

APROXIMACIÓN A LOS SMART CONTRACTS DESDE
UN PUNTO DE VISTA DEL DERECHO INTERNACIONAL
PRIVADO

*APPROACH TO SMART CONTRACTS FROM AN INTERNATIONAL
PRIVATE LAW POINT OF VIEW*

Actualidad Jurídica Iberoamericana N° 18, febrero 2023, ISSN: 2386-4567, pp. 634-657



Antonio
MERCHÁN
MURILLO

ARTÍCULO RECIBIDO: 8 de octubre de 2022

ARTÍCULO APROBADO: 5 de diciembre de 2022

RESUMEN: A través de este trabajo se trata de realizar un estudio en relación al marco normativo de los Smart contract o contratos inteligentes. De esta forma, partiendo de una conceptualización propia, se trata de hacer una profundización en la normativa, que les resultará aplicable, para finalmente tratar de determinar la Ley aplicable a estos contratos, a través de las normas de Derecho internacional privado.

PALABRAS CLAVE: Contratos inteligentes; Blockchain; Inteligencia Artificial; Computación en nube; Identidad electrónica.

ABSTRACT: *Through this work we try to carry out a study in relation to the regulatory framework of the Smart contract or intelligent contracts. In this way, starting from their own conceptualization, it is a matter of making a deepening of the regulations, which will be applicable to them, to finally try to determine the Law applicable to these contracts, through the rules of private international law.*

KEY WORDS: *Smart contracts; blockchain; Artificial intelligence; cloud computing; e-Identity.*

SUMARIO.- I. INTRODUCCIÓN.- II. CONCEPTUALIZACIÓN DEL SMART CONTRACT Y SUS CARACTERÍSTICAS.- III. CONSIDERACIONES NORMATIVAS PREVIAS.- IV. LA PROBLEMÁTICA PROPIA DEL CONTEXTO TECNOLÓGICO USADO.- V. LOS SMART CONTRACTS Y EL DERECHO INTERNACIONAL PRIVADO.- I. La repercusión transfronteriza del smart contract.- 2. La determinación de la ley aplicable en supuesto de responsabilidad contractual.- VI. CONCLUSIONES.

I. INTRODUCCIÓN.

Los Smart contracts o contratos inteligentes son aclamados como uno de los primeros avances tecnológicos verdaderamente disruptivos para la práctica del derecho. Estos contratos se están desarrollando en una gran variedad de sectores, que van desde el sector financiero, el sector público, la gestión de la cadena de suministro a los seguros, etc. Ante esto, se ha intensificado el debate sobre las implicaciones legales de este fenómeno.

Junto a los Smart contracts aparece la tecnología Blockchain, que ha alimentado el interés de los legisladores, quienes han comenzado a reconocer las incertidumbres regulatorias y están haciendo los primeros intentos de introducir soluciones legislativas para abordarlas. La motivación detrás de las iniciativas legislativas de contratos inteligentes introducidas hasta ahora tiende a reducir la inseguridad jurídica y mitigar los riesgos potenciales de los contratos inteligentes, aunque no del todo.

Junto a Blockchain y los Smart contracts, aparece la informática en la nube que puede definirse como los servicios informáticos (por ejemplo, el almacenamiento y el procesamiento de datos) por Internet¹ o lo que es lo mismo el almacenamiento, tratamiento y utilización de datos en ordenadores a distancia a los que se tiene acceso a través de Internet²; es decir, la computación en nube permite la disponibilidad de capacidad informática en todas partes y para cualquier persona.

Además, de todo lo anterior, no debe perderse de vista la Inteligencia artificial, es decir el “software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I y que puede, para un conjunto determinado

1 CNUDMI: *Labor prevista y posible labor futura: parte cuarta Propuesta del Gobierno del Canadá: posible labor futura en materia de comercio electrónico: cuestiones jurídicas que afectan a la informática “en la nube”*, Nueva York, 7 a 18 de julio de 2014, p. 4.

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

• **Antonio Merchán Murillo**

Prof. Ayudante Doctor
Universidad Pablo de Olavide (España)
e.mail amermur@upo.es

de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa” (artículo 3,1 de la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión).

Con esta breve introducción, se pueden observar las implicaciones jurídicas que conllevan los Smart contracts, en el mundo empresarial y personal. Es una cuestión de suma importancia, ante el desarrollo tecnológico que supone, el avanzado estado en el que se encuentra y el uso cada vez más cotidiano que se realiza, a nivel nacional y transfronterizo. Habida cuenta de lo anterior, surge la necesidad de estudiar su problemática desde el punto de vista del Derecho Internacional Privado.

II. CONCEPTUALIZACIÓN DEL SMART CONTRACT Y SUS CARACTERÍSTICAS.

El término contrato inteligente y la idea subyacente datan de mucho antes del surgimiento de Bitcoin y la tecnología Blockchain. Szabo³, en 1994, definió un contrato inteligente como una pieza de protocolo de transacción computerizado que satisface condiciones contractuales tales como condiciones de pago, confidencialidad o cumplimiento, reduce las excepciones y minimiza la necesidad de intermediarios de confianza. Mencionó los protocolos de efectivo digital como ejemplos de contratos inteligentes, ya que los mecanismos permiten el pago en línea en combinación con las características del efectivo en papel, como la divisibilidad y la confidencialidad.

En cualquier caso, y quizá de una manera más sencilla, puede decirse que los contratos inteligentes son, en resumen, pequeños programas que se ejecutan; es decir, “si esto sucede, haz aquello”⁴. Los contratos inteligentes que se ejecutan en Blockchain son más difíciles de definir de manera concisa. No obstante, estos Smart contracts los podemos identificar como scripts anclados en una cadena de bloques o una infraestructura distribuida similar. Tan pronto como se activa mediante una transacción de Blockchain y se valida en toda la red, se ejecutan acciones predefinidas. Dado que las condiciones de un contrato inteligente se almacenan de forma transparente en la cadena de bloques, siempre funcionará según lo previsto por todas las partes, lo que puede reducir los problemas de

3 SZABO, N.: *Smart contracts Go to reference in article*, 1994. Disponible en: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts.html (última fecha de consulta 29 de noviembre de 2022)

4 GRAFF, T. J.: “From old to new: From internet to smart contracts and from people to smart contracts”, *Computer Law & Security Review*, núm. 35, octubre, 2019.

confianza entre las partes involucradas. Los contratos inteligentes son scripts de software, al igual que los scripts que se ejecutan en aplicaciones que no son de cadena de bloques⁵.

