REVISTA ESPACIOS

4 décadas difundiendo conocimiento

Volumen 41 • No. 19 • Año 2020 • Art. 10

Recibido: 26/01/2019 • Aprobado: 14/05/2020 • Publicado: 28/05/2020

Seguridad de la información en sistemas de resolución de disputas en línea (ODR): Revisión de la literatura y análisis a la luz del contexto colombiano

Information Security in Online Dispute Resolution (ODR) Systems: Literature review and analysis considering the Colombian context

CAMACHO, Jefferson[1]
GAMBOA, Sonia C. [2]
GÓMEZ, Luis C.[3]

Resumen
Los sistemas ODR se han convertido en una solución que facilita el acceso a la justicia, sin embargo, la gestión de la seguridad de la información ha generado varias preocupaciones. Este artículo presenta el resultado de una revisión sistemática de la literatura, siguiendo la metodología de Tranfield, donde se estudian los controles de seguridad aplicados en sistemas ODR alrededor del mundo y se contrastan con las disposiciones legales en Colombia para definir su aplicabilidad en el país.
Palabras clave: resolución de disputas en línea, seguridad de la información, acceso a la justicia.

Abstract
ODR systems have become a solution that facilitates access to justice, however, information security management has generated several concerns. This article presents the result of a systematic review of the literature, following Tranfield's methodology, where the security controls applied in ODR systems around the world are studied and contrasted with the legal provisions in Colombia to define their applicability in the country.
Keywords: online dispute resolution, information security, access to justice

1. Introducción

En los últimos años la tecnología ha avanzado a pasos agigantados en el campo de la informática y las telecomunicaciones. Las innumerables posibilidades que ofrece hoy en día el uso de las TIC (Tecnologías de

1 Investigador del grupo de investigación en Sistemas y Tecnologías de la Información, Universidad Industrial de Santander. jefferson.camacho@correo.uis.edu.co
2Profesora titular, escuela de ingeniería de sistemas e informática, Universidad Industrial de Santander. scgamboa@uis.edu.co
3 Director del grupo de investigación en Sistemas y Tecnologías de la Información. Profesor titular laureado, escuela de ingeniería de sistemas e informática, Universidad Industrial de Santander. lcgomezf@uis.edu.co.

Información y Comunicaciones) en el desarrollo de diferentes actividades socioeconómicas, han supuesto un cambio de paradigma social y el surgimiento de la denominada sociedad de la información y del conocimiento.

En el sector gobierno, por ejemplo, las TIC se han convertido en una herramienta fundamental para establecer un canal de comunicación directa con los ciudadanos y mejorar los servicios prestados por los diferentes entes gubernamentales. En este sentido, el Ministerio de Justicia y del Derecho, con el propósito de incorporar las TIC al mecanismo de conciliación en Colombia, definió una modalidad de conciliación virtual, donde la comunicación entre las partes y el proceso en general son llevados a cabo a través de internet con el apoyo de un sistema informático (Ministerio de Justicia, 2011). Sin embargo, hasta el momento, no se han establecido ni las condiciones legales ni el soporte tecnológico y de gestión de la información necesario para la implementación de dicha iniciativa en el país.

En contraste a la realidad observada en Colombia y en general en América Latina, donde se evidencia un marcado rezago en el uso de TIC aplicadas a la solución de disputas (Ministerio de Justicia & Banco mundial, 2011), en países como Estados Unidos, desde mediados de la década de 1990, gracias a los importantes aportes del profesor Ethan Katsh, actual director del centro nacional de tecnología y resolución de disputas de los Estados Unidos, se trabaja en el campo de la Resolución de Disputas en Línea (ODR, por sus siglas en inglés) (Katsh & Rule, 2016); aunque en principio ODR fue concebido como un mecanismo de solución de disputas en línea orientado al comercio electrónico, donde clientes y vendedores dirimieran sus conflictos a través de internet, dos décadas más tarde, ODR se ha trasladado a diferentes escenarios socioeconómicos alrededor del mundo, incluyendo aquellos de orden jurídico (Rabinovich-Einy & Katsh, 2014).

Poniendo sobre la mesa este panorama y tomando ventaja de la experiencia y el conocimiento adquirido en los más de cuatro años de trabajo apoyando al Ministerio de Justicia y del Derecho en su labor de inspección, control y vigilancia de los operadores de los Métodos Alternativos de Solución de Conflictos – MASC en Colombia, mediante el desarrollo del Sistema de Información de la Conciliación, el Arbitraje y la Amigable Composición - SICAAC, el grupo Sistemas y Tecnologías de la Información (STI), durante el año 2018 y parte del 2019, ha venido ejecutando un proyecto de investigación tendiente a proponer una estrategia para la incorporación de sistemas ODR en los procesos de conciliación extrajudicial en derecho en Colombia, mediante la cual, se busca definir el soporte tecnológico y de gestión de la información necesario para la formulación de una política pública nacional de conciliación virtual.

