



Revista IUS

ISSN: 1870-2147

Instituto de Ciencias Jurídicas de Puebla, Departamento de Investigaciones

Cotino Hueso, Lorenzo

Confidencialidad y protección de datos en la mediación en la Unión Europea*

Revista IUS, vol. 12, núm. 41, 2018, Enero-Junio, pp. 311-341

Instituto de Ciencias Jurídicas de Puebla, Departamento de Investigaciones

Disponible en: <https://www.redalyc.org/articulo.oa?id=293258387017>

- ▶ Cómo citar el artículo
- ▶ Número completo
- ▶ Más información del artículo
- ▶ Página de la revista en redalyc.org

LUZEM redalyc.org

Sistema de Información Científica Redalyc

Red de Revistas Científicas de América Latina y el Caribe, España y Portugal
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

Confidencialidad y protección de datos* en la mediación en la Unión Europea*

Confidentiality and Data Protection in Mediation in the European Union

Lorenzo Cotino Hueso**

RESUMEN

La mediación, su confidencialidad y la protección de datos son muy importantes en el siglo XXI y objeto autónomo de muchos estudios. No obstante, en raras ocasiones se analiza la conjunción de estos elementos y las muchas exigencias jurídicas que se derivan. Se efectúan propuestas de mejora en la normativa y en los marcos contractuales de la mediación. Primero, el estudio analiza la confidencialidad y su interacción con la protección de datos. Se analizan los sujetos obligados, el alcance de las obligaciones, su duración y garantías así como, finalmente las excepciones y restricciones a la confidencialidad. La segunda aproximación se hace desde la protección de datos, pues toda mediación implica un "tratamiento" de datos. Es por ello que se analizan y se hacen propuestas respecto de: la legitimación del tratamiento de datos; el responsable y encargado del tratamiento en la mediación; los derechos ARCO y la anonimización y las medidas de seguridad y el diseño de plataformas. Finalmente se analizan los requisitos para las transferencias internacionales de datos en la mediación.

PALABRAS CLAVE

Mediación, mecanismos de resolución de conflictos, privacidad, protección de datos, confidencialidad, Unión Europea.

ABSTRACT

Mediation, confidentiality and data protection are very important issues in the 21st Century and are the subject of many studies. However, in rare cases the combination of these elements and the many legal requirements that are derived are analyzed. Proposals are made for improvement in the regulations and in the contractual frameworks for mediation. First this study analyzes confidentiality and its interaction with data protection. The obligated subjects are analyzed, the scope of the obligations, their duration and guarantees as well, lastly, the exceptions and restrictions to the confidentiality. The second approach is done from data protection, since all mediation involves a "processing" of data. That is why we analyze and make proposals regarding: the legitimization of data processing; the persons in charge of the treatment in the mediation; ARCO rights (Access, Rectification, Cancellation and Opposition), anonymization, security measures and platform design. Finally, the requirements for international data transfers in mediation are analyzed.

KEYWORDS

Mediation, dispute resolution mechanisms, privacy, data protection, confidentiality, European Union

*Artículo recibido el 13 de junio de 2017 y aceptado el 3 de octubre de 2017. El presente estudio es producto de investigación en el marco de proyecto financiado por la Corporación Universitaria de Sabaneta - Unisabaneta-, línea de "Derecho Público", Grupo de Investigación "Estudios constitucionales, medio ambiente y territorio" (Colciencias COL0111291). Una versión muy abreviada y en inglés puede seguirse en "The confidentiality intrinsic to mediation and the demand for data protection", en Bujosa Vadell, Lorenzo M. (dir.) y Gallardo Rodríguez, Almudena (coord.), *Electronic mediation and e-mediator: proposal for the European Union*, Comares, Granada, 2017, pp. 105-110.

**Catedrático de Derecho Constitucional de la U. Valencia desde 2017, Prof. Titular desde 2002. (cotino@uv.es) orcid 0000-0003-2661-0010

SUMARIO

1. Planteamiento de objeto, metodología y objetivos
2. Una aproximación a la protección de datos y la mediación electrónica en la Unión Europea, su importancia y las dificultades que plantea su nexo
3. La confidencialidad propia de la mediación; su interacción y concurrencia con las exigencias de la protección de datos
4. Tratamiento de datos para la mediación y finalidades afines: legitimación, derechos y las figuras de encargado y responsable
5. Exigencias en el diseño de plataformas de mediación y la seguridad de la información confidencial
6. Los requisitos para admitir las transferencias internacionales
7. Conclusiones

1. Planteamiento de objeto, metodología y objetivos

El desarrollo futuro de la mediación —especialmente electrónica— es incuestionable y tiene que adaptarse plenamente a las exigencias de la protección de datos, cada vez más intensas. Al tiempo, la confidencialidad, que es propia a la mediación, se confunde en ocasiones con la protección de datos. No obstante, pese a la afinidad, se trata de regímenes jurídicos que se superponen y deben armonizarse. Estas cuestiones se han analizado escasamente hasta la fecha, aunque son esenciales para el futuro de la mediación. Por ello, constituyen el objeto de este trabajo.

El presente estudio se aborda desde la metodología que es propia al ámbito jurídico. El mismo se centra en el derecho de la Unión Europea, el cual regula tanto la mediación como la protección de datos. Sólo en algunas ocasiones puntuales se hace referencia al derecho español, básicamente como muestra de la concreción nacional del derecho europeo, pero no para abordar cuestiones internas. El análisis puede ser de utilidad y referencia comparativas, dado que los problemas que se abordan también se dan más allá de la Unión Europea.

La mediación es un mecanismo de resolución de conflictos en clara expansión en el siglo XXI. Mientras, la protección de datos es un derecho fundamental también emergente y expansivo. El régimen jurídico de la protección de datos se superpone, y condiciona más ámbitos, cada día. En clave de protección de datos, la mediación, en todas sus variantes, implica necesariamente un “tratamiento” de datos.

Sobre estas bases, buena parte del estudio proyecta el régimen europeo de protección de datos en la mediación, teniendo en cuenta la naturaleza, finalidades y elementos propios de la misma y los ámbitos más problemáticos que pueden presentarse. Pese a la abundante literatura sobre la mediación y sobre la protección de datos, son escasos los estudios realizados sobre este nexo. La determinación de los elementos clave de este cruce bien justifican el trabajo.

Ahora bien, el trabajo parte de la confidencialidad como uno de los principios rectores de la mediación. Esta confidencialidad suele confundirse con las exigencias de protección de datos. Ello exige detenerse en el régimen de la confidencialidad y su superposición y armonización con las exigencias de la protección de datos.

Este enfoque prácticamente no ha sido abordado por la literatura jurídica en español y evidencia la posible utilidad de este estudio. Por ello, los objetivos del presente son:

- Apuntar los elementos básicos del nexo protección de datos y mediación a la luz del derecho europeo.
- Observar en particular el régimen de la confidencialidad propia a la mediación y su interacción, convergencias y divergencias con la protección de datos.
- Señalar el marco de responsabilidades de los sujetos de la mediación como encargados en materia de protección de datos.
- Delimitar las singulares exigencias de seguridad de la información de la mediación y su concurrencia con las exigencias de seguridad de la normativa de protección de datos.
- En particular, y en relación con lo anterior, se tienen en cuenta los especiales riesgos, la naturaleza sensible de la información de la mediación y su especial confidencialidad. De ello, se derivan diversas especialidades y particulares obligaciones por la normativa de seguridad de protección de datos en la mediación.
- Dada la transnacionalidad creciente de la mediación y la actuación de sus sujetos, se fija especial atención en las exigencias de las transferencias internacionales de datos en la mediación.

La descripción casi inédita de estas cuestiones se acompaña a lo largo del estudio con diversas propuestas o elementos básicos de mejora. En este punto, se tienen en cuenta hipotéticas regulaciones de la mediación así como elementos que bien podrían ser recogidos en los acuerdos y marco contractual de la mediación.

2. Una aproximación a la protección de datos y la mediación electrónica en la Unión Europea, su importancia y las dificultades que plantea su nexo

La protección de datos está firmemente reconocida en el derecho de la Unión Europea. Cabe recordar que, el 28 de enero de 1981, en el seno del Consejo de Europa, se firmó el Convenio 108, para la Protección de las Personas respecto al Tratamiento Automatizado de Datos de Carácter Personal. En éste, se fijaron los principales elementos del actual régimen jurídico del tratamiento de datos. A partir de entonces, los Estados europeos comenzaron a reconocer jurisprudencialmente este derecho —como lo haría el Tribunal Constitucional de Alemania, en 1984— y a aprobar sus leyes de protección de datos personales.

El Tribunal Europeo de Derechos Humanos (TEDH) en caso *Leander*, de 26 de marzo de 1987, incluyó este derecho fundamental en el ámbito protegido por el artículo 8 del Convenio Europeo de Derechos Humanos (CEDH). Éste garantiza el derecho de toda persona al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. A partir de entonces, otras sentencias TEDH han ido perfilando este derecho.

