

LA IDENTIDAD DIGITAL EN LA CONTRATACIÓN
ELECTRÓNICA: UNA MIRADA DESDE EL DERECHO
INTERNACIONAL PRIVADO

*DIGITAL IDENTITY IN ELECTRONIC PROCUREMENT: A VIEW FROM
PRIVATE INTERNATIONAL LAW*

Actualidad Jurídica Iberoamericana N° 16, febrero 2022, ISSN: 2386-4567, pp. 1386-1411



Antonio
MERCHÁN
MURILLO

ARTÍCULO RECIBIDO: 15 de noviembre de 2021

ARTÍCULO APROBADO: 10 de enero de 2022

RESUMEN: La identidad electrónica es un componente importante en la contratación electrónica. Por ello, en este artículo se pretende hacer un estudio partiendo del marco normativo existente. Todo ello, nos va a llevar, como decimos, a reflexionar acerca de los debates que surgen en torno a la identidad digital en la contratación electrónica, especialmente, el enfoque lo daremos desde una mirada del derecho internacional privado.

PALABRAS CLAVE: Contratación electrónica; Identidad digital; Responsabilidad; Competencia judicial; Ley aplicable.

ABSTRACT: *Electronic identity is an important component in electronic procurement. Therefore, this article aims to make a study based on the existing regulatory framework. All this will lead us, as we say, to reflect on the debates that arise around digital identity in electronic procurement, especially, the focus will be given from a perspective of private international law.*

KEY WORDS: *Electronic contracting; Digital identity; Responsibility; Judicial competence; Applicable law.*

SUMARIO.- I. INTRODUCCIÓN. II. EL ENCAJE NORMATIVO DE LA IDENTIDAD ELECTRÓNICA. 1. El primer enfoque normativo. 2. Evolución del Modelo Normativo. 3. Desarrollo normativo final. III. EL MARCO NORMATIVO PARA LA DETERMINACIÓN DE LA COMPETENCIA Y LA LEY APLICABLE. IV. LA APLICABILIDAD DE LA CONVENCION SOBRE LA UTILIZACION DE LAS COMUNICACIONES ELECTRONICAS EN LOS CONTRATOS INTERNACIONALES COMO ASPECTO RELEVANTE. V. CONCLUSIONES.

I. INTRODUCCIÓN

Un elemento importante en la contratación electrónica, que a veces se pasa por alto, es la identidad digital (en adelante, e-ID). No debemos olvidar que toda transacción cumple tres funciones: identificación, autenticación de la identificación y autorización/autenticación de la transacción.

En todo proceso de contratación interesa todo lo relacionado con la identidad de las partes que emiten su voluntad y la confidencialidad de sus datos personales, la existencia y validez de sus declaraciones de voluntad, la autoría e integridad de sus mensajes electrónicos y el no rechazo del mensaje en su origen y destino, lo que concierne a su seguridad y validez jurídica y existencia del documento electrónico, así como su autenticación a través de la firma electrónica; pues, todo ello va a constituir la prueba electrónica en sí. Con todo, puede decirse que a través de la e-ID se va a garantizar: que la persona que va a firmar es quien dice ser; ya que puede probarlo, así como la capacidad de obrar y la libertad de la actuación, a la hora de asumir el contenido del documento.

En el contexto que describimos, la e-ID puede observarse como 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, en la contratación electrónica; pues, con fecha 3 de junio de 2021, la Comisión ha presentado una propuesta de modificación del Reglamento eIDAS, que incluye la tecnología Blockchain para las e-ID.

Habida cuenta de lo anterior, surge la necesidad de estudiar su problemática desde el punto de vista del Derecho Internacional Privado, especialmente, cuando en la contratación se utiliza la tecnología Blockchain.

Lo haremos planteando la e-ID como un criterio de conexión, para determinar tanto la competencia judicial internacional como la ley aplicable, ya que la e-ID

• **Antonio Merchán Murillo**
Prof. Ayudante doctor.
Universidad Pablo de Olavide

va a guardar relación bien con el domicilio del demandado o residencia habitual, 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 en las que se da 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 las partes contratantes, así como los administradores de la sociedad, los empleados o los clientes².

Debemos tener presente que todos los esquemas de e-ID 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. Así, se producirán dos elementos que se unirán para facilitar la identidad de la persona que pretende acceder a la plataforma. Estos dos elementos fundamentalmente son: la identidad fijada al individuo y otra fijada a la propia transacción que se realiza. Todo ello, nos va a llevar, como decimos, a reflexionar acerca de los debates que surgen en torno a la identidad digital en la contratación electrónica, especialmente, el enfoque lo daremos desde una mirada del derecho internacional privado.