Es una realidad que la información se ha convertido en el más valioso de los activos para las organizaciones de hoy en día, por ello, la preocupación por la seguridad de la información en los sistemas ODR ha generado un sinnúmero de inquietudes entre gobiernos, operadores de justicia y usuarios en general, toda vez que la información manejada proviene de conflictos de intereses de diferente naturaleza.

En este artículo se presenta una revisión de la literatura realizada en el marco del proyecto de investigación mencionado, utilizando la metodología de Tranfield (Tranfield, Denyer & Smart, 2003), donde se presenta una serie de amenazas a la seguridad de la información en sistemas ODR que han sido identificadas y reportadas en la literatura y los controles propuestos por diferentes autores para mitigar posibles riesgos, y se analiza su aplicabilidad al contexto colombiano.

2. El mecanismo de conciliación en Colombia

En Colombia, los ciudadanos cuentan con tres Mecanismos Alternativos de Solución de Conflictos (MASC), la conciliación, el arbitraje y la amigable composición, para resolver amigablemente sus conflictos evitando llegar a los estrados judiciales. Según la corte constitucional, los MASC buscan hacer efectivo uno de los fines constitucionales como el de la convivencia pacífica, permiten la participación directa de los interesados en la resolución de sus conflictos, son otra forma de hacer efectivo el derecho de acceso a la administración de justicia y su uso aporta a la descongestión judicial (Corte Constitucional de Colombia, 2013).

Por su parte, la conciliación es un mecanismo a través del cual, dos o más personas gestionan por sí mismas la solución de sus diferencias, con la ayuda de un tercero neutral y calificado denominado conciliador (Ministerio de Justicia, 2014); ésta se clasifica como judicial si se realiza dentro de un proceso judicial y extrajudicial en derecho si se realiza antes o por fuera de un proceso judicial y, a través de conciliadores de centros de conciliación o ante autoridades en cumplimiento de funciones conciliatorias (Congreso de la república de Colombia, Ley 640 de 2001).

3. Resolución de Disputas en línea (ODR)

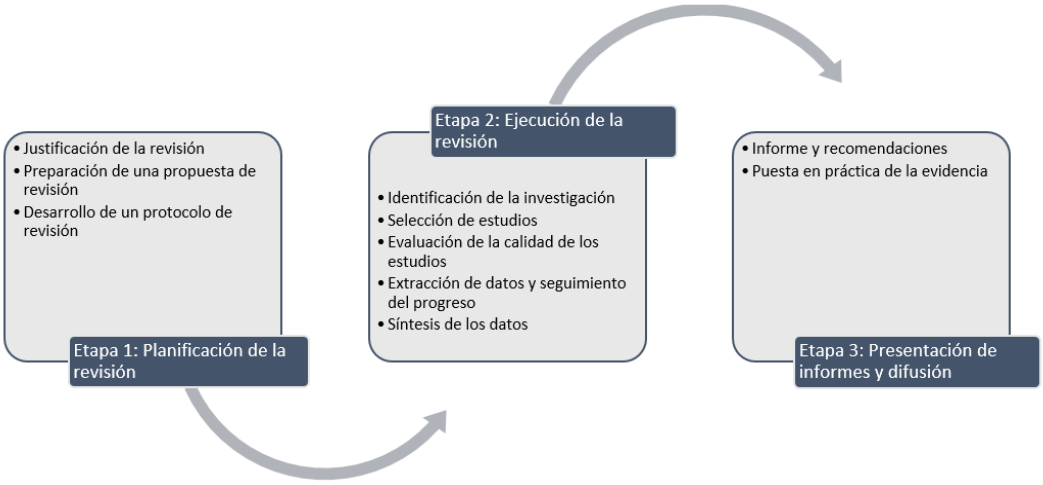
El concepto de Resolución de Disputas en Línea, más conocido en inglés como Online Dispute Resolution (ODR), fue propuesto por Ethan Katsh (Katsh, 2012) para referirse al uso del Internet para resolver disputas (Katsh & Rule, 2016). Aunque inicialmente se concibió para la solución de disputas derivadas de las transacciones comerciales en el ciberespacio, hoy en día el concepto ha tomado grandes proporciones y es ampliamente usado en otras áreas, por ejemplo, en los procesos de mediación y arbitraje para dar solución a conflictos que se generan en el mundo real. En Israel, por ejemplo, se adoptó un sistema ODR para las reclamaciones por daños a propiedades en la industria de seguros, en Estados Unidos para abordar las disputas de la Ley de Libertad de Información (FOIA) con un sistema (Rabinovich & Katsh, 2012), en Australia, el estado de Victoria ha implementado sistemas ODR parciales los cuales asisten a los participantes para resolver los conflictos del vecindario y para la protección de los derechos del consumidor (Sourdin, Tania & Liyanage, 2012). Así mismo, varios países han empezado a adoptar ODR como una extensión de los Mecanismos de Solución de Conflictos –MASC (ADR, por sus siglas en inglés). Autores como Katsh y Rifkin describen ODR como los MASC que se llevan a cabo vía internet, como una herramienta de resolución de disputas que se generan tanto en el ciberespacio (online) como en el mundo real (offline) (Katsh & Rifkin, 2001). Esto mismo es llamado por Katsh como “The Fourth Party”, que podría traducirse como “La Cuarta Parte” haciendo alusión a un cuarto rol en el proceso de solución de conflictos en el que usualmente participan tres roles, las dos partes involucradas en el conflicto y un tercero neutral que ayuda a explorar posibilidades de acuerdo entre las partes, en este caso “La Cuarta Parte” hace referencia a la inclusión de las TIC en el proceso de solución de conflictos.

