad de registro

[32] A. Madrid Prra, "La identificación en el comercio electrónico", *Revista de Contratación Electrónica*, nº 15, abril 2001, pp. 3–60.

[33] Cnudmi/Uncitral: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009, pp. 15 ss.

[34] La identidad puede comprobarse mediante la aseveración realizada por la propia entidad o mediante comparación con registros existentes; y se entiende por "demostración de identidad.

obtiene y verifica suficiente información para identificar una entidad con un nivel de garantía especificado o tácito[35].

La gestión de la identidad cada vez juega un papel más importante. Como ha señalado la Comisión Europea[36], la gestión de la identidad electrónica constituye un elemento clave para la prestación de cualquier servicio electrónico. Por otra parte, la identificación electrónica confiere a las personas que utilizan procedimientos electrónicos la garantía de que su identidad y sus datos personales no se utilizan sin autorización. De esta forma, puede decirse que desempeña un papel clave en el establecimiento de relaciones de confianza. Asimismo, es un componente esencial de cualquier estrategia, para proteger los sistemas de información y las redes, los datos financieros, la información personal y otros activos contra el acceso no autorizado o el robo de identidad. Entre las ventajas[37] de ésta pueden figurar, desde la perspectiva del prestador, mejoras en la seguridad, la facilitación del cumplimiento de las normas pertinentes y la agilización de las transacciones, así como, desde el punto de vista del usuario, la facilitación del acceso a la información.

Visto lo anterior, puede concluirse que la gestión de la identidad y los propios procedimientos de identificación pueden servir de base para la definición de los niveles de confianza de los sistemas de identificación[38]. Al considerar la confianza debemos pensar en la seguridad jurídica y técnica de los propios servicios prestados, que deben tener efectos legales indiscutibles, siempre que cumplan con los requisitos básicos exigidos. Desde este punto de vista, debemos tener en cuenta que la confianza no es una simple cuestión de la percepción subjetiva, sino una cuestión objetiva que debe venir dada por la propia transacción.

Por ello, deben usarse ciertos factores de autenticación, por ejemplo, los establecidos en el Reglamento de Ejecución 2015/1502, de 8 septiembre 2015, sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el art. 8, ap. 3, del Reglamento 910/2014, que establece especificaciones técnicas mínimas, las normas y los procedimientos con referencia a los cuales se especificarán los niveles de seguridad de los medios de identificación electrónica. En el marco de la determinación de los niveles de seguridad vinculados a la gestión de la identidad, se fijan tres ni-

[35] Cnudmi/Uncitral: *Cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza. Términos y conceptos relativos a la gestión de la identidad y los servicios de confianza*, Nueva York, 24 a 28 abril 2017, p. 6.

[36] Comisión Europea: *Plan de acción sobre la firma electrónica y la identificación electrónica para facilitar la prestación de servicios públicos transfronterizos en el mercado único (COM (2008) 798 final)*, Bruselas, 28 noviembre 2008, p. 11.

[37] Cnudmi/Uncitral: Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica, Viena, 2009, p. 131.

[38] Cnudmi/Uncitral: *Aspectos jurídicos relacionados con la gestión de la identidad y los servicios de confianza*, Nueva York, 16 a 20 abril 2018, p. 5.

veles: a) nivel de seguridad bajo; b) nivel de seguridad sustancial, y c) nivel de seguridad alto.

Estos niveles de seguridad se describen de acuerdo con especificaciones técnicas, normas y procedimientos conexos. De este modo, puede decirse que se crea un mecanismo de cooperación, así como un marco de interoperabilidad, para definir los criterios de seguridad, para intercambiar la información relativa a los medios de identificación electrónica y sus respectivos niveles de seguridad, consagrando así el principio de reconocimiento mutuo para los medios de identificación que tuvieran un nivel de garantía equivalente, a partir del nivel de garantía suficiente o superior.

Con ello, podría plantearse el establecimiento de un entorno transfronterizo de confianza, en aras de asegurar los derechos e intereses jurídicos de todas aquellas personas que realicen en forma electrónica operaciones informáticas con significación jurídica mediante el empleo de Internet u otros sistemas abiertos de uso masivo de tecnologías de la información y las comunicaciones[39], ayudando a resolver el problema del intercambio transfronterizo de documentos electrónicos, que es de actualidad y se ha señalado en declaraciones a nivel mundial y regional[40].