Ya en el marco de la Unión Europea, con el fin de evitar divergencias legislativas, se aprobó la Directiva 95/46/CE sobre Protección de Datos Personales o la Directiva 97/66/CE sobre Protección de Datos y Telecomunicaciones (actualmente, Directiva 2002/58/CE). En 1997, el derecho a la protección de datos pasó expresamente a los tratados constitutivos de la Unión Europea. Así, culminó con su reconocimiento autónomo en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea, jurídicamente vinculante desde la entrada en vigor del Tratado de Lisboa el 1 de diciembre de 2009.

El artículo 7 de la Carta reconoce asimismo el derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones. Previo al reconocimiento en la Carta, el Tribunal de Justicia de la Unión Europea (TJUE) vino a reconocer la protección de datos en el marco de la vida privada y familiar, precisamente en su primera sentencia de derechos fundamentales (STJCE de 12 de noviembre de 1969, caso *Stauder*). Con claridad, desde la STJCE de 20 de mayo de 2003, caso *Österreichischer Rundfunk*, el TJUE reconoció el derecho a la protección de datos como autónomo y de modo contundente.

El fundamento del derecho de protección de datos es la dignidad de la persona, el libre desarrollo de la personalidad, sin la cual se priva a la persona del disfrute de los demás derechos fundamentales. Todos los Estados europeos han considerado que el objeto del derecho a la protección de datos personales es garantizar al individuo el derecho a organizar y determinar por sí mismo

aspectos esenciales de su vida. Por ejemplo, a quién y en qué momento quiere comunicar cuestiones personales, pensamientos, sentimientos o emociones e incluso su identidad.

Tanto el Convenio 108 como las directivas se han sometido a un proceso de revisión desde 2010. El mismo ha concluido con un nuevo marco jurídico constituido esencialmente por el nuevo Reglamento de la Unión Europea 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016. Éste es 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, en adelante RGPD).¹

A nadie escapa que el creciente régimen de protección de datos impregna todos los ámbitos, como es, en nuestro caso, la mediación. Por cuanto la mediación se trata de un procedimiento estructurado, en cuya virtud “dos o más partes en un litigio intentan voluntariamente alcanzar por sí mismas un acuerdo sobre la resolución de su litigio con la ayuda de un mediador. Este procedimiento puede ser iniciado por las partes, sugerido u ordenado por un órgano jurisdiccional o prescrito por el derecho” (artículo 3 Directiva 2008/52/CE, del Parlamento Europeo y del Consejo, de 21 de mayo de 2008, sobre ciertos aspectos de la mediación en asuntos civiles, en adelante, Directiva 2008/52/CE).

En 2002, el Libro verde sobre modalidades alternativas de solución de conflictos en el ámbito del derecho civil y mercantil² (en adelante, Libro verde) afirmaba “las ventajas inherentes a estas modalidades de justicia privada y la crisis de eficacia de los sistemas judiciales suscitaron un interés renovado hacia estos métodos de apaciguamiento de los conflictos más consensuales que el recurso al juez o a un árbitro”.

Como afirma el autor, se trata de un mecanismo más amable y suave de solucionar conflictos.³ Asimismo, la Directiva 2008/52/CE ya apostaba por el uso de las tecnologías de la información y la comunicación (TIC) en la mediación: “la presente Directiva no debe impedir en modo alguno la utilización de las nuevas tecnologías de comunicaciones en los procedimientos de mediación” (considerando noveno).

¹ Sobre el nuevo reglamento europeo, véase PIÑAR MAÑAS, JOSÉ LUIS, *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*, Madrid, Reus, 2016; RALLO LOMBARTE, ARTEMI Y GARCÍA MAHAMUT, ROSARIO (coords.), *Hacia un nuevo derecho europeo de protección de datos*, Valencia, Tirant lo Blanch, 2015.

² Presentado por la Comisión, COM (2002) 196 final, Bruselas, 19 de abril, 2002.

³ RAMÓN FERNÁNDEZ, FRANCISCA, “La mediación electrónica, la confidencialidad y la protección de datos de carácter personal”, *Revista InDret*, núm. 3, p. 4.

El avance del uso de las TIC en la resolución no judicial de disputas, y en particular la mediación electrónica o mediación mediante medios electrónicos, resulta imparable en los últimos tiempos. Incluso se apuesta por la inteligencia artificial.⁴ La mediación electrónica aúna ventajas propias de la mediación con las de las TIC: inmediatez, facilidad de contacto, sincronía o asincronía, deslocalización, mejores especialistas, mayor tiempo posible de contacto con mediador, reducción de costes, entre otras.

La creciente importancia de la mediación, en conjunción con el carácter expansivo de la protección de datos, obliga a un análisis del nexo que existe entre una y otra. Ahora bien, se debe particular atención a un elemento básico de la mediación: la confidencialidad. No en vano, la misma concurre, se funde y confunde con exigencias de protección de datos.

3. La confidencialidad propia de la mediación; su interacción y concurrencia con las exigencias de la protección de datos

3.1. La confidencialidad difiere de la protección de datos

La confidencialidad es un principio fundamental de la mediación ya recogido en la Recomendación R (98) 1, 21 de enero de 1998 del Comité de Ministros del Consejo de Europa a los Estados miembro en mediación familiar. Se trata de “la condición *sine qua non* para el buen funcionamiento” (Libro verde, apartado 79),⁵ la cual exige el artículo 7 de la Directiva 2008/52/CE.

La finalidad esencial de la confidencialidad es la eficacia y éxito de la mediación. Se pretende evitar el temor o condicionamiento, porque las comunicaciones y la información generada en la mediación pudiera utilizarse luego en contra de una de las partes, en un procedimiento posterior de resolución de controversias.

Gracias a la confianza mutua que les da la confidencialidad, las partes tienen libertad de expresarse para alcanzar voluntariamente la solución que consideren oportuna. La finalidad de la confidencialidad determina su régimen jurídico, en cuanto al contenido, ámbito, sujetos, duración, garantías o consecuencias de su incumplimiento.

⁴ BUENO DE MATA, FEDERICO, “Mediación electrónica e inteligencia artificial”, *Actualidad civil*, núm. 1, 2015.

⁵ “La confidencialidad parece ser la condición *sine qua non* para el buen funcionamiento de las ADR, porque contribuye a garantizar la franqueza de las partes y la sinceridad de las comunicaciones durante el procedimiento.”

Esta confidencialidad, propia de la mediación, es paralela y semejante, pero diferente, a otros regímenes jurídicos de confidencialidad o protección de la información que pueden exigirse en razón de la normativa profesional o sectorial correspondiente y de secreto profesional.⁶ Se trata de regímenes jurídicos que pueden superponerse y concurrir, y que deben, en su caso, armonizarse.

En ocasiones, el alcance de la protección de la información es bien diferente según se dé un régimen u otro. Y es que, habitualmente, se confunde este régimen jurídico de confidencialidad o protección de la información. Sería recomendable que una hipotética normativa de mediación haga mención a la naturaleza y finalidad que son propias de la confidencialidad de la mediación, así como su posible concurrencia con otras exigencias normativas.

3.2. Contenido de la confidencialidad propia de la mediación

En cuanto al contenido, la confidencialidad propia de la mediación implica el derecho y obligación de que cualesquiera hechos o informaciones producidos en la mediación sean reservados y no se divulguen o revelen. Esta obligación alcanza a todo interviniente en la mediación.

Asimismo, las partes no deben requerir al mediador o a cualquier interviniente en la mediación para que intervenga como perito o testigo o para que facilite información en todo tipo de procedimiento o litigio que afecte en el objeto de la mediación. A este respecto, el Libro verde apunta que, cuando no ha tenido éxito la mediación,

el tercero que hubiere intervenido en ella no debería poder ser citado como testigo ni intervenir como árbitro [...] No obstante, la obligación de confidencialidad del tercero puede descartarse si las partes del procedimiento de ADR están de acuerdo para que se revelen algunas de estas informaciones protegidas, o en caso de que el propio tercero, sometido por su profesión al secreto profesional, se vea obligado a revelar parte de dichas informaciones en virtud de la legislación aplicable (apartado 82. Como ejemplo, se hace referencia a la normativa de blanqueo de dinero).

⁶ En esta dirección, y de modo bastante exhaustivo, cabe señalar el artículo 31 del Real Decreto 980/2013, de 13 de diciembre, por el que se desarrollan determinados aspectos de la Ley 5/2012, de 6 de julio, de mediación en asuntos civiles y mercantiles. En virtud de éste, el responsable o institución de mediación ha de "garantizar a las partes la seguridad, el buen funcionamiento de la plataforma y de los sistemas electrónicos utilizados, así como la privacidad, la integridad y el secreto de los documentos y las comunicaciones, la confidencialidad en todas las fases del procedimiento y asegurará el cumplimiento de las previsiones exigidas en la normativa en materia de protección de datos de carácter personal".

En esta dirección, por ejemplo, cabe mencionar la sentencia del Tribunal Supremo español: “las partes se comprometen a mantener el secreto y, por lo tanto, renuncian a proponer la persona mediadora como testigo en algún procedimiento que afecte al objeto de la mediación; también la persona mediadora debe renunciar a actuar como perito en los mismos casos”.⁷

También, pese a su derecho a no ser llamado, si el mediador es requerido, éste debe abstenerse y acogerse a su deber de silencio o secreto profesional. El artículo 7.1 de la Directiva 2008/52/CE sólo afirma en razón de la confidencialidad que “ni los mediadores ni las personas que participan en la administración del procedimiento de mediación estén obligados a declarar, en un proceso judicial civil o mercantil o en un arbitraje, sobre la información derivada de un procedimiento de mediación o relacionada con dicho proceso”.