La tecnología Blockchain, tecnología subyacente a los contratos inteligentes, es una de las tecnologías de libro mayor distribuido (también conocida como libro mayor público descentralizado, libro mayor público sin confianza, tecnologías de libro mayor compartido). En este mismo contexto aparece la tecnología computacional, el uso de claves criptográficas, el almacenamiento de datos distribuidos. Ahora bien, la cuestión principal a tratar es la Blockchain que va a ayudar a resolver el problema de cómo se podría asegurar la coordinación de la actividad de los individuos sin una autoridad central que garantice la validez de las transacciones.

En este punto, aparecen varios debates sobre la naturaleza de los contratos inteligentes. Para participar en ellos, sin duda es útil comprender las diferencias entre los distintos tipos de programas informáticos con los que operamos a diario, para ver cómo han evolucionado los Smart contracts⁶, para comprobar que hoy en día, los contratos inteligentes se entienden principalmente como acuerdos codificados en un código informático y colocados en una infraestructura virtual descentralizada. Los protocolos informáticos verifican y ejecutan las cláusulas y la ejecución de un contrato, lo que hace innecesarias algunas actividades contractuales tradicionales involucradas en la ejecución. La tecnología permite la implementación automática de los términos de un acuerdo⁷. Tanto el término inteligente como el término contrato son engañosos, ya que un contrato inteligente consiste en un código informático, hecho por otra persona física o jurídica, para un fin, por lo que puede ser considerado, en nuestra opinión como obediente.

Si bien los contratos inteligentes parecen tener una amplia gama de beneficios, existen muchos desafíos y riesgos. Un contrato inteligente no puede activarse solo. Solo cobra vida cuando una de sus funciones aparece programada en una transacción. Por lo tanto, los contratos inteligentes en ningún caso son autónomos, sino que siempre requieren un evento externo (por ejemplo, una transacción) para activarlos. Un desafío de los casos de uso de contratos inteligentes se refiere al problema del procesamiento de información y eventos que no ocurren directamente en la cadena de bloques. Si bien un contrato inteligente puede reaccionar de inmediato a una transacción de la cadena de bloques, ya que todo

5 LENNART, A.: "Smart contracts on the blockchain – A bibliometric analysis and review", *Telematics and Informatics*, núm. 57, marzo 2021, pp. 10-19.

6 SURDEN, H.: *Computable Contracts*, University of California, 2012, Vol. 46. Disponible en: https://lawreview.law.ucdavis.edu/issues/46/2/articles/46-2_surden.pdf

7 EENMAA-DIMITRIEVA, H.; SCHMIDT-KESSEN, J.: "Creating markets in no-trust environments: The law and economics of smart contracts", *Computer Law & Security Review*, núm. 35, 2019, pp. 69-88.

el proceso se maneja en la cadena, si la información requerida, por ejemplo, se refiere a una persona que no está en la cadena, el script no puede recopilar la información por sí mismo. Si bien la cadena de bloques proporciona un entorno confiable, es posible que los participantes de un contrato inteligente no confíen en la información que se transmite a la cadena de bloques. Esto se conoce como el problema del oráculo y se aplica a cualquier individuo, software o hardware involucrado en estos procesos.

En principio, la cadena de bloques no es una tecnología eficiente: todos los participantes de la red deben almacenar una copia de la cadena de bloques, lo que también se aplica al código informático anclado. En las cadenas de bloques públicas, los contratos inteligentes se ejecutan globalmente, lo que significa que cada nodo de la cadena de bloques ejecuta el contrato cada vez. Dado que la computación es un proceso determinista, la ejecución global puede no ser estrictamente necesaria⁸. Otro desafío que surge del almacenamiento de toda la información por parte de todos los participantes de la red es la protección de datos. Los datos almacenados no se eliminan fácilmente, lo que entra en conflicto con requisitos legales como el derecho al olvido⁹.

Por otro lado, cuando hablamos de los contratos inteligentes, debemos hacer referencia a donde se ejecutan. Hasta la fecha, existe una multitud de plataformas de contratos inteligentes. En este contexto, destacamos la informática en la nube o computación en nube, conocida principalmente por su denominación en inglés, cloud computing (en adelante, CC), que permite el acceso por medio de una red de telecomunicación (Internet), a demanda y en régimen de autoservicio, a recursos informáticos compartidos configurables¹⁰.

Los servicios prestados son muy variados y pueden ir desde el mero suministro de infraestructuras informáticas, programas informáticos y herramientas de comunicación a servicios más sofisticados, destacando el almacenamiento de datos. Son muchos los proveedores que ofrecen capacidades de almacenamiento de diferentes tamaños y bajo diferentes fórmulas comerciales, ya sea de manera gratuita o de pago. Estas capacidades de almacenamiento están destinadas, habitualmente, al uso privativo del beneficiario, pero también pueden contener funcionalidades compartidas.

8 GREENSPAN: "Gideon. Smart contracts: The good, the bad and the lazy", *Private blockchains, Smart contracts*. 2015. Disponible en: <https://www.multichain.com/blog/2015/11/smart-contracts-good-bad-lazy/>

9 FINCK, M.: "Blockchains and Data Protection in the European Union", *European Data Protection Law Review*, 4 (1) (2018), pp. 17-35.

10 POLITOU, E.; CASINO, F.; ALEPIS, E.; C. PATSAKIS, C.: "Blockchain Mutability: Challenges and Proposed Solutions", *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2019, pp. 1-13.

A modo de reflexión, puede afirmarse que la CC puede entenderse como la combinación de tres elementos interdependientes: las infraestructuras que almacenan y gestionan los datos, las redes que transportan los datos y los ordenadores que pueden utilizarse para procesarlos. La CC dispone de una gama de características definitorias: autoservicio a pedido (servicio que está disponible en cualquier momento, a pedido y sin necesidad de una intervención humana por parte del proveedor de servicios); acceso a la red (la nube está disponible a través de conexiones a la Internet); combinación de recursos (la capacidad informática del proveedor de servicios no está asignada específicamente a cada usuario); elasticidad (los recursos informáticos del proveedor de servicios están puestos a disposición ilimitada de todos los usuarios); y escala de servicios (y adaptan en función de las necesidades de cada cliente)¹¹.

Debe tenerse claro que hablamos de un modelo que permite acceso de red ubicuo, conveniente y bajo demanda a un conjunto de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios)¹² que pueden aprovisionarse y liberarse rápidamente con un mínimo esfuerzo de gestión o interacción por parte del proveedor de servicios¹³.