4. Protección de los datos

Los datos son oro electrónico, la extracción y explotación de este activo se ha convertido en un modelo comercial clave, para innumerables empresas. El acceso ubicuo a Internet y el aumento de la capacidad informática de la nube hace que cada vez haya más usuarios en línea y, por tanto, más conflictos. Al mismo tiempo, el carácter transfronterizo que lleva de suyo Internet ha traído consigo un problema evidente en torno a la protección de los datos.

En este punto, vuelve a surgir la transparencia del procedimiento arbitral y de la actuación del proveedor de servicios ODR, como factor esencial para que el usuario confíe en la ODR, para la solución de sus reclamaciones.

La transparencia está ligada a la confidencialidad, que vendrá de las medidas y prácticas adecuadas de protección de datos, que contemplen, entre otras cosas, el secreto de las comunicaciones entre las partes litigantes y el administrador de servicios; pues, las condiciones del servicio de computación en nube o requisitos de ubicación de los datos, pueden variar dependiendo del Estado en el que se vaya a resolver el litigio.

La confidencialidad de las comunicaciones entre las partes litigantes y el administrador de servicios ODR y el proveedor, son un aspecto importante

[39] Cnudmi/Uncitral: *A/CN.9/WG.III/WP.136 – Solución de controversias en línea en las operaciones transfronterizas de comercio electrónico. Documento presentado por la Federación de Rusia*, Viena, 30 de noviembre a 4 diciembre 2015, p. 6.

[40] Cnudmi/Uncitral: *A/CN.9/WG. IV/WP.141 – Cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza, Nueva York*, 24 a 28 abril 2017, pp. 2 – 4.

de la relación del administrador de servicios ODR con las partes y ayuda a fomentar un clima de confianza, para que tenga lugar el proceso ODR.

Con lo anterior, debe tenerse en cuenta que las obligaciones contractuales entre ellos deben ser conocidas por las partes, como comentamos antes, especialmente, en materia de privacidad y de protección de datos. Sin embargo, puede darse el caso en el que los términos no proporcionen las clausulas referentes a las garantías de privacidad y protección de datos, por lo que habrá que preguntarse si la privacidad y la protección de datos pueden estar implícitas en el contrato de servicio, reconociéndose así, implícitamente, los requisitos de protección y privacidad de los datos. Aún, si la respuesta fuera afirmativa o no, ninguna duda cabe respecto al deber de informar sobre los peligros existentes y las opciones disponibles para minimizarlos.

En cualquier caso, las comunicaciones electrónicas deben estar protegidas en el curso del proceso en línea, pero también antes y después. De hecho, desde un entendimiento y reconocimiento de la importancia del deber de confidencialidad y la necesidad de una protección especial en un proceso en línea, cabe distinguir tres fases en la confidencialidad que deberá tenerse presentes en el curso de un arbitraje: la privacidad durante las actuaciones, la confidencialidad previa a la emisión del laudo y la confidencialidad a raíz de la emisión del laudo. Se tendrán por confidenciales[41] el curso de las actuaciones, la existencia del arbitraje aún pendiente de la emisión del laudo y el contenido del laudo, una vez emitido.

En el marco de la ODR, la confidencialidad es un requisito estrechamente vinculado al requisito de seguridad interna de la vía informática utilizada para la solución de la controversia. Además de aplicar las medidas técnicas destinadas a dotar de seguridad al intercambio por vía electrónica de comunicaciones y datos. La confidencialidad, como sabemos, debe tener por objeto impedir que cierta información llegue a personas no legitimadas para acceder a ella y prohibir a todo intermediario que comparta información con otras personas a fin de amparar toda información o dato confidencial que se comunique en el curso de las controversias. No obstante, puede observarse como los términos de privacidad de muchos contratos de servicios de computación en la nube no son lo suficientemente transparentes[42]; pues, no revelan la información necesaria a los usuarios y pueden no integrar todos los requisitos legales, llegando incluso a incluir términos imprecisos que se refieren a posibles terceros a quienes se pueden transferir los datos sin más aclaraciones.