4. Metodología

La metodología de revisión sistemática de la literatura fue originalmente desarrollada en medicina y ciencias de la salud, de donde evolucionó hacia las ciencias sociales (Velásquez, 2014); tiempo después fue adaptada por Kitchenham para su uso en la ingeniería del software (Kitchenham & Charters, 2007), por Tranfield en el campo de la gestión (Corte Constitucional de Colombia, Sentencia C – 222 de 2013) y por Sorrell en el análisis de políticas energéticas (Sorrell, 2007). Así pues, siendo el eje central de este trabajo la gestión de la seguridad de la información, se consideró que la metodología adecuada para este, es la metodología propuesta de Tranfield, la

cual, maneja un enfoque basado en la evidencia y, una vez finalizado el proceso, proporciona una base confiable de conocimiento para formular decisiones y tomar medidas en una organización (Tranfield, Denyer & Smart, 2003). En la figura 1 se muestra una representación gráfica de la metodología de Tranfield, la cual, consta de diez fases distribuidas en 3 etapas.

Figura 1
Metodología de Tranfield



Fuente: Adaptación de la metodología de Tranfield descrita en (Tranfield, Denyer & Smart, 2003).

5. Resultados

5.1. Etapa 1: Planificación de la revisión

Justificación de la revisión: Se realizó una búsqueda de revisiones de literatura relevantes a la gestión de seguridad de la información en sistemas ODR en la base de datos bibliográfica Scopus; la ecuación de búsqueda utilizada fue TITLE-ABS-KEY((("security" OR "risk" OR "privacy" OR "threat" OR "data protection") AND ("online dispute resolution")) AND "review"). El número de documentos que arrojó esta búsqueda fue cero. Por esta razón, para el desarrollo de esta investigación, se hace necesario la realización de una revisión sistemática de la literatura relevante a esta temática.

Propuesta de revisión: Para la formulación de la pregunta de investigación que se pretende responder tras el desarrollo de esta revisión sistemática, se utilizó la estrategia PICO[1] (Santos, Pimenta, et al, 2007), la cual, permite construir adecuadamente preguntas de investigación en diferentes ámbitos, maximizando la recuperación de evidencias en las bases de datos, enfocando el propósito de la investigación y evitando realizar búsquedas innecesarias. En la tabla 1 se presenta la descripción de la estrategia PICO.

[1] Acrónimo de: Problem, Intervention, Comparison, Outcome.

Tabla 1
Descripción de la estrategia PICO

Acrónimo	Definición	Descripción
P	Problem	Individuo o población problema
I	Intervention	Interés de la intervención
C	Comparison	Estándar para la intervención
O	Outcome	Resultados esperados

Fuente: Adaptado de (Santos, Pimenta, et al, 2007)

En la tabla 2, se presenta la descripción de los componentes PICO aplicados a esta revisión. El componente "C", Comparison, no fue tenido en cuenta dado que no se quiere limitar esta revisión a un determinado estándar de intervención.

Tabla 2
Descripción de los componentes PICO

Acrónimo	Descripción
P	Sistemas ODR
I	Seguridad de la información
C	N/A
O	Riesgos

Fuente: Autor

Con base en lo definido en la tabla 2, se propone la siguiente pregunta de investigación:

¿Qué riesgos de seguridad de la información asociados al uso de sistemas ODR han sido reportados en la

literatura científica?