Los servicios de CC se ofrecen a través de servicios gratuitos, siendo de pago a partir de cierto volumen, pero la escala y el uso resulta especialmente relevante desde un punto de vista empresarial, como resultado directo de las transformaciones tecnológicas y que las empresas necesitan nuevas formas para reducir los costes informáticos. Las empresas externalizan las capacidades de procesamiento de datos, los recursos basados en Internet y la entrega de aplicaciones de tecnologías de la información y la comunicación, almacenamiento y espacio de memoria a los servicios en la nube.

III. CONSIDERACIONES NORMATIVAS PREVIAS.

En relación a lo dicho anteriormente, será necesario ver que normas se va a aplicar y, por tanto, van a ser relevantes. De esta forma, los acuerdos atributivos de competencia incluidos en el contrato subyacente, en la medida en que sean eficaces conforme a las reglas de nuestro sistema de Derecho internacional privado (en principio conforme a lo establecido al Reglamento 1215/2012, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la

11 CNUDMI: *Labor prevista y posible labor futura: parte cuarta Propuesta del Gobierno del Canadá: posible labor futura en materia de comercio electrónico: cuestiones jurídicas que afectan a la informática "en la nube"*, Viena, 29 de junio a 16 de julio de 2015, p. 3.

12 SHOJAIEMEHRA AMIR, B.; RAHMANIA NOORULDEEN, M.; Qader, N.: "Cloud computing service negotiation: A systematic review", *Computer Standards & Interfaces*, vol., 2018, pp. 196-206.

13 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), U. S. Department of Commerce: *The NIST Definition of Cloud Computing - Recommendations of the National Institute of Standards and Technology*, Septiembre, 2011, p. 2.

ejecución de resoluciones judiciales en materia civil y mercantil – Reglamento Bruselas I bis), que restringe significativamente su operatividad en las transacciones con consumidores.

Al margen de esas transacciones, habrá que observarse la eventual incidencia de reglas especiales como la del artículo 25.2 Reglamento Bruselas I bis con respecto a la forma escrita en la contratación electrónica, presupuesto de la eficacia de los acuerdos atributivos de competencia. Asimismo, habrán de observarse las situaciones en las que llegue a ser aplicable el fuero especial del artículo 7.1 Reglamento 1215/2012 podrá resultar controvertido en qué medida la automatización de ciertas prestaciones condiciona la determinación del lugar de cumplimiento de la obligación a los efectos de esa norma.

En relación con la Ley aplicable vamos a tener presente cuestiones que tienen que ver con el significado del cumplimiento automatizado de ciertos compromisos y su interacción con la relación subyacente entre las partes. El criterio de base es que habrá que estar en principio a lo dispuesto en el Reglamento Roma I (incluido su régimen específico de protección de los consumidores y la aplicación de normas de transposición de las Directivas sobre consumidores) en relación con la transacción subyacente entre las partes, sin desconocer que la aplicación de ciertas disposiciones puede ser fuente de controversia –por ejemplo, su art. 14.2 y la concreción en este marco del lugar de cumplimiento-, así como que otros instrumentos normativos también pueden ser relevantes.

Por ejemplo, el criterio de origen de la Directiva sobre el comercio electrónico en relación con los aspectos contractuales incluidos en el ámbito coordinado de la Directiva cuando ésta resulte de aplicación. Necesario será también tener en cuenta la existencia de cuestiones sometidas a conexión autónoma, entre otras, la capacidad para contratar y, muy especialmente, todo lo relativo al régimen aplicable en materia de protección de datos personales, en el que habrá que estar a lo dispuesto en el artículo 3 del Reglamento 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 lo que concierne a la necesidad de cumplir con lo dispuesto en el mismo en las situaciones incluidas dentro de su ámbito de aplicación territorial y el artículo 79,2 del mismo, pues en estos artículos se plantean las normas de conflicto en relación a la competencia judicial y ley aplicable.

Ahora bien, sin perjuicio de lo anterior, la eficacia probatoria para acreditar transacciones u otras circunstancias en el marco de procesos judiciales vendrá en principio determinada, en tanto que cuestión procesal, por la *lex fori*.

En el contexto de la UE resulta de especial relevancia a estos efectos el Reglamento 910/2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE y, aún más, la modificación que se de éste en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea, publicada el 3 de junio de 2021¹⁴, que se presenta fundamental, como se verá más adelante, ya que su objetivo es proporcionar, para la utilización transfronteriza, entre otras cuestiones el “acceso a soluciones de identidad electrónica altamente seguras y fiables, la garantía de que los servicios públicos y privados puedan apoyarse en soluciones de identidad digital fiables y seguras y la garantía de que las personas físicas y jurídicas puedan utilizar soluciones de identidad digital”.

IV. LA PROBLEMÁTICA PROPIA DEL CONTEXTO TECNOLÓGICO USADO.

Todo esto conforme al principio de preexistencia del derecho existente. Ahora bien, en la relación contractual subyacente nos vamos a encontrar supuesto en los que se pueda dar una no-nacionalidad la tecnología, como hemos visto antes, pudiendo encontrarnos con problemas en los criterios de conexión, insolvencias transfronterizas que Blockchain nos detecta, etc., son problemas que, si no ahora lo serán con el tiempo, cuando la inteligencia artificial avance y, además, las empresas evolucionen a la nube.

¿Por qué? La cadena de bloques plantea diferentes riesgos como consecuencia de la tecnología y la forma de las operaciones: uno de los principales problemas afectará a la cadena de bloques es la incapacidad de controlar y detener su funcionamiento. Además, la falta de control sobre el funcionamiento puede provocar la falta de responsabilidad de la empresa que administra la plataforma¹⁵. Pensemos que, en su forma más simple, Blockchain es una tecnología descentralizada o un libro mayor distribuido en el que las transacciones se registran de forma anónima. Esto significa que el libro mayor de transacciones se mantiene simultáneamente en una red de ordenadores o servidores no relacionados.

Por lo tanto, la asignación y la atribución del riesgo y la responsabilidad en relación con un servicio de Blockchain que no funciona correctamente deberán analizarse cuidadosamente, no solo a nivel de proveedor-cliente, sino también en torno a todos los participantes en el sistema.