Una hipotética normativa podría afirmar no sólo que no están obligados, sino que tampoco pueden participar voluntariamente en los procedimientos. Asimismo, merced a su estatuto de confidencialidad, el mediador no debe participar en un posterior proceso y revelar información, incluso en el caso de que las partes estuvieran de acuerdo en que lo haga. De igual modo, si se llegase a aportar información confidencial de una mediación en un procedimiento judicial o arbitral posterior, ésta no debe admitirse como prueba o elemento de juicio, salvo las excepciones previstas. En cuanto a la duración, la confidencialidad en la mediación va más allá del proceso mismo y se extiende ilimitadamente en el futuro.

3.3. *Los sujetos y el alcance de la confidencialidad propia a la mediación*

El deber de confidencialidad alcanza a las partes en la mediación y al mediador, pero también a otros intervinientes como abogados o profesionales, que asesoran a las partes. La Directiva 2008/52/CE habla de “personas que participan en la administración del procedimiento de mediación” (artículo 7.1) y el Libro verde deja claro que “La confidencialidad se impone tanto a las partes como a los terceros” (apartado 79). Incluso “Cuando una de las partes comunica información al tercero con motivo de conversaciones bilaterales [procedimiento designado bajo el nombre de *caucus*] (apartado 81).

La confidencialidad alcanza también a las entidades o instituciones públicas o privadas que gestionan la mediación y tienen acceso a información sobre la misma. De igual modo, la confidencialidad alcanza a quienes prestan servicios

⁷ STS, 1ª, 2.3.2011 (RJ 2011\2616; ponente, Antonio Salas Carceller).

instrumentales para ejecución de la mediación, a través de servicios que incluyan la tenencia, custodia o mera transmisión de la información. Así sucede especialmente con quienes prestan el servicio de plataforma electrónica de mediación.

La confidencialidad también alcanza a operadores de telecomunicaciones, plataformas virtuales, alojadores, servicios de la nube, entre otros. En estos casos, la confidencialidad coincide con las exigencias en materia de protección de datos y la normativa de privacidad y secreto de las comunicaciones.

En todos ellos recaen deberes de confidencialidad, seguridad de la información, etcétera, que ya se exigen tanto por normativa sectorial específica como por normativa de protección de datos o de privacidad en las comunicaciones. En clave de protección de datos, estos prestadores instrumentales de servicios para la mediación serán considerados encargados del tratamiento.

Si quienes han accedido a la información de la mediación lo hacen en el ejercicio de su profesión, este deber de confidencialidad forma parte del más amplio secreto profesional. La gama de sujetos a quienes alcanza la confidencialidad es muy amplia. Es por ello que, en todos los casos, resulta recomendable que los contratos o cláusulas de confidencialidad alcancen a todos los sujetos.

Respecto al ámbito, la información sometida a confidencialidad propia de la mediación es diferente a la protegida por el derecho a la protección de datos. La protección de datos protege toda información sobre una persona física identificada o identificable, pero no la relativa a una empresa o persona jurídica, mientras que la confidencialidad propia de la mediación no necesariamente ha de ser relativa a una persona física. Así pues, el ámbito de la confidencialidad propia de la mediación es mayor y no siempre quedará cubierto por la protección de datos.

La confidencialidad imprime este carácter reservado a toda información generada en el proceso mediador, sobre sus sesiones y resultados “sobre la información derivada de un procedimiento de mediación o relacionada con dicho proceso” (artículo 7.1 Directiva 2008/52/CE). La confidencialidad recae también sobre el proceso y su existencia misma, “incluida la mera existencia de la mediación en el presente o en el pasado” (Código de Conducta Europeo para mediadores, apartado 4).⁸

Según se ha adelantado, la confidencialidad alcanza tanto a las sesiones conjuntas de las partes, como a las entrevistas individuales con el mediador (*caucus* apartado 81 Libro verde). Es por ello que la información de estas

⁸ “El mediador respetará la confidencialidad sobre toda información, derivada de la mediación o relativa a la misma, incluida la mera existencia de la mediación en el presente o en el pasado”.

entrevistas individuales no se comunicarán a la otra parte, salvo autorización expresa. El carácter confidencial alcanza, pues, a todo hecho, información, documento, comunicación habida, ya sea verbal o en cualquier forma: entrevistas, expedientes, actas generadas, sean o no la sesión final.

Ahora bien, la confidencialidad no alcanza a aquella información o documentación de la mediación “que puede obtenerse de manera independiente”.⁹ Debe señalarse que hay alguna incertidumbre, al menos en España, sobre el alcance de la confidencialidad y la posibilidad de presentar como prueba —y que se admita— de acuerdos de mediación ante los tribunales. No en vano, el Tribunal Supremo español ha llegado a admitir como prueba —que había sido inadmitida por tribunales inferiores— acuerdos de las partes en mediación.

Se ha afirmado que la confidencialidad “no puede extenderse al caso presente en que se pretende traer a un proceso judicial lo que una de las partes considera que es un acuerdo libremente adoptado y referido a las consecuencias de la ruptura matrimonial”.¹⁰ Bajo el punto de vista de la protección de datos, un tratamiento de la información de la mediación con una finalidad diferente (ulteriores procesos o procedimientos judiciales o arbitrales) puede considerarse como un uso especialmente incompatible con el tratamiento de origen para la mediación. Obviamente, si es un juez quien adopta la decisión, ésta gozará de la singular base legítima para el tratamiento de datos.

Respecto de los resultados de la mediación, si ésta se ha malogrado, sólo se hará público que no ha habido éxito en la mediación, pero la confidencialidad alcanza también los motivos por los cuales no se ha llegado al acuerdo. Si la mediación concluye con acuerdo, la confidencialidad sólo alcanza cuando el resultado haya de ejecutarse, ratificarse u homologarse para su efectividad (artículo 7.1 b Directiva 2008/52/CE). Es decir, la publicidad alcanzará sólo lo necesario para aplicar y ejecutar los acuerdos alcanzados.

3.4. Conveniencia de regulación, acuerdo de mediación y otras garantías de la confidencialidad

La legislación ha de reflejar los sujetos, alcance y consecuencias del incumplimiento de la confidencialidad propia de la mediación. Al mismo tiempo, la

⁹ Así, por ejemplo, el “Acuerdo de mediación” de la Oficina de propiedad intelectual de la Unión Europea, Cláusula 6, Confidencialidad, apartado 3.

¹⁰ Se trataba de documentos redactados por el mediador durante el proceso de mediación familiar y firmados por las partes relativos a valor de la vivienda, la finalidad de alcanzar para la posible compra, por parte de la esposa, de la mitad pro indiviso del cónyuge. STS, 1ª, 2.3.2011 (RJ 2011\2616; ponente, Antonio Salas Carceller).

normativa debe aprovecharse para dotar de legitimación legal al tratamiento de datos que se produce. Debe dotarse de base legal al tratamiento de datos que supone la mediación, así como para dar también base legal a posibles afectaciones de derechos en juego.

Ahora bien, además de la legislación, la mediación es connatural a la expresión de la autonomía de la voluntad. Esta expresión se da a través de un acta de inicio o un acuerdo o contrato de mediación. El mismo es también muy recomendable para que exista una expresa asunción y conocimiento del régimen de la confidencialidad, por todas las partes e intervinientes. De este modo, las obligaciones normativas se refuerzan y se concretan en razón del consentimiento, al igual que se pueden reforzar diversas garantías concretas.

Desde el punto de vista del derecho de protección de datos, la existencia de un consentimiento y un contrato también juega un papel importante para legitimar tratamientos, cesiones o transferencias internacionales de datos tanto en el RGPD como en la Directiva 95/46/CE, así como para garantizar la información obligatoria (artículo 10 Directiva 95/46/CE). Por ello, el acuerdo de mediación debe aprovecharse para expresar el consentimiento y reforzar la legitimación del tratamiento de datos que supone la mediación.

Las organizaciones e instituciones tienen una especial responsabilidad respecto al marco contractual de la mediación y la confidencialidad en la elaboración de sus contratos tipo. Desde el inicio, también los mediadores deben asegurar que las partes conocen y comprenden el régimen de confidencialidad: la reserva o secreto que implica, la obligación de no citar como testigos o peritos ni solicitar la información confidencial para utilizarla en procedimiento alguno, así como que se facilite la información obligatoria en materia de protección de datos.

El mediador debe velar porque acepten este régimen y que conste la correspondiente aceptación. En esta dirección, Código de Conducta de los Mediadores Europeos, cuyo apartado 3.1, en el párrafo 2, establece: “El mediador en especial se asegurará de que antes del comienzo de la mediación las partes hayan comprendido y hayan acordado expresamente las condiciones del acuerdo de mediación, que incluye en especial las disposiciones relativas a la obligación de confidencialidad por parte del mediador y de las partes”.

También hay que velar porque profesionales y terceros intervinientes que asumen obligaciones estén al corriente de su régimen jurídico y, en su caso, dejen constancia de su conocimiento del deber de confidencialidad, tanto la propia de la mediación, como la exigible por protección de datos u otros motivos. También, sería aconsejable que la legislación precise con mayor claridad este elemento de garantía respecto del resto de intervinientes.