Protocolo de revisión

Criterios de inclusión (Tipos de publicación).

- Artículos
- Ponencias
- Capítulos de libro

Criterios de Exclusión

- No relevancia para el objetivo de esta revisión
- Publicaciones no accesibles a través de los recursos de la universidad.

Bases de datos utilizadas

- Scopus

Selección de estudios

- La selección de estudios se realizó con base en la pertinencia observada en primer lugar en el título y en segundo lugar en el resumen de cada publicación encontrada.

- Se recuperaron las publicaciones seleccionadas relevantes al contexto de las preguntas de investigación planteadas para esta revisión.

Valoración de la calidad

Ya que las publicaciones identificadas fueron obtenidas a través de una búsqueda en Scopus, se da por sentado que los estudios proceden de revistas con un nivel de calidad aceptable para este estudio.

5.2. Etapa 2: Ejecución de la revisión

Identificación de la investigación: En la tabla 3, se presenta la pregunta de investigación definida como objetivo de esta revisión, la ecuación de búsqueda utilizada, el número de publicaciones obtenidas como resultado de su ejecución y el número de publicaciones tenidas en cuenta.

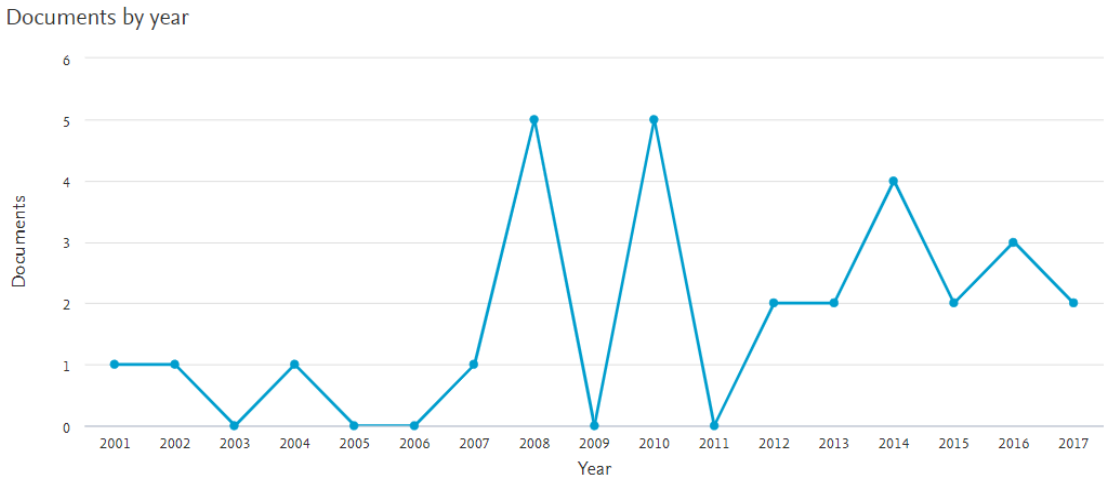
Tabla 3
Identificación de la investigación

Pregunta	Ecuación	Publicaciones encontradas
¿Qué riesgos de seguridad de la información asociados al uso de sistemas ODR han sido reportados en la literatura?	TITLE-ABS-KEY ((("security" OR "risk" OR "privacy" OR "threat" OR "dataprotection") AND (“online dispute resolution"))	29

Fuente: Autor

En la figura 2 se presenta la tendencia de publicaciones discriminada por años, producto de la ejecución de la ecuación de búsqueda definida.

Figura 2
Análisis bibliométrico para Online Dispute Resolution



Fuente: Scopus

Selección de estudios

Una vez revisados el título y el resumen de las publicaciones encontradas, fueron seleccionadas 10 publicaciones que se consideraron relevantes a esta revisión, ya que aportan elementos valiosos para la construcción de la respuesta a la pregunta de investigación planteada.

Evaluación de la calidad de los estudios

Como se dijo anteriormente, un primer filtro de calidad de las publicaciones seleccionadas es el hecho de que estas fueron obtenidas a través de una búsqueda realizada en la base de datos bibliográfica Scopus, lo cual, en principio, asegura cierto nivel de calidad. Adicionalmente, los investigadores, analizaron las publicaciones seleccionadas y, de común acuerdo, concluyeron que estas cumplen con niveles aceptables de calidad.

Extracción y síntesis de los datos

Una vez seleccionadas las publicaciones para tener en cuenta en esta revisión, se procedió a su respectivo estudio y extracción de datos de interés para responder la pregunta de investigación planteada. En la tabla 4 se presenta la matriz de extracción de datos empleada.