14 Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea {SEC(2021) 228 final} - {SWD(2021) 124 final} - {SWD(2021) 125 final}. Disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52021PC0281>

15 BURDEN, K.: “Eu Update”, *Computer Law & Security Review*, Vol. 34, Núm. 2, Abril, 2018, Pp. 409-418.

Debe tenerse en cuenta, respecto al proceso, que Blockchain que tiene la capacidad de cruzar límites jurisdiccionales ya que los nodos en una Blockchain pueden ubicarse en cualquier parte del mundo.

Esto puede plantear una serie de problemas complejos que requieren una cuidadosa consideración en relación con las relaciones ciudadanos-Estado, empresa-Estado, empresa-empresa, ciudadanos-empresa, empresa-administración, ciudadano-Administraciones de un mismo Estado y de distintos. En este sentido, deberá observarse que, en un entorno descentralizado, puede ser difícil identificar el conjunto apropiado de reglas a aplicar. Estonia lo hace.

Y lo hace planteando la identidad electrónica como un criterio de conexión, ya que guarda relación con la residencia, en este caso electrónica, en tanto que la necesidad de vincular la información y su manejo, únicamente, con quien la emite se hace esencial para numerosas interacciones diferentes: una infraestructura organizativa (gestión de la identidad) y una infraestructura técnica (sistemas de gestión de identidad), para desarrollar, definir, designar, administrar y especificar los niveles de autorización, asignando roles y atributos de identidad relacionados con grupos específicos de personas, como los administradores de la sociedad, los empleados o los clientes

La evolución de la tecnológica está creando grandes archivos electrónicos, con ello grandes bases de datos comerciales y estatales. Un identificador nacional, contenido en una cédula de identidad, permite capturar información sobre una persona, que se halla en diferentes bases de datos, con el fin de que ellas puedan ser fácilmente enlazadas y analizadas a través de determinadas técnicas de análisis de datos. Al mismo tiempo, las cédulas de identidad también se están volviendo más inteligentes. La generación de los datos tiene, además, la virtualidad de ofrecerse en un medio donde pueden pasar a ser directamente tratados. De esta forma, se crean archivos susceptibles de cruce y estructuración, así como de cesión. Por esta razón, hay que poner especial atención ante cualquier sistema de gestión de la identidad y ver quiénes son dónde se encuentran las personas.

En su nivel más simple, cada transacción podría caer dentro de la jurisdicción de la ubicación de cada nodo en la red. Con ello, debe advertirse que en un entorno en línea autenticar la identidad de la parte remota es más importante que nunca. Desempeña un papel clave en la lucha contra el fraude de identidad y, además, es esencial para establecer una confianza necesaria que facilite cualquier tipo las transacciones electrónicas.

En este punto, debe tenerse en cuenta que la relación Derecho e informática va más allá de lo que se ha visto hasta ahora¹⁶. Es por eso por lo que una de las cuestiones principales que se plantean, con respecto a los servicios transfronterizo, son la seguridad y la confidencialidad de la información transmitida por Internet, que nos debe llevar a garantizar la protección de los datos de carácter personal que conducen a la identificación de su titular.

Con ello nos referimos a que la identidad electrónica, es una identidad que se compone de información almacenada y transmitida a los distintos usuarios de ésta. Pensemos que la identidad es un elemento fundamental, que vincula la información a su propietario, localizado en algún Estado dando lugar a su localización, y, por tanto, al buen manejo efectivo y seguro de los datos específicos que dan entrada a la nube.

Debemos tener presente que todos los esquemas de identidad electrónica dependen de dos procesos: primero, autenticación de identidad y, posteriormente, verificación de identidad. Cuando se autentica, la identidad se registra en el sistema y luego se puede usar para realizar transacciones. La identidad se verifica en el momento de cada transacción, desde dentro de la propia nube. De la información registrada en ese momento, surge la información de identificación o que va a identificar a la persona, tal y como si fuera la firma, que se usará, posteriormente, para vincular a un individuo de manera inseparable.

V. LOS SMART CONTRACTS Y EL DERECHO INTERNACIONAL PRIVADO.

I. La repercusión transfronteriza del smart contract.

Una cuestión fundamental en el Derecho internacional privado es ver si el contrato inteligente en cuestión va a estar conectado o no con dos o más ordenamientos jurídicos, con independencia de la naturaleza, relevancia o intensidad del elemento extranjero¹⁷. Refiriéndonos a los datos, debe observarse que son elementos que se localizan en la nube, fundamentalmente, asociados a la tecnología, siendo destacable la no nacionalidad de ésta. Ahora bien, esto no significa que los servidores, en los que se ubican los datos, no la tengan, aunque este aspecto puede cambiar, en función a la temporalidad de éste.

Lo anterior nos lleva a la necesidad de ver la nacionalidad o residencia habitual o domicilio de alguna de las partes o a las mismas en relación con los interesados o al lugar en el que están ubicados los datos o, incluso, al lugar de celebración

16 VIGUERA REVUELTA, R.: "Los contratos informáticos", *Revista de la Contratación Electrónica*, núm. 97, 2008, p. 61

17 CALVO CARAVACA, A-L.; CARRASCOSA GONZÁLEZ, J.: *Derecho Internacional Privado*, vol. II, 18ª ed., Comares, Granada, 2018, p. 1003.

de este. En este contexto, cabría afirmar que la naturaleza transfronteriza del contrato se verificaría cuando estuviese vinculados con dos o más ordenamientos jurídicos nacionales de tal manera que surgiera la duda de cuál de ellos sería el reclamado para regularla. Para ello resultaría conveniente lo siguiente¹⁸:

1ª En primer término el carácter transfronterizo podría derivar de un elemento endógeno de la situación (personal, objetivo o territorial), de un elemento exógeno a la misma, esto es, de la voluntad de los concernidos mediante la determinación como competente de una autoridad extranjera o como aplicable de un ordenamiento foráneo, todo ello para una situación en principio meramente interna.

2ª En segundo lugar se requeriría que el elemento extranjero presentase una mínima importancia hasta el punto de que su presencia en la situación justificase variar la respuesta legal prevista para supuestos internos¹⁹.

3ª Finalmente no sería preciso que el o los ordenamientos extranjeros vinculados con el supuesto en cuestión fuesen de un país cuyas autoridades aplicasen los Reglamentos; pudiendo también ser de un Estado de la Unión cuyas autoridades no lo aplicasen o de un Estado tercero cualquiera.