La confidencialidad es un deber cuyo incumplimiento puede generar diversas consecuencias penales, administrativas, laborales, entre otras. Asimismo, su incumplimiento puede generar daños y responsabilidad civil. Es dable exigir al mediador garantías frente eventuales daños por infracción de la confidencialidad y secreto. Tal responsabilidad debe extenderse, de igual modo, al cumplimiento de la normativa de protección de datos. En esta dirección cabe tener en cuenta la normativa nacional. La española afirma expresamente la responsabilidad por daños y la necesidad, incluso, de aseguramiento (artículo 14 de la Ley 5/2012¹¹ y artículos 26-29 Real Decreto 980/2013, reglamento de desarrollo).

Asimismo, cabe recordar que la responsabilidad de la institución de mediación alcanza la *culpa in eligendo*, en la selección del mediador. En este sentido, cabe recordar que dicha extensión de culpa se da en el ámbito administrativo sancionador respecto de la elección de encargado de protección de datos (artículo 20.2 Real Decreto 1720/2007, Reglamento LOPD).

3.5. Las excepciones a la confidencialidad propia de la mediación a la luz de las exigencias de la protección de datos

La confidencialidad propia a la mediación puede tener diversas excepciones. Las mismas, en principio, deben estar contempladas en la ley, así como integrarse en el marco contractual. Hay que armonizar las excepciones propias a la confidencialidad de la mediación y las exigencias de la protección de datos.

La obligación de no revelar información por el mediador o algún interviniente es “salvo acuerdo contrario de las partes” (artículo 7.1 Directiva 2008/52/CE). “Las partes pueden, por ejemplo, decidir de común acuerdo que la totalidad o parte del procedimiento no sea confidencial.” (Libro verde, apartado 80). Sin embargo, cabe concretar la regulación de esta excepción. De un lado, dado que la confidencialidad viene recogida en un contrato o acuerdo, es idóneo que se exija el consentimiento del uso de información para posteriores procedimientos, de modo expreso, por escrito, con formalidad y, en su caso, publicidad.

Desde el punto de vista corporativo profesional del mediador u otros profesionales intervinientes, puede no bastar el acuerdo de las partes para terminar

¹¹ “Artículo 14. Responsabilidad de los mediadores. La aceptación de la mediación obliga a los mediadores a cumplir fielmente el encargo, incurriendo, si no lo hicieren, en responsabilidad por los daños y perjuicios que causaren. El perjudicado tendrá acción directa contra el mediador y, en su caso, la institución de mediación que corresponda con independencia de las acciones de reembolso que asistan a ésta contra los mediadores. La responsabilidad de la institución de mediación derivará de la designación del mediador o del incumplimiento de las obligaciones que le incumben.”

con la confidencialidad, pues es posible que los mediadores deseen no ser habitualmente utilizados en conflictos. Desde la perspectiva de protección de datos, el solo consentimiento de las partes en poner fin a la confidencialidad no alcanzaría ni legitimaría el tratamiento o comunicación de datos relativos de terceros para otros usos.

No olvidemos que en la mediación no sólo se tratan datos de las partes mediadas, sino posiblemente de terceros. Ahora bien, en perspectiva de protección de datos, el uso de la información de la mediación para ulteriores procedimientos judiciales o arbitrales podría contar con una legitimación diferente a la del consentimiento.

La confidencialidad propia de la mediación se excluye por “razones imperiosas de orden público [...] la protección del interés superior del menor o la prevención de daños a la integridad física o psicológica de una persona” (artículo 7.1 a Directiva 2008/52/CE).¹² En acuerdos tipo de mediación, se hace referencia a “obligación legal imperiosa”.¹³ Se tratan supuestos difíciles de regular y cuya aplicación, por su propia naturaleza, hay que analizar en el caso concreto. Por ejemplo, la presencia de datos de relevancia para una investigación judicial o policial, o que supongan indicios de delito pueden prevalecer sobre el deber de confidencialidad de los mediadores.

La persecución de algunos delitos o ilícitos puede llegar a justificar la obligación de aportar la información confidencial. En estos supuestos serán las autoridades responsables, en especial, el juez o el fiscal, quienes requerirán que se aporte la información sobre la mediación. El requerimiento precisará ponderar la necesidad respecto de las finalidades concretas que se persiguen. Al ser difícil fijar los presupuestos, para una mejora normativa se puede precisar qué tipo de autoridad (administrativa, policial, fiscalía o judicial) es la que tiene la capacidad de exigir la quiebra de la confidencialidad. Cabe resaltar que aceptar como prueba o elemento de juicio la información de la mediación puede suponer una lesión del proceso debido. Por ello, también sería recomendable que la norma exprese que quien efectúe el requerimiento, haya ponderado la prevalencia de un interés superior.

¹² “Cuando sea necesario por razones imperiosas de orden público en el Estado miembro de que se trate, en particular cuando así lo requiera la protección del interés superior del menor o la prevención de daños a la integridad física o psicológica de una persona”.

¹³ “El mediador/los mediadores no divulgará(n) dicha información a nadie sin consentimiento, a menos que exista una obligación legal imperiosa de hacerlo.” “Acuerdo de mediación”, *Oficina de propiedad intelectual de la Unión Europea*. Disponible en: <https://goo.gl/WozeSS>

En clave de protección de datos hay supuestos, más allá del consentimiento, los cuales legitimarían la cesión de información de la mediación que contuviera datos personales. Ello queda regulado en el artículo 6.1 RGPD (hasta ahora, artículos 7 y 11 de la Directiva 95/46/CE).

Como se ha adelantado, el consentimiento de las partes de la mediación para excepcionar la confidencialidad puede no ser suficiente en clave de protección de datos porque se trata de datos de otras personas. En estos casos, la legitimación del tratamiento y cesión de datos de la mediación podrá darse por estas otras bases legítimas, más allá del consentimiento.

En general, si se da una excepción a la confidencialidad propia a la mediación por intereses superiores, esta excepción tendrá la cobertura de la normativa de la protección de datos. En este sentido cabe recordar que, en virtud del artículo 6.1 RGPD, es posible un tratamiento o comunicación de datos si es “necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento” (letra c).

También es legítimo el tratamiento o cesión de datos “para proteger intereses vitales del interesado o de otra persona física” (letra d). De igual modo, se pueden tratar o ceder datos “para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos” (letra e). Y la más polémica legitimación de tratamientos de datos es para la “satisfacción de intereses legítimos ponderados con intereses o derechos” (letra f).

Así, en clave de protección de datos, no sería problema revelar datos confidenciales de una mediación por un requerimiento judicial, de fiscalía, o similar. En estos supuestos la legitimación del tratamiento, fácilmente caería en las referidas letras d) o e) del artículo 6.1 RGPD. No obstante, para que sea posible la excepción a la confidencialidad, habrá de realizarse una ponderación superpuesta y más exigente que es la concurrencia de “intereses superiores”. Ésta exige la confidencialidad propia a la mediación.

4. Tratamiento de datos para la mediación y finalidades afines: legitimación, derechos y las figuras de encargado y responsable

4.1. La mediación supone un tratamiento de datos que debe contar con una base legítima

La mediación, en todas sus variantes, implica un tratamiento de datos de personas identificadas o identificables (artículo 4.2 RGPD; artículo 2 b Directiva 95/46/

CE).¹⁴ Así será siempre que, entre toda la información que se maneje en la mediación, se incluyan datos de personas físicas identificadas o identificables.

Aunque se trate de conflictos entre empresas u otras personas jurídicas, es inconcebible que no haya un tratamiento de datos personales de las partes, mediadores, intervinientes y terceros. Ello, además, quedará soportado en ficheros, de ahí que en la mediación concorra la normativa de protección de datos.

La información de cada procedimiento quedará integrada en un sistema de información o en un fichero más amplio. Los ficheros acogerán los distintos procedimientos de mediación en razón de diversos criterios, como la organización o institución que impulsa, gestiona y organiza la mediación, según materias y ámbitos sectoriales; según el sistema o plataforma de gestión de la mediación utilizado, entre otras clasificaciones. Según se estructure y organice la mediación también es natural pensar en la existencia de registros de mediadores, registros o plataformas de asuntos que integren a las partes e intervinientes en los procesos.

Todo tratamiento de datos, para ser legítimo, requiere del consentimiento o de un fundamento legítimo previsto en la ley (artículo 8 Carta Derechos Fundamentales). El consentimiento, acuerdo y contrato de las partes mediación juega un papel importante para legitimar tratamientos, cesiones o transferencias internacionales de datos (artículo 6 RGPD; artículos 7 a) y b), 26.1 a), b) y c) Directiva 95/46/CE). Asimismo, permite garantizar que se cumpla con la información obligatoria para el tratamiento de datos (artículo 12 RGPD; artículo 10 Directiva 95/46/CE).

Cabe recordar que el tratamiento de datos se legitima gracias al consentimiento para uno o varios fines específicos: *a)* si es necesario para la ejecución de un contrato; *b)* si el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable; *c)* para proteger intereses vitales; *d)* para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos; *e)* o para la satisfacción de intereses legítimos perseguidos; *f)* el derecho de la Unión Europea o de los Estados puede fijar determinadas legitimaciones para tratar datos (artículo 6; 2-4 RGPD).