En este punto, debemos tener en cuenta que la computación en nube implica cadenas de proveedores y otros agentes, tales como proveedores de

[41] D. Lavi, "Three is not a crowd: online mediation–arbitration in business to consumer internet disputes", *University of Pennsylvania Journal of International Law*, vol. 37, 2016, pp. 5 –71. Disponible en: "https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?referer=https://scholar. google.com/&httpsredir=1&article=1918&context=jil" (Última visita: 24/5/2018).

[42] Comisión Europea: *Comunicación se la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Las plataformas en línea y el mercado único digital Retos y oportunidades para Europa*, Bruselas, 25 junio 2016, p. 12.

infraestructuras o de comunicaciones[43], tal y como puede pensarse del estudio del que partimos, por lo que resulta necesario disponer de directrices más concretas sobre protección de datos, en particular, para identificar y distinguir los derechos y obligaciones correspondientes de los controladores y procesadores de datos que trabajan para los proveedores de servicios en la nube, o los agentes de la cadena de valor[44].

5. Ejecutividad de las ODR

Otro reto importante se plantea respecto al atractivo que ganarían las ODR si se les dotara a todo arreglo o transacción que se negocie de un régimen ejecutorio expeditivo. En síntesis, un arbitraje online debe, ante todo, sustentarse en factores tales como el aseguramiento sobre la naturaleza de los datos a transferir, el país de origen, el país receptor, la razón por la cual se procesan los datos y las medidas de seguridad vigentes para la transferencia y el procesamiento de los datos personales en juego.

Internacionalmente, el marco legal del arbitraje es una mezcla de Convenciones internacionales, instrumentos legales, y Leyes nacionales, que regulan tanto su procedimiento como las Leyes de fondo aplicables. Los textos internacionales y nacionales requieren que la libre decisión de las partes conste de forma indubitada. De ahí que, se requiera que el convenio arbitral conste "por escrito". No se trata de un requisito de pura formalidad que se agota en sí mismo. Se exige, como primer paso, que haya una manifestación de voluntad fácilmente accesible, para conocer la voluntad de las partes y el alcance de ésta. Luego vendrá la determinación del contenido de la cláusula arbitral, que señala el ámbito o límites de la actuación arbitral; pues, el primer paso en pro de la electronificación[45], se da por parte del regulador al admitir, expresamente, que la constancia escrita del convenio arbitral, no se circunscribe al soporte papel, sino que abarca también el soporte electrónico.

En cualquier caso, el debate sobre la validez del convenio arbitral, perfeccionado por medios electrónicos se plantea como consecuencia de los requisitos de forma exigidos por la Convención sobre Reconocimiento y Ejecución de Sentencias Arbitrales Extranjeras (Nueva York el 10 junio 1958), que por un lado, el art. 2 exige que el acuerdo conste por escrito y firmado por las partes, a no ser que resulte contenido en un canje de cartas o telegramas; y por otro, el art. 4, a efectos de reconocimiento y ejecución, obliga a las parte ejecutante a presentar el acuerdo arbitral original o copia que reúna las con-

[43] Cnudmi/Uncitral: *Aspectos contractuales de la computación en la nube*, Nueva York, 24 a 28 abril 2017, p. 4 y 5.

[44] Comisión Europea: *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Liberar el potencial de la computación en nube en Europa ({SWD (2012) 271 final}, COM (2012) 529 final,* Bruselas, 27 septiembre 2012, p. 9.

[45] A. Madrid Parra, "Electronificación del arbitraje", *Revista Internacional de Estudios de Derecho Procesal y Arbitraje (Riedpa)*, 2011, nº 2, "http://www.riedpa.com/COMU/documentos/ RIEDPA21103.pdf" (última visita: 8/5/2018).

diciones requeridas para su autenticidad, lo que genera problemas de consentimiento de las partes al arbitraje.

La Convención de Nueva York no admite, expresamente, el canje de e–mails u otro tipo de comunicaciones electrónicas. Sin embargo, esta realidad fáctica si ha sido contemplada por el art. 7.2º LMU al aceptar el télex, telegramas u "otros medios de telecomunicación que dejen constancia del acuerdo". Aquí se pone de manifiesto esa posición abierta a la recepción de toda innovación, que facilite la contratación y la resolución de conflictos de intereses, y el art. 6.1º de la Ley Modelo sobre Comercio Electrónico dispone: "cuando la Ley requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos si la información que éste contiene es accesible para su ulterior consulta". Asimismo, el art. 2 nos dice que se entenderá "por mensaje de datos: la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax".