Todo lo anterior va a aparecer, pues la informática en la nube suele incluir un componente internacional debido a que los datos con frecuencia son almacenados o transferidos entre servidores situados en diferentes países, siendo los principales riesgos los vinculados con la divulgación accidental o ilegítima de información confidencial o secreta de un cliente de la nube, así como los riesgos vinculados con un incumplimiento de la provisión de los servicios, tales como una interrupción de los servicios de informática en la nube o de la conectividad y la pérdida de datos.

En ambos casos los riesgos pueden ser resultado de acciones u omisiones del proveedor de servicios o de circunstancias fuera de su control.

Estos problemas se plantean cada vez con mayor frecuencia y, a la vez, resultan más complejos, habida cuenta de que muchos proveedores de servicios pueden alojar los datos de su cliente en cualquier país en el que opere, apareciendo un elemento extranjero en la relación contractual. Al aparecer este elemento puede que más de un Tribunal tenga competencia para conocer del asunto en cuestión y, además, que la relación jurídica pueda quedar supeditada a varias leyes.

18 A. RODRÍGUEZ BENOT (Dir.): *Manual de derecho internacional privado*, 9ª Ed., Tecnos, 2022, p. 23.

19 FERNÁNDEZ ROZAS, J.C.; SÁNCHEZ LORENZO, S.: *Derecho internacional privado*, 13ª ed, Cizur Menor, Aranzadi, 2022, p. 24. A ello ya se refirió J.A. Carrillo Salcedo señalando que no todo elemento extranjero convierte una situación en una manifestación de la vida internacional de las personas, pues lo que realmente importa es que "la finalidad social de los hechos reclame una reglamentación que corresponda a esa internacionalización" (*Derecho internacional privado*, 3ª ed., Madrid, Tecnos, 1983, p. 39).

Lo anterior tiene sentido si pensamos que en internet tienen los datos su entorno²⁰ y los diferentes estados de los datos, en nuestra opinión, son:

Datos en reposo o almacenamiento: cuando se almacenan en una ubicación física o virtual y no se accede a ellos, no se procesan ni se utilizan. En principio, están en un dispositivo de almacenamiento, en un físico o virtual, de algún tipo y no se mueven a través de la red.

Datos en movimiento o de comunicación o contenido: tienen lugar cuando los datos se transmiten, transfieren o envían a través de un medio, canal, red u otro medio de comunicación.

Datos en uso o procesados: son los que se sitúan donde actualmente se accede a los datos, se procesan, se utilizan o se someten a algún tipo de cálculo u operación.

Además, de los anteriores, podemos considerar extrapolables a todo, se pueden observar datos que son relevantes para el cifrado, que incluyen los metadatos, y que son cualquier dato informático relativo a una comunicación por medio de un sistema electrónico, generado por el mismo y que forma parte de la cadena de comunicación, indicando el origen, destino, ruta, hora, fecha, tamaño de la comunicación, duración o tipo de servicio subyacente.

A lo anterior debe sumarse, que la tecnología a la que hacemos referencia, como todas, tienen su valor en los datos, que no solo abarcan una serie de etapas diferentes en el control y el procesamiento de los datos, sino que también involucra a una diversa gama de actores, que están ubicados, por la propia naturaleza de internet, en diferentes Estados. Esos diferentes actores son, entre otros²¹:

El generador de los datos, una máquina o un sensor, así como los datos que se generan a partir de otros datos. Aquí podemos situar a los nodos

El sujeto de los datos o persona a quien se refieren los datos.

El proveedor de los datos o persona que suministra los datos, incluida la persona que proporciona los datos que se ponen en común en una plataforma en línea

El receptor de los datos o la persona que recibe los datos, incluida la persona que accede a los datos que se ponen en común en una plataforma en línea.

20 DIZON, M. A.: "Laws of encryption: An emerging legal framework", *Computer Law & Security Review*, 43, 2021, pp. 1-19.

21 CNUDMI: *Cuestiones jurídicas relacionadas con la economía digital: las operaciones de datos*, Nueva York, 6 a 17 de julio de 2020.

El procesador de los datos o la persona que procesa los datos, independientemente de que los genere o los reciba.

El operador de la plataforma de datos o persona que aloja los datos en una plataforma en línea.

Como podemos observar nos encontramos con cadenas de proveedores y otros agentes, tales como proveedores de infraestructuras o de comunicaciones²², por lo que resulta necesario disponer de directrices concretas, para identificar y distinguir los derechos y obligaciones correspondientes de los controladores y procesadores que trabajan para los proveedores de servicios en la nube, o los agentes de la cadena de valor²³; pues, la naturaleza específica de la computación en nube, plantea cuestiones sobre ley aplicable en caso de infracción, por ejemplo, cuando se trate de usuarios de fuera de la UE, o de proveedores de fuera de la UE, cuando utilicen equipos que funcionen en la UE. En este sentido, es posible que los factores tradicionales no puedan ser fácilmente identificados en el caso de un determinado contrato. Ante esto, se plantea un riesgo importante, que consiste en ver cómo la responsabilidad se diluye respecto de las operaciones llevadas a cabo por los proveedores de servicios, si los criterios de aplicabilidad de la legislación no están lo suficientemente claros, motivo por el que pensamos en la necesidad de plantear posibles soluciones al problema de ley aplicable planteado.

Dicho lo anterior, supongamos que un cliente sube datos en a la nube, de un proveedor de servicios. Este cliente afirma que se ha violado su privacidad, en el sentido de que parte de esta información ha sido proporcionada por el proveedor de servicios a terceros. ¿Qué deberá hacer para emprender acciones legales contra el proveedor del servicio? En este contexto, debe tenerse en cuenta la relación contractual de la que debe partirse, para determinar las principales cuestiones que podrían plantear los contratos de computación en la nube firmados por entidades mercantiles, en los que una de las partes (el proveedor) proporciona a la otra (el cliente) uno o más servicios para un usuario final.

2. La determinación de la ley aplicable en supuesto de responsabilidad contractual.

Cabe argumentar que la provisión de los datos cargados por un proveedor de servicios fue una vulneración contractual que existía entre el cliente y el proveedor del servicio, resultando aplicable el Reglamento 598/2008 del Parlamento Europeo

22 CNUDMI: Aspectos contractuales de la computación en la nube, Nueva York, 24 a 28 de abril de 2017, p. 4.

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

y del Consejo, de 17 de junio de 2008, sobre la ley aplicable a las obligaciones contractuales (Roma I).