Tabla 4
Estudios seleccionados

Ref.	País del estudio	Riesgos de seguridad identificados	Controles de seguridad propuestos
(Loutocký, 2016)	República Checa	Las entidades operadoras de ODR se pueden sesgar en beneficio de una de las partes.	Control por parte del estado a los operadores de ODR.
(Santos, 2014)	España	Los sistemas ODR no salvaguardan la privacidad y seguridad de la información de acuerdo a las leyes de protección de datos de la Unión Europea.	Incorporar en los sistemas ODR mecanismos para tratar adecuadamente los datos personales de acuerdo con la regulación establecida en la Unión Europea.
(Martic, 2014)	España	Grabación de audiencia sin autorización.	Compromiso de acuerdo de confidencialidad entre ellas, con términos específicos y altas sanciones en caso de incumplimiento.
(Hörnle, 2013)	Inglaterra	Filtración de datos desde la base de datos central.	No compartir más datos de los estrictamente necesarios a efectos de aplicación. No almacenarlos datos más tiempo del necesario.
(Suquet-Capdevila, 2012)	España	Las comunicaciones de las partes, por ejemplo, mediante mensajes de texto o videoconferencia en tiempo real, pueden ser vigiladas, interceptadas, alteradas o incluso destruidas.	El procedimiento en línea debe cumplir los requisitos de seguridad relativos a la privacidad, la integridad y la autenticidad. Además, también se requiere no repudio. Sistemas de claves públicas y privadas para las tecnologías de cifrado, firmas digitales y funciones hash. Los cortafuegos pueden ser útiles para impedir el acceso a los datos almacenados.

Ref.	País del estudio	Riesgos de seguridad identificados	Controles de seguridad propuestos
(Suquet-Capdevila, 2012)	España	Suplantación de identidad.	Firmas electrónicas avanzadas basadas en certificados reconocidos. Utilización de sistemas de autenticación comúnmente utilizados en otros ámbitos, como los basados en nombres de usuario y contraseñas.
(Carneiro et al, 2011)	Portugal	Violación de la privacidad.	Uso de Login y Password. Establecer sesiones seguras con el usuario.
(De Laat, 2001)	Países bajos	Intercepción y alteración de mensajes durante la comunicación.	Sistemas de criptografía de clave pública y privada.
		Suplantación de identidad.	Firma digital.
		Repudio de mensajes	Marca de agua electrónica. Sello de tiempo (hora y fecha en que se transmitió la información).

Fuente: Autor

6. Seguridad de la información en medios electrónicos para la generación y procesamiento de información con validez jurídica en Colombia.

6.1. Ley 527 de 1999

Sin duda, uno de los grandes avances en Colombia en materia del uso de medios electrónicos en el ámbito jurídico, ha sido la expedición de la ley 527 de 1999, por medio de la cual, se define, reglamenta y otorga efectos jurídicos a la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares y, se incorporan elementos y principios de acción adoptados en materia internacional por parte de la UNCITRAL, en lo que respecta al comercio electrónico y las formas de originar, transmitir y otorgarle efectos legales a la transferencia de todo tipo de datos a través de la red (Ministerio de Justicia & Banco mundial, 2011). En la tabla 5 se presenta una serie de definiciones conceptuales para facilitar la comprensión de lo estipulado en la ley 527 de 1999.

Es de resaltar que el ámbito de aplicación de la ley 527 de 1999 abarca todo tipo de información en forma de mensaje de datos, excepto en dos circunstancias:

1. Cuando se trate de obligaciones contraídas por el estado colombiano en virtud de convenios o tratados internacionales.
2. Cuando se trate de advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo.

Tabla 5
Definiciones conceptuales de la Ley 527 de 1999

Mensaje de datos	La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax.
Comercio electrónico	Abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las siguientes operaciones: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; todo tipo de operaciones financieras, bursátiles y de seguros; de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera.
Firma digital	Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.
Entidad de Certificación	Es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.
Intercambio Electrónico de Datos (EDI)	La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto.
Sistema de Información	Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

Fuente: Ley 527 de 1999

Requisitos para la validez jurídica de un mensaje de datos

El artículo 5 de la ley 527 de 1999 establece que no se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos si estos cumplen con tres requisitos fundamentales, descritos en la tabla 6.

Tabla 6
Requisitos para la validez jurídica de un mensaje de datos

Originalidad	Se deben implementar herramientas que garanticen que la información contenida en el mensaje de datos ha conservado su integridad, es decir, ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación, desde el momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma.
Disponibilidad	La información contenida en un mensaje de datos debe ser accesible para su posterior consulta.
Frima	Es necesario utilizar un método apropiado para el propósito por el cual el mensaje de datos fue generado o comunicado, que permita identificar al emisor de un mensaje de datos y determinar que el contenido cuenta con su aprobación.