La expresión, que indica el requisito necesario para que se aplique el principio de equivalencia funcional a "escrito"; esto es, que la información esté "accesible para su ulterior consulta", ha sido incorporada a distintos ordenamientos jurídicos que han seguido la pauta de la Ley Modelo al contemplar la validez jurídica de la información existente en soporte electrónico[46], especialmente, la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (2005), que en el art. 9.2º dice: "cuando la ley requiera que una comunicación o un contrato conste por escrito, o prevea consecuencias en el caso de que eso no se cumpla, una comunicación electrónica cumplirá ese requisito si la información consignada en su texto es accesible para su ulterior consulta", observándose que su art. 20.1º dispone la posibilidad de que las disposiciones de la Convención serán aplicables al empleo de comunicaciones electrónicas en lo concerniente a la formación o el cumplimiento de un contrato al que sea aplicable cualquiera de los siguientes instrumentos internacionales, en los que un Estado contratante de la presente Convención sea o pueda llegar a ser parte de: Convención sobre el Reconocimiento y Ejecución de las Sentencias Arbitrales Extranjeras (Nueva York, 10 junio 1958); Convención sobre la Prescripción en Materia de Compraventa Internacional de Mercaderías (Nueva York, 14 junio 1974) y su Protocolo (Viena, 11 abril 1980); Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías (Viena, 11 abril 1980); Convenio de las Naciones Unidas sobre la Responsabilidad de los Empresarios de Terminales de Transporte en el Comercio Internacional (Viena, 19 abril 1991); Convención de las Naciones Unidas sobre Garantías Independientes y Cartas de Crédito Contingente (Nueva York, 11 diciembre 1995); Convención de las Naciones Uni-

[46] A. Madrid Parra, "Electronificación del arbitraje", *Revista Internacional de Estudios de Derecho Procesal y Arbitraje (Riedpa)*, 2011, nº 2, "http://www.riedpa.com/COMU/documentos/ RIEDPA21103.pdf" (última visita: 6/5/2018).

das sobre la Cesión de Créditos en el Comercio Internacional (Nueva York, 12 diciembre 2001).

6. Ley aplicable

En este ámbito habrá que distinguir por un lado la ley aplicable al contrato de *cloud computing* suscrito entre el proveedor del servicio y el administrador de servicios ODR; y por otra parte la ley aplicable al contrato que hayan celebrado entre sí los terceros respecto de dicho contrato de servicio. En ambos casos se trata de una cuestión relevante por el carácter transfronterizo de estos contratos, por la complejidad del diseño de la operación negocial, por los diferentes intereses en presencia, así como por la necesidad imperiosa de previsibilidad y seguridad jurídica.

En relación con el primero de los contratos indicados, nos encontraremos a menudo con situaciones en las que el proveedor especificará en el contrato la ley aplicable al mismo, sin que sea necesario vínculo alguno entre ésta y el contrato (aunque normalmente será la del lugar en la que se encuentra la sede principal de negocios del citado proveedor o su principal centro de actividades)[47]. No obstante, en función del objeto de la controversia, es posible que normas imperativas (por ejemplo, en materia de protección de datos, régimen de insolvencia, etc.) prevalezcan sobre las cláusulas del contrato, incluidas las relativas a la elección de la ley y, en su caso, de foro.

Respecto del segundo de los contratos señalados, probablemente ocurrirá que los terceros que lo suscriban desconozcan las cláusulas contractuales pactadas entre el administrador de servicios ODR y el proveedor del servicio en su contrato de *cloud computing*. Como en este último, las partes podrán pactar, al concertar su operación, cuál será la ley aplicable a su contrato[48]. Ese pacto suele formar parte de las condiciones generales del vendedor que sean aplicables a la operación concertada. Las partes podrán también determinar cuál habrá de ser la ley aplicable al arbitraje, cuando ya haya surgido la controversia.