Deberá tenerse en cuenta la libertad de elección de la ley aplicable (Artículo 3,1), que evitará controversias entre las partes en torno a la cuál es la Ley del contrato, facilitando la elección del Derecho material más adecuado al interés de las partes. Esta elección deberá manifestarse expresamente o resultar de manera inequívoca de los términos del contrato o de las circunstancias del caso.

Probablemente, el contrato incluirá una cláusula de elección de la ley por la que se regirá y, además, vendrá impuesta por el propio proveedor de servicios. Esta cuestión es respetada por el Reglamento a través de su Artículo 3,3 al determinar que “cuando todos los demás elementos pertinentes de la situación estén localizados en el momento de la elección en un país distinto de aquel cuya ley se elige, la elección de las partes no impedirá la aplicación de las disposiciones de la ley de ese otro país que no puedan excluirse mediante acuerdo”. De esta forma, la Ley aplicable al contrato será limitada por las normas imperativas del país con el que el contrato está objetivamente vinculado (por ejemplo, el Reglamento General de Protección de Datos).

Esta solución sintoniza con un entorno globalizado, como la red, permitiendo que los contratos objetivamente internos se regulen por Leyes extranjeras si los contratantes estiman que resulta útil, y al mismo tiempo permite estandarizar el régimen jurídico de los contratos que celebra una empresa de carácter objetivamente internacional, como el de CC.

Por otro lado, debe tenerse en cuenta el tipo de contrato ante el que nos encontramos, Estos contratos, evidentemente, estarán influenciados por el tipo de servicios de computación en la nube de que se trate (por ejemplo, IaaS, PaaS o SaaS), de su modelo de despliegue (por ejemplo, público, compartido, privado o híbrido) y de las condiciones de pago (con o sin remuneración), que para su comparación nos remitimos a lo manifestado en el apartado anterior.

Lo comentado, nos sitúa fuera del ámbito de los tipos de contratos reflejados en el artículo 4,1 del Reglamento, lo que nos debe llevar a la residencia habitual de la parte que deba realizar la prestación característica del contrato o que resulte claramente que el contrato presenta vínculos manifiestamente más estrechos con otro país.

Este hecho puede llevar al Tribunal a tener en cuenta la verdadera intención de las partes, las circunstancias del caso o las costumbres o prácticas comerciales. No obstante, en un entorno virtual ¿cuál es el lugar donde el contrato fue negociado

y firmado? ¿En qué lugar está previsto que el contrato sea ejecutado? ¿Dónde se encuentra la sede del proveedor de servicios de informática en la nube?

En este contexto, en nuestra opinión, resultaría acertado plantear la identidad electrónica como un criterio de conexión, en tanto que guarda relación con la residencia, en este caso electrónica²⁴, en tanto que la necesidad de vincular la información y su manejo, únicamente, con quien la emite se hace esencial para numerosas interacciones diferentes: una infraestructura organizativa (gestión de la identidad) y una infraestructura técnica (sistemas de gestión de identidad), para desarrollar, definir, designar, administrar y especificar los niveles de autorización, asignando roles y atributos de identidad relacionados con grupos específicos de personas, como los administradores de la sociedad, los empleados o los clientes²⁵.

Con ello nos referimos a que la identidad electrónica, es una identidad que se compone de información almacenada y transmitida a los distintos usuarios de ésta. Pensemos que la identidad es un elemento fundamental, que vincula la información a su propietario, localizado en algún Estado dando lugar su localización, y, por tanto, al buen manejo efectivo y seguro de los datos específicos que dan entrada a la nube. Debemos tener presente que todos los esquemas de identidad electrónica dependen de dos procesos: primero, autenticación de identidad y, posteriormente, verificación de identidad. Cuando se autentica, la identidad se registra en el sistema y luego se puede usar para realizar transacciones. La identidad se verifica en el momento de cada transacción, desde dentro de la propia nube. De la información registrada en ese momento, surge la información de identificación o que va a identificar a la persona, tal y como si fuera la firma, que se usará, posteriormente, para vincular a un individuo de manera inseparable.

Observamos, que dentro de la nube se producirán dos elementos que se unirán para facilitar la identidad de la persona que pretende acceder a la nube. Estos dos elementos fundamentalmente son: la identidad fijada al individuo y otra fijada a la propia transacción que se realiza²⁶. La primera, será la que identifique a las partes y, por tanto, tendrá un efecto directo sobre la formación y la exigibilidad del contrato, determinando así su capacidad para obligarse contractualmente, al incluir elementos tales como el nombre de la persona jurídica, su forma legal, su número de inscripción en el registro (si procede), su domicilio social o dirección

24 DIAGO DIAGO, M^a.: "La residencia digital como nuevo factor de vinculación en el Derecho Internacional Privado del Ciberespacio ¿posible conexión de futuro?", *Diario LA LEY*, núm. 8432, 2014, p. 2.

25 MERCHÁN MURILLO, A.: "Identidad electrónica: necesidad de un entorno transfronterizo de confianza" en *Derecho mercantil y tecnología* (Dir. MADRID PARRA, A.), Thomson Reuters Aranzadi, 2018, pp. 181-183.

26 Resulta interesante el servicio de e-Residencia creado en Estonia. El servicio está dirigido, principalmente, a aquellos que ya tienen vínculos con Estonia, ya sea a través de negocios, estudios o por turismo. Se trata de plataforma que proporciona y utiliza servicios digitales en todo el mundo. Con ello, se espera que el e-residente atraiga a nuevos clientes a los servicios digitales de Estonia. (Véase, CUTHBERTSON, A.: "Estonia First Country to Offer E-Residency Digital", *International Business Times*, octubre, 2014).

del centro de negocios, junto con la mención de sus documentos fundacionales. La segunda, sería el cuerpo más grande de la información de la transacción y que se actualiza continuamente, en función de las transacciones que realice en la nube.

Si lo anterior no fuera suficiente, habrá que apreciar el contrato en concreto y las vinculaciones específicas, de dicho contrato, con los distintos países atendiendo, como indica el TJUE, en su Sentencia de 23 de octubre de 2014, asunto C-305/13, a la “apreciación global de la totalidad de los elementos objetivos que caracterizan la relación contractual y apreciar el elemento o elementos que, a su juicio, son más significativos” y “en el supuesto de que se alegue que un contrato presenta lazos más estrechos con un país que no sea el país cuya ley venga designada en virtud de la presunción que establece dicho apartado, el juez nacional deberá comparar los lazos existentes entre el contrato y el país cuya ley venga designada en virtud de la presunción, por una parte, y entre el contrato y el otro país de que se trate, por otra. El juez nacional deberá tener en cuenta todas las circunstancias que concurran, incluida la existencia de otros contratos relacionados con el contrato en cuestión”²⁷.