Fuente: Ley 527 de 1999

Comunicación de los mensajes de datos

La ley 527 de 1999, también establece algunas directrices a tener en cuenta para la comunicación de mensajes de datos con validez jurídica. En la tabla 7 se presentan las directrices dadas al respecto.

Tabla 7

Comunicación de los mensajes de datos

Formación y validez de contratos	En la formación del contrato, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos.
Reconocimiento de los mensajes de datos por las partes.	En las relaciones entre el iniciador y el destinatario de un mensaje de datos, no se negarán efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración por la sola razón de haberse hecho en forma de mensaje de datos.
Atribución de un mensaje de datos	Se entenderá que un mensaje de datos proviene del iniciador, cuando éste ha sido enviado por el propio iniciador, por alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje o por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.
Acuse de recibo	Si al enviar o antes de enviar un mensaje de datos, el iniciador solicita o acuerda con el destinatario que se acuse recibo del mensaje de datos, pero no se ha acordado entre éstos una forma o método determinado para efectuarlo, se podrá acusar recibo mediante toda comunicación del destinatario, automatizada o no, o todo acto del destinatario que baste para indicar al iniciador que se ha recibido el mensaje de datos.
Fecha de envío	De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido cuando ingrese en un sistema de información que no esté bajo control del iniciador o de la persona que envió el mensaje de datos en nombre de éste.
Fecha de recepción	De no convenir otra cosa el iniciador y el destinatario, la fecha de la recepción de un mensaje de datos se determinará de la siguiente forma, 1) si el destinatario ha designado un sistema de información para la recepción de mensaje de datos, la recepción tendrá lugar en el momento en que ingrese el mensaje de datos en el sistema de información designado o de enviarse el mensaje de datos a un sistema de información del destinatario que no sea el sistema de información designado, en el momento en que el destinatario recupere el mensaje de datos; y 2) Si el destinatario no ha designado un sistema de información, la recepción tendrá lugar cuando el mensaje de datos ingrese a un sistema de información del destinatario.

Fuente: Ley 527 de 1999

6.2. Ley 1581 de 2012

Más conocida como la ley de protección de datos, tiene como objetivo desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar la información que se hayan recogido sobre ellas en bases de datos o archivos por parte de terceros.

El ámbito de aplicación de la ley 1581 de 2012 son todos aquellos datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada, salvo algunas excepciones.

La ley 1581 de 2012 establece un tipo particular de datos personales, denominados datos sensibles, entendidos como los datos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de

cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos. El tratamiento de este tipo de datos sin la autorización explícita del titular está prohibido por la ley 1581 de 2012, salvo algunas excepciones. En caso de tratarse de datos personales de niños, niñas y adolescentes, solo se podrán tratar aquellos datos de naturaleza pública.

En la figura 5 se muestran los 8 principios rectores para el tratamiento de datos personales establecidos en la ley 1581 de 2012.

Tabla 8

Principios rectores para el tratamiento de datos

Principio de legalidad en materia de tratamiento de datos	El tratamiento de datos personales es una actividad reglada que debe sujetarse a lo establecido en la ley y en las demás disposiciones que la desarrollen.
Principio de finalidad	El tratamiento de datos personales debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley, la cual debe ser informada al titular.
Principio de libertad	El tratamiento de datos personales solo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.
Principio de veracidad o calidad	La información personal sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible, en este sentido, se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
Principio de transparencia	En el tratamiento de datos personales debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.
Principio de acceso y circulación restringida	El tratamiento de datos personales está sujeto a los límites que se derivan de la naturaleza de los mismos, de las disposiciones de ley y la Constitución. En este sentido, su tratamiento solo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en leyLos datos personales, salvo la información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la presente ley.
Principio de seguridad	La información personal sujeta a tratamiento por el Responsable del tratamiento o encargado del tratamiento a que se refiere la ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
Principio de confidencialidad	Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la misma.

Fuente: Ley 1581 de 2012

7. Análisis y discusión

Sin duda el mundo está evolucionando hacia una era cada vez más digital. La historia reciente nos muestra que, muchos procesos que años atrás se realizaban de forma manual han ido migrando hacia las TIC. En el caso puntual de la justicia, y particularmente de la solución de conflictos, este fenómeno se ha dado gracias al desarrollo de sistemas ODR, campo relativamente joven, revolucionario y que vive una constante evolución y adaptación.