A falta de acuerdo entre las partes, serán las normas de Derecho internacional privado vigentes en el Estado sede de la autoridad que conozca del asunto las que determinarán normalmente el Derecho sustantivo aplicable a cada contrato. En el arbitraje por vía informática, esta solución podría resultar ambigua al no estar claro cuál es el lugar efectivo del arbitraje. Por otra parte, cabe que el reglamento de arbitraje o las partes en el acuerdo de arbitraje autoricen al árbitro para decidir cuál será la ley aplicable al arbitraje en materia de derecho sustantivo.

Cabe, que las partes hayan remitido en su contrato, al concertar su operación, a un reglamento de arbitraje, en cuyo caso ese reglamento será aplica-

[47] Cnudmi/Uncitral: *Aspectos contractuales de la computación en la nube*, Nueva York, 24 a 28 abril 2017, pp. 6 y 7.

[48] Cnudmi/Uncitral: *Labor prevista y posible labor futura: parte cuarta Propuesta del Gobierno del Canadá: posible labor futura en materia de comercio electrónico: cuestiones jurídicas que afectan a la informática "en la nube"*, Nueva York, 7 a 18 julio 2014, p. 36.

ble a todo arbitraje que se entable a raíz de esa operación. Cabe, también, que las partes decidan dejar esta cuestión para cuando surja una controversia; ahora bien, existe el peligro de que, surgida la controversia las partes tengan dificultad en comunicarse, por razón de la controversia y la distancia que pudiera mediar entre ellas.

El régimen procesal que sea aplicable al arbitraje a tenor de la ley del foro servirá, a título de Derecho supletorio, para resolver toda cuestión procesal no resuelta por el reglamento designado de común acuerdo por las partes o por el árbitro.

IV. Conclusión

Sin lugar a duda, el advenimiento de Internet presentó un serio desafío para el movimiento de resolución alternativa de disputas. El ejercicio efectivo de las libertades de mercado, que ofrece Internet, hace necesario garantizar un acceso efectivo a los medios de resolución de disputas electrónicos. No hay duda de que la transición de las ADR al ciberespacio y su reformulación como ODR, crea desafíos que deben ser resueltos, pero también presenta oportunidades que no deben ser ignoradas.

La búsqueda de soluciones ante los tribunales o fuera de ellos forma parte del derecho de acceso a la justicia, protegido a nivel internacional, europeo y nacional. Este postulado se basa en la autonomía de poder elegir una forma de resolver el conflicto. Sin embargo, para el desarrollo de estos medios, LA resolución de conflictos resulta necesario crear un marco legal, que involucre herramientas electrónicas, que permitan el desarrollo de este tipo procedimientos electrónicos extrajudiciales.

Para poder hacer frente a los retos que se evocan en este artículo, es de capital importancia que se adopten medidas eficaces, para mantener la confianza de todos, garantizando un nivel adecuado de seguridad, portabilidad de los datos e interoperabilidad, así como el cumplimiento de los requisitos jurídicos prestablecidos. Sólo de esta forma, se aceptarán los beneficios resultantes y se podrá hacer frente al reto que presenta la computación en la nube para las ODR.

Bibliografía

AIGE MUT, M.B.: “Aproximación a los diferentes mecanismos alternativos de resolución de conflictos: especial referencia a la nueva plataforma europea para resolución de litigios”, *Diario La Ley*, núm. 8732, abril, 2016.

ARMBRUST, M.; FOX, A.; GRIFFITH, R.; JOSEPH, A.; KATZ, R.; KONWINSKI, A.; LEE, G.; PATTERSON, D.; RABKIN, A.; STOICA, I.; ZAHARIA, M.: “Above the Clouds: A Berkeley View of Cloud Computing”, *Electrical Engineering and Computer Sciences University of California at Berkeley*, febrero, 2009.

CERRILLO MARTÍNEZ, A.: *A las puertas de la administración digital,* Madrid, Instituto Nacional de Administración Pública (INAP), 2016.

Cnudmi/Uncitral: *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica*, Viena, 2009.

Cnudmi/Uncitral: *A/CN.9/WG.III/WP.105 – Solución por vía informática de controversias surgidas en el marco de operaciones de comercio electrónico transfronterizas*, Viena, 13 a 17 diciembre 2010.