En razón de los incisos *a)* o *b)*, el acuerdo de mediación puede ser una vía importante para la legitimación del tratamiento de datos. No obstante, no alcanzaría el tratamiento de datos de quienes no forman parte del acuerdo o

¹⁴ «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción».

contrato de mediación. Asimismo, la legitimación del tratamiento de datos que supone la mediación como un “interés legítimo” es un terreno inseguro. Por ello, la normativa de mediación debería expresar qué es base legal suficiente para legitimar los tratamientos de datos. En su caso, la normativa habría de expresar que la búsqueda de un acuerdo con un mediador para resolver un conflicto es un “interés legítimo” suficiente para justificar un tratamiento de datos (artículo 6.1 f, 2 y 3 RGPD; artículo 7 f Directiva 95/46/CE).

4.2. Las dificultades de uso de los datos de un procedimiento de mediación para nuevas o distintas finalidades a la inicial

Como dispone la Carta de derechos fundamentales en el artículo 8.1, los datos serán tratados de manera leal y lícita para fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines. Así pues, un uso diferente al de la finalidad que le es propia a la mediación requerirá de una nueva fuente de legitimación. Los usos diferentes a los propios de la mediación pueden quedar legitimados, por diferentes vías, en razón del artículo 6.1 RGPD: consentimiento, acuerdo de mediación, protección de intereses vitales, intereses o poderes públicos o intereses legítimos.

De igual modo, el derecho de los Estados o de la Unión Europea puede dar base normativa a diferentes finalidades y resulta especialmente importante evaluar la compatibilidad de los fines distintos con los fines iniciales, como indica el artículo 6.4. Cabe tener en cuenta algunos fines diversos a los propios de la mediación que pueden darse.

Especialmente cuando fracasa la mediación, es posible que se pretendan usar los datos tratados en la misma para lograr una solución arbitral o judicial, por ejemplo. Se trata de finalidades diferentes a la mediación y de nuevos tratamientos de datos. En razón de la necesaria confidencialidad propia a la mediación, estas finalidades son claramente incompatibles y se requeriría una nueva base legitimadora; hay que buscarla en el artículo 6 RGPD.

En este marco, las excepciones a la confidencialidad reguladas para la mediación, ya por consentimiento o intereses superiores, han de reconducirse como posibles bases de legitimación en clave de protección de datos. Y según lo expuesto el consentimiento o el contrato pueden ser insuficientes bases legitimadoras.

Asimismo, la normativa de protección de datos hace compatible los usos para fines históricos, estadísticos y de investigación con determinadas garantías, en especial el artículo 89 y los artículos 5.1 b y e; 9.2 j y 14.5 b del RGPD;

hasta ahora artículos 6.1 b, 10 y 13 de la Directiva 95/46/CE). El uso de la información de la mediación para la investigación o la estadística, en principio, será posible y se consideran usos compatibles con la finalidad de origen, sin perjuicio de que hayan de cumplirse determinadas exigencias.

La información de mediación puede resultar útil en la formación. Sin embargo, se trataría de una nueva finalidad que requiere de una legitimación específica. Una futura normativa de la mediación o, en su caso, el marco contractual de la mediación, podría contemplar también esta posible excepción de la confidencialidad y la protección de datos. No obstante, en razón de la confidencialidad propia de la mediación, cabría establecer garantías adicionales, como que, en lo posible, se lleve a cabo la anonimización de la información, en el sentido que luego se expone.

También es conflictiva la difusión de la mediación y de sus resultados, por ejemplo, a través de bases de datos de mediación o la publicidad activa sobre procedimientos de mediación. Estos usos ponen en peligro la confidencialidad propia de la mediación. Además, desde la perspectiva de la protección de datos, son finalidades que pueden considerarse incompatibles. Por ello, para que estos usos se admitan, deben estar expresamente contemplados por la normativa o expresamente consentidos por las partes. En su caso, la anonimización o disociación que se produzca para estos usos debiera ser intensa.

En ocasiones, la ejecución de un acuerdo de mediación exige la intervención de “un órgano jurisdiccional u otra autoridad competente, según el artículo 6.2 de la Directiva 2008/52/CE). En este caso, se tratará de un tratamiento de datos para una finalidad obviamente compatible con la inicial. Lo que variará será el responsable del tratamiento de datos; lo será dicho órgano o autoridad.

4.3. Las figuras de responsable y encargado de protección de datos en la mediación

Para la normativa de protección de datos, el responsable del tratamiento de datos es quien decide hacer el tratamiento y determina los fines; el encargado del tratamiento es un tercero externo que trata los datos por cuenta del responsable, por ejemplo, prestando un servicio al responsable. Quienes forman parte de la organización responsable tratan los datos bajo la autoridad del responsable; no son encargados.

La consideración de responsable y encargado en la mediación puede depender de la organización y configuración de cada sistema de mediación. Los responsables del tratamiento muy posiblemente externalizarán y contratarán

mediadores, empresas que implanten los sistemas de mediación por medios electrónicos; presten servicios de comunicaciones, servicios informáticos, de alojamiento, de nube; anonimicen los datos para posteriores tratamientos, entre otras funciones. Si los prestadores externos de estos servicios acceden a los datos personales o los tratan, serán encargados, a efectos de protección de datos.

Respecto del tratamiento de datos que se generan por la mediación en sí, lo natural es que haya unas instituciones de mediación (administraciones, institutos, fundaciones, asociaciones, colegios profesionales, cámaras de comercio, empresas, universidades) que impulsen la mediación, faciliten el acceso y administren la misma, incluyendo la designación de mediadores. Estas instituciones serán responsables del tratamiento de datos, y quienes los traten dentro la organización lo harán bajo autoridad del responsable, no como encargados.

Las instituciones de mediación contarán con una serie de intervinientes que, al prestar servicios, serán encargados, a efectos de protección de datos. Así sucederá con los mediadores mismos, como con las empresas que implanten los sistemas de mediación por medios electrónicos. Del mismo modo, sucederá con quienes accedan o traten datos para prestar servicios instrumentales como de comunicaciones, servicios informáticos, alojamiento, servicios en la nube, por mencionar algunos.

También la disociación o la anonimización de los datos es un tratamiento de datos que, en su caso, podrá encargar el responsable para que se pueda hacer un uso posterior de los datos. Este esquema de sujetos intervinientes en la mediación como responsables o encargados, desde el punto de vista de la protección de datos, puede seguirse en el artículo 31 del Real Decreto 980/2013, reglamento de desarrollo Ley 5/2012 de mediación en España.

La naturaleza pública o privada del responsable del tratamiento puede ser relevante en clave de protección de datos. Por ejemplo, el artículo 5.1 de la Ley 5/2012 expresamente dispone que la institución de mediación pueden ser “entidades públicas o privadas”. Cabe recordar, sin ser exhaustivo, que un tratamiento de datos público se legitima más fácilmente. Asimismo, las finalidades públicas suponen excepciones y limitaciones de diversos derechos. Los tratamientos públicos son el presupuesto de la obligatoria existencia del delegado de protección de datos. A los efectos del nivel de seguridad exigible, la naturaleza pública o privada del responsable en las legislaciones nacionales también puede tener incidencia.¹⁵

¹⁵ Así, por ejemplo, cabe tener en cuenta la hasta ahora vigente regulación del título VIII del Real Decreto 1720/2007, Reglamento LOPD, así como y en su caso, el Real Decreto 3/2010, de 8 de enero, por el cual se regula el esquema nacional de seguridad en el ámbito de la administración electrónica.

Sin perjuicio de la importancia de ser responsable o encargado del tratamiento, uno y otro tienen el deber de confidencialidad o secreto respecto a los datos que tratan. Este deber concurre con la confidencialidad propia de la mediación o del correspondiente deber de secreto que en particular pueda estar regulado.

El responsable del tratamiento ha de ser diligente en la elección de un encargado “que reúna garantías suficientes” y debe asegurarse de que se cumplan sus instrucciones. La relación entre responsable y encargado ha de formalizarse en un contrato escrito o del que quede constancia en el que conste el entramado de obligaciones en materia de protección de datos.

El acceso o tratamiento de los datos por el encargado no se considera comunicación de datos que requiera de consentimiento de los afectados o una base legal. No obstante, ha de cumplir con las instrucciones del responsable, las exigencias legales y del contrato, como no destinar los datos a otras finalidades, no comunicarlos y mantener los niveles de seguridad de los datos correspondientes. Si el encargado está establecido en la Unión Europea, debe cumplir con la normativa europea y ello es así con independencia de que el tratamiento se realice fuera de la Unión Europea.

Ahora bien, si el encargado no está establecido en la Unión Europea, habrán de cumplirse los requisitos para la transferencia internacional de datos del responsable al encargado. Hasta el nuevo Reglamento, la determinación del lugar del establecimiento del responsable o del encargado del fichero era importante a los efectos de la determinación del derecho nacional aplicable, como indica el artículo 4 de la Directiva 95/46/CE)

En la mediación europea, el responsable del tratamiento necesariamente estará establecido en un Estado de la Unión Europea. Es posible que haya varios corresponsables en varios países. Todos ellos habrán de cumplir con el reglamento. Si hay diversos corresponsables, hay que distinguir si lo que se comparte es un sistema de información, por ejemplo una plataforma, pero sin acceso de cada uno de los responsables a todos los datos.