De esta forma, deben tenerse en cuenta todos los elementos de contactos del contrato en cuestión y de la situación contractual; pues, como indican CALVO CARAVACA Y CARRASCOSA GONZÁLEZ, “el Reglamento Roma I no contiene una tabla cerrada de contactos, ni precisa la importancia de estas, ni dicha importancia es necesariamente estable, pues depende del caso concreto. Por tanto, cuentan todos los contactos del contrato con los diferentes países”²⁸.

Atendiendo al conjunto de circunstancias del contrato destaca un sobre todas ellas: la ubicuidad de las partes; es decir, el acceso a la red desde cualquier ubicación. Este aspecto es importante pues es lo que va a determinar la ley aplicable a en materia de datos personales, datos contables y datos del sector público, así como el control de las exportaciones que pueden limitar la transmisión de determinados datos o programas informáticos a ciertos países e incluso pueden derivarse de obligaciones contractuales, por ejemplo, de las licencias de propiedad intelectual que pueden llegar a exigir que el contenido bajo licencia se aloje en los servidores seguros del propio usuario. Asimismo, establecer requisitos de ubicación de los datos puede resultar deseable por meras razones prácticas, entre ellas, para aumentar la latencia²⁹.

27 STJUE de 23 de octubre de 2014, *Haeger & Schmidt GmbH y Mutuelles du Mans assurances IARD (MMA IARD), Jacques Lorio, Dominique Miquel, en calidad de administrador concursal de Safraim intercontinental SARL, Ace Insurance SA NV, Va Tech JST SA, Axa Corporate Solutions SA*, asunto C305/13, apartados 49 y 51.

28 CALVO CARAVACA, A-L.; CARRASCOSA GONZÁLEZ, J.: *Derecho Internacional Privado*, vol. II, 18ª ed., Comares, Granada, 2018, p. 1004.

29 Debe observarse que la latencia tiene su importancia desde un punto de vista contractual y extracontractual, en tanto en cuanto desde la perspectiva del cliente va a medir la demora entre la solicitud del usuario y la respuesta del proveedor, afectando de pleno al servicio de CC.

Una presunción a favor de la ubicación sería la indicación que da el propio prestador de servicios sobre su establecimiento, entendiendo éste como el lugar donde una parte mantiene un centro de operaciones no temporal³⁰, para realizar una actividad económica distinta del suministro transitorio de bienes o servicios desde determinado lugar. En caso de que el prestador tuviera más de un establecimiento podría determinarse a través de la que la relación más estrecha con el contrato pertinente, habida cuenta de las circunstancias conocidas o previstas por las partes en cualquier momento antes de la celebración del contrato o al concluirse éste³¹, refiriéndonos con ello sólo a la relación más estrecha del contrato.

Esta presunción resulta más razonable que la de determinar un factor de conexión la ubicación del equipo y la tecnología, ya que, si bien puede ser criterio para determinar los vínculos más estrechos, no necesariamente es el más importante, entre otras cosas porque es más que rebatible y no es absoluta al poder llevar aparejadas situaciones de fórum shopping.

Por otro lado, si centramos nuestra atención en la referencia al sistema de información utilizados en el curso de una comunicación para negociar el contrato y suministrar los bienes y servicios, se puede determinar la ubicación del establecimiento de la empresa, englobando con ello a todos los proveedores de servicios de información y los servidores web, aun cuando no guardaran relación alguna con las partes que hubieran negociado el contrato.

La referencia combinada al contrato y a su cumplimiento, tal y como se establece en la actualidad en el Reglamento, puede crear incertidumbre al poder plantearse situaciones en que un determinado establecimiento de una de las partes guardara una relación más estrecha con el contrato, pero otro establecimiento de la misma parte tuviera un vínculo más estrecho con el cumplimiento del contrato. Estas situaciones no son inhabituales en los contratos celebrados por grandes empresas transnacionales y pueden volverse incluso más frecuentes a raíz de la actual tendencia a una mayor descentralización de las actividades comerciales³².

Otro aspecto que debe ser tenido en cuenta en relación con el régimen contractual es la interrupción o corte del servicio relativamente prolongados durante las horas normales de trabajo, aun cuando se trate de un servicio prestado ininterrumpidamente. También puede tener otros efectos negativos, como el tener que realizarse cambios en las aplicaciones del cliente o en sus sistemas informáticos,

30 El concepto de centro “no temporal” califica a la palabra “establecimiento” (Véase, CNUDMI: *Nota explicativa de la Secretaría de la CNUDMI sobre la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales*, Nueva York, 2007, p. 45).

31 Véase el Artículo 6,2 de la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales.

32 CNUDMI: *Nota explicativa de la Secretaría de la CNUDMI sobre la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales*, Nueva York, 2007, p. 47.

que impidan el acceso al servicio, o las cuestiones relativas a interrupciones en la conexión a Internet. De esta forma, atendiendo a que el proveedor procurará por mantener los servicios disponibles las 24 horas del día, 7 días a la semana o que el período de disponibilidad del servicio alcance el 100%, pero sin garantizarlo, podríamos estar ante acuerdos que podrían determinar pérdidas financieras para la empresa cliente y el usuario final, lo que se encuadraría, en nuestra opinión, dentro de un posible enriquecimiento injusto.

Asimismo, podríamos encontrarnos en situaciones en las que las partes intervienen en desigualdad de condiciones, las leyes aplicables sobre contratos suelen establecer que el contrato en cuestión es un contrato de adhesión. Los proveedores de servicios suelen estar familiarizados con un número limitado de leyes locales y especialmente con las leyes locales que gobiernan los contratos y el derecho a la privacidad³³. Por esa razón procederán a elegir una ley aplicable que establezca los requisitos relativos a la protección de la información que el proveedor de servicios en cuestión pueda o esté dispuesto a cumplir, lo cual ofrece reglas para la elaboración de contratos que son predecibles y aceptables para sus fines.