Cnudmi/Uncitral: *Labor prevista y posible labor futura: parte cuarta Propuesta del Gobierno del Canadá: posible labor futura en materia de comercio electrónico: cuestiones jurídicas que afectan a la informática "en la nube"*, Nueva York, 7 a 18 julio 2014.

Cnudmi/Uncitral: *A/CN.9/WG.III/XXXII/CRP.3 – Solución de controversias en línea en las operaciones transfronterizas de comercio electrónico. Documento presentado por Colombia y los Estados Unidos de América*, Viena, 30 de noviembre a 4 diciembre 2015.

Cnudmi/Uncitral: *A/CN.9/WG.III/WP.140 – Solución de controversias en línea en las operaciones transfronterizas de comercio electrónico. Proyecto de documento final con principios y elementos de un proceso ODR*, Nueva York, 29 de febrero a 4 marzo 2016.

Cnudmi/Uncitral: *Cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza. Términos y conceptos relativos a la gestión de la identidad y los servicios de confianza*, Nueva York, 24 a 28 abril 2017.

Cnudmi/Uncitral: *Notas técnicas de la CNUDMI sobre la solución de controversias en línea*, Naciones Unidas, Nueva York, 2017.

Cnudmi/Uncitral: *A/CN.9/WG.IV/WP.148 – Aspectos contractuales de la computación en la nube*, Nueva York, 16 a 20 abril 2018.

Comisión Europea: *Comunicación relativa a la mejora del acceso de los consumidores a mecanismos alternativos de solución de litigios (COM/2001/0161 final)*, Bruselas, 4 abril 2001.

Comisión Europea A: *Plan de acción sobre la firma electrónica y la identificación electrónica para facilitar la prestación de servicios públicos transfronterizos en el mercado único (COM (2008) 798 final)*, Bruselas, 28 noviembre 2008.

Comisión Europea: *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Liberar el potencial de la computación en nube en Europa (SWD (2012) 271 final) COM (2012) 529 final*, Bruselas, 27 septiembre 2012.

Comité Económico y Social Europeo: *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones — Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora COM (2016) 410 final*, DOUE, 10 marzo 2017.

DE MIGUEL ASENSIO, P.A.: *Derecho Privado de Internet*, Madrid, Civitas / Thomsom / Reuters, 2015.

JOYANES AGUILAR, L.: "Computación en la nube (Notas para una estrategia española en cloud computing)", *Revista del instituto español de estudios estratégicos*, nº 0, 2012.

LAVI, D.: "Three is not a crowd: online mediation–arbitration in business to consumer internet disputes", *University of Pennsylvania Journal of International Law*, vol. 37, 2016.

MADRID PARRA, A.: "La identificación en el comercio electrónico", *Revista de Contratación Electrónica*, nº 15, abril 2001.

MANIA, K.: "Online dispute resolution: The future of justice", *International Comparative Jurisprudence*, vol. 1, 2015.

MERCHÁN MURILLO, A.: *Firma Electrónica: Funciones y Problemática (Especial referencia al reglamento (UE) nº 910/2014, relativo a la identificación electrónica por la que se deroga la directiva 199/93/CE de firma electrónica)*, Pamplona, Thomson Reuters – Aranzadi, 2016.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), U. S. DEPARTAMENT OF COMMERCE: *The NIST Definition of Cloud Computing – Recommendations of the National Institute of Standards and Technology*, septiembre, 2011.

OJIAKOAB, U.; CHIPULUC, M.; MARSHALLC, A.; WILLIAMSB. T.: "An examination of the 'rule of law' and 'justice' implications in Online Dispute Resolution in construction projects", *International Journal of Project Management*, vol. 36, 2018.

SALINAS HINOJOSA, F. D.: "Tokens De Seguridad", *Revista de Información, Tecnología y Sociedad*, nº 8, La Paz, junio, 2013.

SHOJAIEMEHRA AMIR, B.; RAHMANIA NOORULDEEN, M.; QADER, N.: "Cloud computing service negotiation: A systematic review", *Computer Standards & Interfaces*, vol. 2018.

UN/CEFACT: *Recommendation and Guidelines on Establishing a Single Window to Enhance the Efficient Exchange of Information between Trade and Government, Recommendation No. 33*, Nueva York, 2005.