En este supuesto, hay un sistema, pero diversos ficheros con varios responsables. En cambio, si lo que comparten son los datos personales, habrá corresponsables en el tratamiento de datos. En este supuesto, tendrán que determinar el protocolo de gestión y control de datos y “sus responsabilidades respectivas en el cumplimiento de las obligaciones [de protección de datos] en particular por lo que hace a los procedimientos y mecanismos para el ejercicio de derechos del interesado” (artículo 26.1 RGPD; véase también el Dictamen

1/2010, del Grupo del Artículo 29.¹⁶ En el caso de que se actúe bajo la autoridad del responsable y se traten datos fuera de la Unión Europea, se deben cumplir los requisitos de las transferencias internacionales de datos.

Cabe recordar también que con el RGPD desaparece la obligación de notificación del fichero, con el consiguiente registro. Se trata de una obligación que ha sido muy importante en países como España, y se ha emulado en muchos países de Iberoamérica. Su cumplimiento parecía imponer que cada responsable tenía que notificar el fichero, en cada país donde estuviera establecido, como puede en el caso de la mediación. No obstante, ahora está claro que ya no es aplicable en la Unión Europea.

4.4. Los derechos de la protección de datos en la mediación y sus límites

El derecho a la protección de datos implica otros derechos. Así en la Directiva se reconocían los derechos de acceso, rectificación, supresión y bloqueo (artículo 12 Directiva 95/46/CE), así como el derecho de oposición (artículo 16 Directiva 95/46/CE). El nuevo reglamento europeo reconoce el derecho de rectificación; el derecho de supresión (el derecho al olvido); el derecho a la limitación del tratamiento, acompañado de la obligación de notificación relativa a la rectificación o supresión de datos personales, así como a la limitación del tratamiento con el novedoso “derecho a la portabilidad de los datos”.

De igual modo, se reconoce el derecho de oposición en el artículo 21, así como las garantías en torno a las decisiones individuales automatizadas, incluida la elaboración de perfiles. De un modo u otro, todos estos derechos son proyectables en el ámbito de la mediación.

Especialmente el ejercicio del derecho a acceso por terceros a los datos en la mediación puede estar sujeto a restricciones, en razón de la especial confidencialidad propia a la mediación. Esta restricción puede considerarse en el marco de la excepción por “la protección del interesado o de los derechos y libertades de otras personas” (artículo 23.1 i RGPD); artículo 13 g Directiva 95/46/CE).

En cualquier caso, se precisa una previsión específica en la regulación de la mediación, la cual debe determinar el alcance de esta restricción de derechos. Esta regulación debe darse al tiempo que se da la regulación del acceso por las partes y terceros a la información de la mediación, presidida por el principio de confidencialidad.

¹⁶ Dictamen 1/2010, de 16 de febrero sobre los conceptos de “responsable del tratamiento” y “encargado del tratamiento” del Grupo del Artículo 29 (00264/10/ES WP 169).

5. Exigencias en el diseño de plataformas de mediación y la seguridad de la información confidencial

5.1. *La conveniencia de la anonimización o disociación de datos de la mediación*

La anonimización o disociación de los datos, si es efectiva, abate el régimen de confidencialidad propia de la mediación o las exigencias de protección de datos. Así, no hay problemas en el manejo de información que obstruyan la identificación de las partes del conflicto o al conflicto en sí. Para que dicha información quede liberada, esto es, no sometida al régimen jurídico de la confidencialidad y de la protección de datos, hay que anonimizar datos relativos a personas físicas (identificación, pixelación de imágenes, distorsión del sonido, etcétera). Pero, también hay que anonimizar la información relativa a personas jurídicas, pues está protegida por la confidencialidad propia de la mediación que va más allá de la protección de datos personales.

Ahora bien, sobre las dificultades de la anonimización para que exima del régimen jurídico de protección de datos, hay que tener especialmente en cuenta el Dictamen 05/2014 sobre técnicas de anonimización de 10 de abril del Grupo del artículo 29. El mismo señala que la anonimización debe ser completa e irreversible para poder lograr la no aplicación posterior del régimen de protección de datos. Hoy día, en razón de las tecnologías cada vez más avanzadas, no hay ninguna técnica de anonimización totalmente infalible.

De igual forma sucede en cuestiones de seguridad informática. La seguridad total no es posible por lo cual se debe buscar “la solidez necesaria para impedir la reidentificación de los datos mediante los medios más probables y razonables” (Dictamen 05/2014). En esencia, se trata de evitar la singularización de información, hasta identificar a personas; la vinculación de informaciones diferentes y correlacionarlas con personas, o la inferencia de datos personales a partir de informaciones. En nuestro caso, todo ello debe predicarse respecto de la mediación.

5.2. *El diseño y la seguridad de plataformas y contenidos de la mediación y sus responsables*

La información de cada mediación quedará soportada estructuradamente en ficheros. Quedará integrada en uno o varios sistemas de información, plataformas o ficheros más amplios que acojan la información de procedimientos de mediación. Los criterios de estructuración pueden ser bien diversos, como

la organización o institución que impulsa, gestiona y organiza la mediación, según materias y ámbitos sectoriales, según el sistema o plataforma de gestión de la mediación.

La garantía técnica de la confidencialidad propia de la mediación consistirá en el cumplimiento de las medidas de seguridad exigibles por protección de datos. No obstante, el régimen propio de la mediación, en ocasiones, contiene referencias de seguridad que se superponen a las de protección de datos. Así, por ejemplo, la normativa de mediación española impone en el caso de la mediación electrónica que “deberán incorporar mecanismos de registro de actividad que permitan auditar su correcto funcionamiento” (artículo 31.4 Real Decreto 980/2013, reglamento de desarrollo Ley 5/2012 de mediación).

De igual modo, la confidencialidad técnica tiene mucho que ver con el sistema de identificación de las partes que acceden a las plataformas en línea. De ahí que sea importante el cumplimiento de los requisitos de identificación y autenticación. No es extraño que los acuerdos de confidencialidad en sus cláusulas integren garantías de preservación de la misma, como la prohibición de grabación o transcripción de sesiones y la destrucción de información o materiales en poder del mediador tras la conclusión.¹⁷

Esta normativa propia de la confidencialidad de la mediación concurre y, en su caso, se superpone con las medidas de seguridad y otras exigencias propias de la protección de datos.

Los datos personales en el ámbito de la mediación civil no tienen por qué formar parte de las categorías especiales de datos que conllevan un régimen jurídico y de garantías específicos. La mediación penal o administrativa sancionadora sí quedaría bajo el régimen específico del artículo 10 RGPD (hasta ahora, artículo 8.5 de la Directiva 95/46/CE). Pese a que en general no se trate de datos especialmente protegidos, los datos personales vinculados a la mediación sí tienen una especial sensibilidad jurídica por diversos motivos:

- Toda la información, con o sin datos personales, de la mediación tiene un régimen específico de confidencialidad.
- Se trata de información sobre un ámbito objetivamente conflictual.
- En la mediación familiar la vida privada y la intimidad pueden quedar habitualmente afectadas, al igual que puede ser habitual el tratamiento

¹⁷ Así, por ejemplo, el “Acuerdo de mediación” de la Oficina de propiedad intelectual de la Unión Europea, Cláusula 6, Confidencialidad, apartado 6: “ Ni el mediador/los mediadores ni las partes llevarán a cabo grabaciones o transcripciones de la mediación. El mediador/los mediadores se compromete(n) a devolver, destruir o borrar este material en cualquier momento una vez concluida la mediación, sin conservar ninguna copia del mismo”.

de datos de menores o discapacitados.

- La mediación electrónica y la gestión integral a través de plataformas implica un masivo uso de telecomunicaciones y muy posiblemente de imágenes y audios de las personas intervinientes.

Esta especial sensibilidad jurídica se debe reflejar en mayores garantías de seguridad del tratamiento de datos en la mediación. En concreto, ello se tendrá en cuenta a la hora de determinar el “nivel de seguridad adecuado al riesgo” (artículo 32.1 RGPD). En buena medida, la determinación de tales niveles de seguridad queda en manos de las autoridades nacionales. Pero, en cualquier caso, la calificación de un nivel medio o alto de seguridad tiene una gran relevancia a la hora de toda la protección y gestión de la información.

De igual modo, los tratamientos de datos de una mediación, especialmente a través de plataformas electrónicas, reúnen los caracteres para que el responsable realice, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Tal evaluación de impacto se ha de realizar, “en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas” (artículo 35.1 RGPD).

No obstante, son las autoridades nacionales de protección de datos quienes deben determinar si las plataformas de mediación deben realizar o no este tipo de evaluación (artículos 35.4 y 5 RGPD). Si se considera que procede realizar la evaluación de impacto, ésta deberá prever los tratamientos y evaluar sus riesgos, así como tomar medidas, garantías y mecanismos frente a los mismos.¹⁸

También, en razón de los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, hay que seguir la protección de datos desde el diseño y por defecto (artículo 25 RGPD). La institución de mediación, como responsable del tratamiento de datos, debe adoptar todo tipo de medidas técnicas y organizativas apropiadas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento (artículo 25.1).