Estas cuestiones pueden obligar a la empresa cliente a asumir ciertas responsabilidades frente a sus usuarios finales en relación a la determinación de la Ley aplicable tipo, pudiendo ser ésta abusiva. Ante esto, como indica la Sentencia del TJUE, de fecha 28 de julio de 2018, asunto C-191/15, al apreciar el carácter abusivo de una determinada cláusula contractual en el marco de una acción de cesación, del artículo 6, apartado 2, del Reglamento Roma I, resulta que la elección de la ley aplicable se hace sin perjuicio de la aplicación de las disposiciones imperativas previstas por la ley del país en el que residen los consumidores cuyos intereses son defendidos mediante esa acción. Entre tales disposiciones pueden figurar las que transponen la Directiva 93/13, siempre que garanticen un nivel de protección más elevado para el consumidor³⁴. En este punto, el principal riesgo de índole jurídica que se plantea para la empresa cliente es no poder evaluar plenamente los riesgos vinculados con el contrato, por ejemplo, desconocimiento de los puntos débiles inherentes a la tecnología que está siendo utilizada; funciones de seguridad que faltan o son inadecuadas; riesgos económicos vinculados con las pérdidas de datos o incumplimientos de lo pactado, etc.

33 CNUDMI: *Propuesta del Gobierno del Canadá: posible labor futura en materia de comercio electrónico: cuestiones jurídicas que afectan a la informática "en la nube"*, Nueva York, 7 a 18 de julio de 2014, p. 2.

34 STJUE, de fecha 28 de julio de 2018, *Verein für Konsumenteninformation contra Amazon EU Sàrl*, asunto C-191/15 (ECLI:EU:C:2016:612), apartado 59.

VI. CONCLUSIONES.

Los Smart contracts o contratos inteligentes plantean cuestiones importantes que deben llevar a examinar las cuestiones jurídicas que afectan al suministro de servicios, ante el aparente desequilibrio que se presenta entre los derechos y las obligaciones de los participantes en un contrato de informática en la nube u otras evidencias, todo ello con vistas a mejorar el comercio internacional.

De esta forma, surge la necesidad de analizar y profundizar en un marco jurídico adecuado, para que tanto los ciudadanos como las empresas puedan confiar en la tecnología con la que interactúan, disponer de un entorno jurídico predecible y contar con la garantía efectiva de que van a protegerse sus derechos y libertades.

En este contexto, debe prestarse especial atención a las cuestiones relacionadas con la Ley aplicable a estos contratos. Pues conllevarán problemas en los que es posible que los factores tradicionales pueden no ser suficientemente fáciles de identificar. Por ello, planteamos la necesidad de revisar determinados criterios para evitar que la responsabilidad se diluya respecto de las operaciones llevadas a cabo por los proveedores de servicios, si los criterios de aplicabilidad de la legislación no están lo suficientemente claros.

BIBLIOGRAFIA

BURDEN, K.: "Eu Update", *Computer Law & Security Review*, Vol. 34, Núm. 2, Abril, 2018, pp. 409-418.

CALVO CARAVACA, A-L.; CARRASCOSA GONZÁLEZ, J.: *Derecho Internacional Privado*, vol. II, 18ª ed., Comares, Granada, 2018.

CNUDMI, *Cuestiones jurídicas relacionadas con la economía digital: las operaciones de datos*, Nueva York, 6 a 17 de julio de 2020.

CNUDMI: *Aspectos contractuales de la computación en la nube*, Nueva York, 24 a 28 de abril de 2017.

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

CNUDMI: *Labor prevista y posible labor futura: parte cuarta Propuesta del Gobierno del Canadá: posible labor futura en materia de comercio electrónico: cuestiones jurídicas que afectan a la informática "en la nube"*, Viena, 29 de junio a 16 de julio de 2015.

CNUDMI: *Nota explicativa de la Secretaría de la CNUDMI sobre la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales*, Nueva York, 2007.

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

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

CUTHBERTSON, A.: "Estonia First Country to Offer E-Residency Digital", *International Business Times*, octubre, 2014.

DIAGO DIAGO, Mª.: "La residencia digital como nuevo factor de vinculación en el Derecho Internacional Privado del Ciberespacio ¿posible conexión de futuro?", *Diario LA LEY*, núm. 8432, 2014.

DIZON, M. A.: "Laws of encryption: An emerging legal framework", *Computer Law & Security Review*, 43, 2021, pp. 1-19.

EENMAA-DIMITRIEVA, H.; SCHMIDT-KESSEN, J.: "Creating markets in no-trust environments: The law and economics of smart contracts", *Computer Law & Security Review*, núm. 35, 2019, pp. 69-88.

FERNÁNDEZ ROZAS, J.C.; SÁNCHEZ LORENZO, S.: *Derecho internacional privado*, 13ª ed, Cizur Menor, Aranzadi, 2022.

FINCK, M.: "Blockchains and Data Protection in the European Union", *European Data Protection Law Review*, 4 (1) (2018), pp. 17-35.

GRAFF, T. J.: "From old to new: From internet to smart contracts and from people to smart contracts", *Computer Law & Security Review*, núm. 35, octubre, 2019.

GREENSPAN, A.: "Gideon. Smart contracts: The good, the bad and the lazy", *Private blockchains, Smart contracts*. 2015. Disponible en: <https://www.multichain.com/blog/2015/11/smart-contracts-good-bad-lazy/>

LENNART, A.: "Smart contracts on the blockchain – A bibliometric analysis and review", *Telematics and Informatics*, núm. 57, marzo 2021.

MERCHÁN MURILLO, A.: "Identidad electrónica: necesidad de un entorno transfronterizo de confianza" en *Derecho mercantil y tecnología* (Dir. MADRID PARRA, A.), Thomson Reuters Aranzadi, 2018.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), U. S. Department of Commerce: *The NIST Definition of Cloud Computing - Recommendations of the National Institute of Standards and Technology*, Septiembre, 2011.

POLITOU, E.; CASINO, F.; ALEPIS, E.; C. PATSAKIS, C.: "Blockchain Mutability: Challenges and Proposed Solutions", *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2019, pp. 1-13.

RODRÍGUEZ BENOT, A. (Dir): *Manual de derecho internacional privado*, 9ª Ed., Tecnos, 2022.

SHOJAIEMEHRA AMIR, B.; RAHMANIA NOORULDEEN, M.; Qader, N.: "Cloud computing service negotiation: A systematic review", *Computer Standards & Interfaces*, vol., 2018, pp, 196-206

SURDEN, H.: *Computable Contracts*, University of California, 2012, Vol. 46.

SZABO, N.: *Smart contracts Go to reference in article*, 1994.

VIGUERA REVUELTA, R.: "Los contratos informáticos", *Revista de la Contratación Electrónica*, núm. 97, 2008, p. 61