Si bien es cierto que en Colombia se han hecho grandes avances para integrar las TIC a múltiples escenarios socioeconómicos y de gobierno, es claro que uno de los mayores obstáculos para la implementación de sistemas ODR en el proceso de conciliación extrajudicial es la ausencia de leyes claras y progresistas que respondan a las necesidades modernas de la sociedad, que incluyan las TIC como elemento fundamental en cada uno de los procesos y, la falta de inversión estratégica en diferentes sectores que permita la eliminación de brechas digitales en los sectores más vulnerables de la población, haciendo posible que todas las personas, sin importar su condición social y/o su ubicación geográfica, pueda acceder a una herramienta tan esencial como lo es hoy en día el internet.

Como se esperaba al inicio de esta revisión, ODR por tratarse de un área relativamente nueva, el tema de la gestión de la seguridad de la información aplicada a esta ha sido poco explorado, lo que se traduce en un número no muy alto de material bibliográfico disponible en la literatura científica, sin embargo, este da cuenta de algunos sistemas ODR diseñados específicamente para responder a las necesidades de un país, y en ellos se han implementado una serie de controles de seguridad que, aunque pueden servir como guía inicial, podrían no ser tan viables en el contexto colombiano para garantizar la seguridad de la información en un sistema ODR orientado a la conciliación extrajudicial, ya que mecanismos usados internacionalmente como la firma digital podrían limitar el acceso a personas de escasos recursos y/o habitantes de zonas rurales.

Esta realidad no puede ser ignorada en un proceso de planificación de un sistema de impacto nacional como el planteado en el presente trabajo, puesto que de este proceso depende que Colombia pueda sacar el máximo provecho de un sistema nacional de solución de disputas en línea (ODR) adaptado a la conciliación extrajudicial, el cual, podría tener un impacto positivo especialmente las zonas rurales, las cuales corresponde al 99.6% del territorio nacional (Instituto geográfico Agustín Codazzi, 2014) y donde por cuestiones geográficas a diario se presentan múltiples dificultades para trasladarse a los cascos urbanos.

Finalmente, pensar en un cambio de paradigma social no es tarea fácil; de todo lo anteriormente expuesto surgen muchas interrogantes sobre cómo gestionar un sistema ODR en un país como Colombia, incluyendo la gestión de la seguridad de la información. No es viable implementar los controles de seguridad propuestos por otros trabajos a nivel mundial en el contexto colombiano, entonces ¿cómo firmar documentos generados a través de medios electrónicos?, ¿cómo asegurar que quien está del otro lado de la pantalla es quien dice ser?, ¿cómo garantizar la privacidad y confidencialidad en una audiencia?, estos y muchos otros son los retos a los que debemos enfrentarnos para hacer de la justicia un elemento más incluyente apoyado en el uso de las TIC

8. Conclusiones

Dado que el campo de la resolución de disputas en línea es relativamente nuevo, no está disponible en la literatura científica un número significativo de estudios (en comparación con otros campos con más trayectoria) que permita establecer un precedente para tomar decisiones en lo concerniente al manejo de la seguridad de la información de este tipo de sistemas en un país como Colombia, esto abre todo un abanico de oportunidades

para la realización de trabajos de investigación en esta área y la aparición de nuevas líneas de investigación relacionadas a esta temática en el país.

Si bien es cierto que se han dado grandes avances en materia de integración de las TIC a los procesos establecidos por la ley en Colombia, para el caso de la conciliación extrajudicial quedan vacíos y ambigüedades en la forma como se debe disponer de los medios electrónicos para la gestión de la información en este proceso.

La implementación de un sistema ODR en el proceso de conciliación extrajudicial en Colombia podría tener un impacto positivo de grandes magnitudes en materia de acceso a la justicia, principalmente en las zonas rurales (las cuales corresponden al 99.6% de la extensión del país) donde se presenta la mayor cantidad de dificultades para acceder a esta por las dificultades que se presentan para el desplazamiento a cascos urbanos.

Dadas las particularidades que se presentan para la implementación de un sistema ODR en el proceso de conciliación extrajudicial en Colombia (principalmente dificultades a causa de las brechas digitales), se hace necesario la realización de un trabajo de investigación que permita establecer un plan para la gestión de la seguridad de la información que permita asegurar el sistema sin hacerlo de difícil acceso en un contexto tan particular como Colombia.