¹⁸ El mejor instrumento en español al respecto es el siguiente. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Guía para una evaluación de impacto en la protección de datos personales*, Madrid, 2014. Disponible en: <https://goo.gl/IWqn9l>

Se debe “garantizar que, por defecto, sólo sean objeto de tratamiento los datos personales que sean necesarios [y que] por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas” (artículo 25.2).

Debe señalarse que, en razón del RGPD, los responsables del cumplimiento de estas medidas de seguridad en las grandes organizaciones responsables o encargadas del tratamiento de datos serán los delegados de protección de datos. También ellos serán quienes implantarán las medidas de protección de datos desde el diseño y por defecto. De igual modo, hay que tener en cuenta la obligatoriedad de notificar las brechas o fugas de seguridad tanto a las autoridades de control, como a los usuarios o afectados.

Las plataformas electrónicas de mediación deberán configurarse como sistemas de intercambio electrónico de datos, en entornos cerrados de comunicación. Deberá ponerse especial énfasis en los sistemas de identificación y autenticación para el acceso a estas plataformas de modo restringido y sólo a los datos pertinentes, según el papel de cada sujeto (mediador, partes, intervinientes, y otros). El diseño y gestión de la plataforma habrá de tener en cuenta las específicas normas relativas al acceso a la información de las partes al procedimiento de mediación.

Este esquema se hace mucho más sencillo merced a las certificaciones del cumplimiento de normas técnicas por el encargado que presta servicios al responsable de la mediación. A este respecto, cabe remitir a la familia de las normas ISO 27000 de seguridad de la información, cuyo cumplimiento incluye la normativa de seguridad y confidencialidad. El impulso del cumplimiento de esta normativa técnica por los responsables y encargados de la mediación puede ser una herramienta útil.

Asimismo cabe tener en cuenta la renovada apuesta por los códigos de conducta, en materia de protección de datos por sectores específicos que pueden jugar un importante papel en la “correcta aplicación” del reglamento (artículos 40-43). La versión final del reglamento no señala sectores especialmente indicados para la elaboración de los códigos de conducta. No obstante, en el artículo 38 de una versión anterior, se señalaba como un sector especial donde elaborarlos: “los procedimientos extrajudiciales y otros procedimientos de resolución de litigios que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento de datos personales”.

Pese a que no exista actualmente esta referencia expresa, puede ser muy recomendable la elaboración de un código de conducta para este ámbito específico.

6. Los requisitos para admitir las transferencias internacionales

En todos los casos donde los datos personales en la mediación crucen las fronteras de la Unión Europea, hay que sujetarse al régimen de las transferencias internacionales de datos. Este movimiento de datos bien puede darse directamente por los responsables del tratamiento o por los encargados que prestan servicios a mediadores y a los sistemas de mediación.

Es posible que haya entidades de mediación transnacionales o que realicen parte de la actividad en el exterior. De igual modo, es muy posible que actúen en países terceros mediadores, las partes, otros intervinientes o quienes presen los servicios de las plataformas de mediación, los alojadores y servicios de nube, operadores de comunicaciones, entre otros.

Para que se pueda llevar a cabo este movimiento de datos, se requiere que el país tercero tenga un nivel esencialmente equivalente de protección de datos. La Comisión Europea, hasta la fecha, ha adoptado once decisiones respecto Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay y Nueva Zelanda.

En el caso de Estados Unidos, la Sentencia TJUE (Gran Sala), de 6 de octubre de 2015, en el asunto C 362/14 anuló su consideración de las empresas que se sumaban al sistema de “puerto seguro” para la transferencia de datos. Asimismo, se establecieron distintos parámetros de garantía efectiva del control por parte de las autoridades de datos del cumplimiento del nivel de seguridad. Tras la sentencia se adoptó un sistema relativamente similar, el llamado escudo de privacidad por Decisión (UE) 2016/1250 de la Comisión, de 12 de julio de 2016. Este mecanismo impone a las empresas que se sumen a seguir los principios de privacidad.

Incluso en los casos de transferencias a estos países (o empresas de Estados Unidos), las autoridades nacionales de protección de datos pueden comprobar que se dan los requisitos de forma concreta. Así pues, los sistemas europeos de mediación podrán realizar movimientos internacionales de datos a los referidos países y a los concretos servicios o empresas estadounidenses.

También es posible la transferencia de datos para la actividad de mediación a un país que no tenga reconocido este nivel esencialmente equivalente de protección de datos. Ahora bien, será posible el movimiento internacional si los interesados han dado su consentimiento o la transferencia es necesaria para el contrato de mediación (artículo 49.1 a y b RGPD. Por ello, es importante que el acuerdo o contrato de mediación incluya la previsión de la transferencia internacional por parte del responsable o sus encargados.

Dado que en la mediación se tratarán datos personales que van más allá de los datos relativos a las partes que firman el acuerdo de mediación, se hace preciso reunir garantías apropiadas. Esto con el fin de que la transferencia sea legítima (artículo 46 RGPD). Así ha de suceder, por ejemplo, en los contratos entre el responsable del tratamiento de datos de la mediación con todos sus encargados (mediadores, plataformas y otros servicios).

En caso de que la transferencia internacional de datos sea dentro de la institución u organización responsable de la mediación, la autorización para la transferencia internacional se obtiene si el responsable de la mediación cuenta con políticas internas de protección de datos (reglas corporativas vinculantes o *binding corporate rules*, BCR). Estas reglas corporativas modelo están fijadas por las autoridades nacionales de protección de datos, siguen criterios de la Comisión Europea y el artículo 47 RGPD las regula extensamente.

No sólo ha de haber estas reglas o políticas, sino que han de cumplirse efectivamente. Las autoridades nacionales en cualquier caso podrán comprobar el cumplimiento de las cláusulas contractuales o las reglas corporativas.

7. Conclusiones

Se ha abordado el binomio protección de datos y mediación. Más bien, pudiera ser un triángulo si se tiene en cuenta la confidencialidad como un tercer vértice. Sin duda, muchas más derivaciones pueden extraerse de este análisis. No obstante, se considera que diversas conclusiones pueden aportar algo de luz a esta materia de interés creciente y que no ha sido objeto de atención desde esta perspectiva, hasta la fecha.

Tanto la regulación, como el acuerdo de mediación o el marco contractual con quienes prestan servicios a la mediación, deben aprovecharse para mejorar, aclarar y subsanar carencias del actual régimen jurídico. La mediación, en todas sus formas, implica un “tratamiento” de datos. Es necesario aclarar y reforzar la legitimación al tratamiento de datos que supone la mediación, para además regular y concretar el régimen de la confidencialidad.

Se concluye que la interacción y concurrencia de la confidencialidad, propia a la mediación con las exigencias de la protección de datos, son dos ámbitos afines, en ocasiones, paralelos. No obstante, sería recomendable que una hipotética normativa de mediación haga mención a la naturaleza y finalidad que son propias de la confidencialidad de la mediación y su posible concurrencia con otras exigencias normativas. La confidencialidad de la mediación alcanza información que puede no estar protegida por el régimen de protección

de datos, como la información empresarial. Si se aplican técnicas de anonimización habrían de darse también respecto de esta información.

Asimismo, la normativa y el acuerdo de confidencialidad en la mediación podría expresar que los participantes no sólo que no están obligados, sino que tampoco pueden participar voluntariamente en los procedimientos. De igual modo, cabe concretar que si se llegase a aportar información confidencial de una mediación en un procedimiento judicial o arbitral posterior, ésta no debe admitirse como prueba o elemento de juicio, salvo las excepciones previstas.

Se han articulado las excepciones a la confidencialidad con el régimen de protección de datos. Se ha concluido que la excepción a la confidencialidad por exigencias imperiosas o finalidades superiores, por lo general, estará amparada por el régimen de protección de datos.

Ahora bien, habrá de realizarse una ponderación superpuesta y más exigente que es la concurrencia de intereses superiores. La normativa podría dejar clara esta especial ponderación, asimismo, habría de precisar qué tipo de autoridad (administrativa, policial, fiscalía o judicial) tiene la capacidad de exigir la quiebra de la confidencialidad.

Por otra parte, aunque las partes pueden consentir y exceptuar la confidencialidad propia de la mediación, el consentimiento legitima el uso de los datos personales de las partes, pero puede no ser suficiente para legitimar una comunicación de datos de terceros. De nuevo, la normativa y los acuerdos de mediación pueden armonizar el régimen de excepciones.

La proyección del régimen de protección de datos en el particular ámbito de la mediación ha llevado a diversas conclusiones. La mediación es un tratamiento de datos que ha de contar con legitimación. El acuerdo de mediación puede no ser suficiente, pues acudir a que la mediación es un interés legítimo es un terreno inseguro. Hay que abogar por que la normativa de mediación exprese, de modo suficiente, la base normativa o el interés legítimo suficiente para legitimar los tratamientos de datos que se dan en la mediación.

También se han examinado las posibilidades de usar la información de la mediación para distintas finalidades. En este sentido, se ha concluido que, dada la necesaria confidencialidad propia a la mediación, el uso de los datos de un procedimiento de mediación, para su uso posterior en el ámbito administrativo o judicial, es una finalidad claramente incompatible que exige una nueva base legitimadora. La regulación y el acuerdo de mediación son los elementos básicos para legitimar estos usos incompatibles.