Referencias bibliográficas

Ministerio de Justicia y del Derecho. Programa Nacional de Conciliación. Conciliación Virtual. Bogotá D.C. [En Línea]. Disponible en: http://conciliacion.gov.co/portal/-Conciliaci%C3%B3n/Conciliaci%C3%B3nVirtual/Definici%C3%B3n

Ministerio de Justicia y del Derecho – Banco mundial, Consorcio Bureau Veritas Colombia Ltda. – Aselink S.A.S. (2011). Diagnóstico de la conciliación Virtual. [En Línea]. Disponible en: https://conciliacion.gov.co/portal/LinkClick.aspx?fileticket=mffRB3kkvWg%3d&portalid

Ethan Katsh & Colin Rule (2016), “What We Know and Need to Know About Online Dispute Resolution,” 67 S.C. L. REV. 329

Orna Rabinovich-Einy & Ethan Katsh (2014), “Digital Justice: Reshaping Boundaries in an Online Dispute Resolution Environment”. International Journal of Online Dispute Resolution. Vol. 1, pp. 5 – 36.

D. Tranfield, D. Denyer and P. Smart. “Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review,” British Journal of Management, vol. 14, pp. 207-222, 2003

Sentencia C - 222/13. Corte Constitucional de la Republica de Colombia. Bogotá D.C., 17 de abril de 2013.

Ministerio de Justicia y del Derecho. ¿Qué es la Conciliación en Derecho? Bogotá D.C. [En Línea]. Disponible en: http://www.minjusticia.gov.co/MASC/-Qu%C3%A9-es-Conciliaci%C3%B3n-en-Derecho

Ley 640 de 2001, artículo 30. Congreso de la Republica de Colombia, Bogotá D.C., 5 de enero de 2001.

Katsh, E. (2012).: ODR: A Look at History. Online Dispute Resolution: Theory and Practice: A Treatise on Technology and Dispute Resolution. pp. 21 – 33

Ethan Katsh & Colin Rule (2016), “What We Know and Need to Know About Online Dispute Resolution,” 67 S.C. L. REV. 329

Daniel Rainey (2014):, "Third - Party Ethics in the Age of the Fourth Party", International Journal of Online Dispute Resolution, 1, 37 - 56

RABINOVICH - EINY, Orna; KATSH, Ethan (2012). Lessons from online dispute resolution for Disputes Systems Design. In: WAHAB, Mohamed S. Abdel; KATSH, Ethan; RAINEY, Daniel (Ed.). Online dispute resolution: theory and practice. A treatise on technology and dispute resolution.

Sourdin, Tania and Liyanage, Kananke Chinthaka (2012), The Promise and Reality of Online Dispute Resolution in Australia

Katsh, M. and Rifkin, J. (2001). Online dispute resolution. San Francisco: Jossey – Bass

Juan D. Velásquez. (2014). Tips for Avoiding Ethical Problems in Scientific Publication. DYNA, 81(187), p.11. [En Línea]. Disponible en: https://doi.org/10.15446/dyna.v81n187.46102.

Kitchenham, B.A. and Charters, S., Guidelines for performing systematic literature reviews in software engineering. Technical Report EBSE-2007-01, 2007.

Sorrell, S., Improving the evidence base for energy policy: The role of systematic reviews, Energy Policy, 35 (3), pp. 1858-1871, 2007.

Santos, Cristina Mamédio da Costa; Pimenta, Cibele Andrucioli de Mattos and Nobre, Moacyr Roberto Cuce. Estrategia PICO para la construcción de la pregunta de investigación y la búsqueda de evidencias. Rev. Latino-Am. Enfermagem [online]. 2007, vol.15, n.3, pp.508-511. ISSN 1518-8345

Loutocký, P. (2016). Online dispute resolution to resolve consumer disputes from the perspective of European union law: Is the potential of ODR fully used? Masaryk University Journal of Law and Technology, 10(1), 113–127.

Santos, C. (2014). Increasing media richness in Online Dispute Resolution and the need for personal data protection. In CEUR Workshop Proceedings (Vol. 1105).

Martic, D. (2014). Blind arbitration: Proposal for anonymous crowdsourced online arbitration. In CEUR Workshop Proceedings (Vol. 1148, pp. 94–106). CEUR-WS.

Hörnle, J. (2013). Encouraging online alternative dispute resolution in the EU and beyond. European Law Review, 38(2), 187–208.

Suquet-Capdevila, J. (2012). Exploring online consumer mediation in Catalonia: Principles and technological uses. International Journal of Law and Information Technology, 20(2), 124–146.

Carneiro, Davide & Gomes, Marco & Novais, Paulo & Neves, Jose. (2011). Lecture Notes in Computer Science. 44-58.

De Laat, P. B. (2001). Emerging roles for third parties in cyberspace. Ethics and Information Technology, 3(4), 267–276.

Instituto geográfico Agustín Codazzi. Bogotá D.C. [En Línea]. Disponible en: https://noticias.igac.gov.co/es/contenido/tan-solo-el-03-por-ciento-de-todo-el-territorio-colombiano-corresponde-areas-urbanas-igac