El uso de la información de mediación para fines históricos, estadísticos y de investigación será posible y compatible con la finalidad de origen. Sin

embargo, el uso de información de mediación para la formación requeriría una legitimación específica. Lo mismo cabe predicar respecto a la difusión de la información de la mediación y sus resultados, a través de bases de datos de mediación o la publicidad activa sobre procedimientos de mediación. Una futura normativa de la mediación o, en su caso, el marco contractual de la mediación, podría contemplar también esta posible excepción. En todos estos casos también se deben contemplar garantías como la anonimización, en lo posible de la información de la mediación.

En cuanto al responsable y encargado del tratamiento de protección de datos, por lo general hay que considerar responsables a las instituciones de mediación. Se recuerda que en su caso pueden ser instituciones públicas lo cual puede desencadenar diversos efectos en materia de protección de datos, como vías específicas de legitimación y de excepción a derechos u obligación de delegado de protección de datos.

Las instituciones de mediación contarán con una serie de intervinientes que les prestarán servicios. Todos ellos serán encargados, a efectos de protección de datos, de modo que pueden ser responsables por infracción de normativa de protección de datos al tiempo que tienen el deber de confidencialidad o secreto. El responsable del tratamiento debe elegir; ha de ser diligente en la elección de un encargado y formalizar la relación con el régimen de obligaciones. El estudio también ha analizado el régimen de obligaciones de responsable y encargado, así como la posibilidad de que sean diversos y actúen fuera de la Unión Europea.

Igualmente, se ha concluido la conveniencia de que el marco normativo y contractual de la mediación exprese las limitaciones que se dan respecto a los derechos de la protección de datos, sobre todo respecto al posible acceso por terceros a la información de la mediación, especialmente protegida por la confidencialidad.

En cuanto a las exigencias de seguridad de plataformas e información de la mediación, hay varias conclusiones. La regulación o el acuerdo de la mediación o las concretas cláusulas de los acuerdos de confidencialidad pueden contemplar referencias y medidas de seguridad concretas. Tales exigencias se superponen a las exigencias de seguridad en razón de la protección de datos, aunque no en general.

La información de la mediación, como pueden ser la penal o administrativa, en algunas ocasiones puede ser una categoría especial de datos, con las implicaciones que conlleva. En todo caso se ha concluido que los datos personales vinculados a la mediación sí tienen un especial riesgo y singular sensibilidad

jurídica. Ello debe tener su reflejo a la hora de determinar el nivel de seguridad adecuado al riesgo que fijan las autoridades nacionales.

Lo anterior afecta a la obligatoriedad de hacer una evaluación del impacto y respecto de la protección de datos desde el diseño y por defecto. Asimismo, en la mediación, generalmente serán exigibles los delegados de protección de datos. También se ha concluido que este esquema se puede hacer mucho más sencillo merced a las certificaciones del cumplimiento de normas técnicas ISO 27000 y que mediación es un sector especialmente indicado para la elaboración de códigos de conducta.

Finalmente, los datos personales en la mediación son habitual objeto de transferencias internacionales de datos. El cumplimiento de la legalidad en la mediación será más sencillo si el movimiento de datos es a un país con un nivel esencialmente equivalente de protección de datos (o a una empresa estadounidense que cumpla con los principios de privacidad del régimen de escudo de privacidad, de 2016).

En todo caso, se ha subrayado la utilidad de prever expresamente la transferencia internacional en el acuerdo de mediación, así como en los contratos entre el responsable del tratamiento de datos de la mediación con todos sus encargados (mediadores, plataformas y otros servicios). De igual modo, el movimiento internacional de datos de las plataformas de mediación puede legitimarse también a través de las normativas internas de protección de datos (reglas corporativas vinculantes o *binding corporate rules*).

Bibliografía

- “Acuerdo de mediación”, *Oficina de propiedad intelectual de la Unión Europea*. Disponible en: <https://goo.gl/WozeSS>
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Guía para una evaluación de impacto en la protección de datos personales*, Madrid, 2014. Disponible en: <https://goo.gl/IWqn9l>
- ÁLVAREZ HERNANDO, JAVIER y PRIETO ESCUDERO, EVA, “Nueva regulación de la mediación por medios electrónicos”, *Iuris. Actualidad y práctica del derecho*, núm. 212, 2014, pp. 24-29.
- ALZATE SÁEZ DE HEREDIA, RAMÓN y VÁZQUEZ DE CASTRO, EDUARDO, *Resolución de disputas en línea (RDL). Las claves de la mediación en línea*, Madrid, Reus, 2014.
- ARENAS RAMIRO, MÓNICA, *El derecho fundamental a la protección de datos personales en Europa*, Valencia, Agencia Española de Protección de Datos - Tirant lo Blanch, 2006.

- BUENO DE MATA, FEDERICO, “Mediación electrónica e inteligencia artificial”, *Actualidad civil*, núm. 1.
- BUJOSA VADELL, LORENZO y GALLARDO RODRÍGUEZ, ALMUDENA, *Electronic mediation and e-mediator: proposal for the European Union*, Granada, Comares, 2017.
- CORVO LÓPEZ, FELISA MARÍA, “El alcance del deber de confidencialidad en el proceso de mediación familiar”, en *2009 Workshop Internacional sobre ADR/ODRS. Construyendo puentes: marco jurídico y principios*, Universitat Oberta de Catalunya - Internet Interdisciplinary Institute. Disponible en: <http://www.uoc.edu/symposia/adr>
- FRANCO CONFORTI, ÓSCAR DANIEL, “La mediación de conflictos por medios electrónicos”, *Mediatio: mediación*, núm. 4, pp. 17-31.
- GARCÍA CUBERO, GUILLERMO, “Mediación por medios electrónicos: procedimiento y herramientas”, en Emiliano Carretero Morales (dir.), *Mediación y resolución de conflictos: técnicas y ámbitos*, Madrid, Tecnos, 2013.
- GARCÍA DEL POYO, RAFAEL, “La mediación electrónica”, *Revista jurídica de Castilla y León, Ejemplar dedicado a Arbitraje y Mediación: Problemas actuales, retos y oportunidades*, núm. 29.
- MARTÍNEZ MARTÍNEZ, RICARD, *Una aproximación crítica a la autodeterminación informativa*, Madrid, Civitas, 2004.
- MONTESINOS GARCÍA, ANA, “Arbitraje on line”, en Javier Plaza Penadés, *Cuestiones actuales de derecho y tecnologías de la información y la comunicación (TICS)*, Cizur Menor, Aranzadi, 2006.
- MONTESINOS GARCÍA, ANA, “Mediación on line”, *Revista de la contratación electrónica*, Núm. 94, 2008, pp. 85-110.
- MONTESINOS GARCÍA, ANA, *Arbitraje on line*, Universitat de València, 2006. Disponible en: <https://dialnet.unirioja.es/servlet/exttes?codigo=73607>
- MORETÓN TOQUERO, ARÁNZAZU, “El secreto profesional y el deber de confidencialidad del mediador”, en Nuria Belloso Martín (coord.), *Estudios sobre mediación: la Ley de mediación familiar de Castilla y León*, España, Junta de Castilla y León, 2006.
- PÉREZ GURREA, ROSANA, “Estudio sistemático, normativo y doctrinal de la mediación en asuntos civiles y mercantiles: una especial referencia a la mediación electrónica”, *Revista Digital Facultad de Derecho, Ejemplar dedicado a Premios García Goyena XII Edición*, núm. 2, pp. 194-223.
- PIÑAR MAÑAS, JOSÉ LUIS, *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*, Madrid, Reus, 2016.
- RALLO LOMBARTE, ARTEMI y GARCÍA MAHAMUT, ROSARIO, *Hacia un nuevo derecho europeo de protección de datos*, Valencia, Tirant lo Blanch, 2015.
- RAMÓN FERNÁNDEZ, FRANCISCA, “La mediación electrónica, la confidencialidad y la protección de datos de carácter personal”, *Revista InDret*, núm. 3, pp. 1-28.
- SANZ PARRILLA, MILAGROS, “El uso de medios electrónicos en la mediación”, en Emiliano Carretero Morales (dir.), *Mediación y resolución de conflictos: técnicas y ámbitos*, Tecnos, Madrid, 2013.

- VÁZQUEZ DE CASTRO, EDUARDO, “Las nuevas previsiones de mediación electrónica”, en Francisco de Paula Blasco Gascó (dir.), *Estudios jurídicos en homenaje a Vicente L. Montés Penadés*, tomo 2, vol. 2, Valencia, Tirant lo Blanch, 2011, pp. 2737-2762.
- VÁZQUEZ DE CASTRO, EDUARDO y FERNÁNDEZ CANALES, CARMEN, “El actual marco normativo de la mediación electrónica”, *Revista Crítica de Derecho Inmobiliario*, núm. 731, pp. 1451-1480.
- VILALTA NICUESA, AURA ESTHER, *Medición y arbitraje electrónicos*, Navarra, Aranzadi, 2013.
- VIOLA DEMESTRE, ISABEL, “La confidencialidad en el procedimiento de mediación”, *IDP: revista de internet, derecho y política*, núm. 11, pp. 1-10.