II. EL ENCAJE NORMATIVO DE LA IDENTIDAD ELECTRÓNICA

Como sabemos, el comercio electrónico genera incertidumbres derivadas, entre otras cuestiones, de la naturaleza de los medios a través de los que se desenvuelve, lo que lleva a la búsqueda de soluciones, necesarias a fin de mitigar los riesgos e incertidumbres, inherentes a las transacciones por medios electrónicos, que permitan hablar de un comercio electrónico seguro.

El hecho de que la transmisión electrónica de datos no se circunscribe sólo al ámbito nacional, ha llevado a la UE a la búsqueda de soluciones, al observarse que la acción nacional, por sí sola, no era suficiente, para alcanzar los objetivos y lograr las metas fijadas en la estrategia Europa 2020.

-
- 1 DIAGO DIAGO, M^a. P., "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, pág. 2.
 - 2 CUTHBERTSON, A., "Estonia First Country to Offer E-Residency Digital," *International Business Times*, octubre, 2014

Con la Directiva 1999/93/CE sobre firma electrónica, si bien contemplaba la eficacia legal de las firmas electrónicas, las disposiciones nacionales realizaron interpretaciones divergentes y, al mismo tiempo, no aplicaron uniformemente las normas técnicas, que se introducían, lo que llevó, con el paso del tiempo, a revisar el marco normativo, para colmar las lagunas que había dejado la citada Directiva, como consecuencia del camino que había desarrollado el mercado de certificación, más heterogéneo y con más posibilidades que las existentes en el momento de su realización.

No obstante, un hecho se pone de manifiesto, el establecimiento de normas básicas comunes y, al mismo tiempo, una mejora del marco normativo para el establecimiento del Reglamento 910/2014, favoreciendo su desarrollo.

Con el Reglamento 910/2014, que deroga la Directiva, si bien mantiene las mismas conceptualizaciones las rediseña, fabricándose una profunda transformación del modelo previo, con una orientación que pretende ofrecer un marco global transfronterizo e intersectorial para garantizar la seguridad, fiabilidad y sencillez de las transacciones electrónicas que incluya la identificación, la autenticación y la firma electrónicas.

De esta forma, la experiencia aprendida ha permitido tomar conciencia en Europa de la necesidad de adoptar este nuevo marco regulatorio e ir más allá de lo que, esencialmente, regulaba la Directiva, sólo la firma electrónica.

Asimismo, el propio Reglamento atribuye a la Comisión la posibilidad de adoptar, por un lado, actos delegados, actos que irán dirigidos a conseguir un alcance general, que completen o modifiquen determinados elementos no esenciales; y, por otro lado, actos de ejecución, con objeto de atribuir competencias de ejecución en los casos en que, de conformidad con el artículo 291 del TFUE, se requieran condiciones uniformes de ejecución de los actos jurídicamente vinculantes de la Unión.

I. El primer enfoque normativo

El 13 de diciembre de 1999 fue aprobada la Directiva 1999/93/CE, del Parlamento Europeo y del Consejo de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica; pues, como dice la propia Directiva en su Considerando cinco, “la comunicación y el comercio electrónicos requieren firmas electrónicas y servicios conexos de autenticación de datos. La heterogeneidad normativa en materia de reconocimiento legal de la firma electrónica y acreditación de los proveedores de servicios de certificación entre los Estados miembros puede entorpecer gravemente el uso de las comunicaciones electrónicas y el comercio electrónico”.

Con la Directiva se pretendía instaurar un marco comunitario sobre condiciones aplicables a la firma electrónica, de manera que aumente la confianza en las nuevas tecnologías y la aceptación general de las mismas. De esta forma, se trataba de armonizar la legislación de los Estados miembros en este ámbito para, no obstaculizar la libre circulación de bienes y servicios en el mercado interior; asimismo, se hizo preciso promover la interoperabilidad de los productos de firma electrónica de conformidad con el Artículo 14 del Tratado; el mercado interior implica un espacio sin fronteras interiores, en el que esté garantizada la libre circulación de mercancías, debiendo satisfacer los requisitos esenciales de los productos de firma electrónica, para fomentar la confianza en la citada firma electrónica.

Sin embargo, la Directiva sobre la firma electrónica si bien ha tenido como resultado un cierto grado de armonización en Europa, los Estados, en su transposición al derecho interno, han establecido marcos jurídicos distintos, que hacían imposible, en la práctica, realizar transacciones electrónicas transfronterizas.

Hay que tener presente que la normativa comunitaria de armonización resultaba un marco que permitía la existencia de divergencias significativas entre las legislaciones de los Estados miembros. En este sentido puede mencionarse el artículo 3,2 de la Directiva que establecía que “los Estados miembros podrán establecer o mantener sistemas voluntarios de acreditación destinados a mejorar los niveles de provisión de servicios de certificación” o el artículo 3,7 que establecía que “los Estados miembros podrán supeditar el uso de la firma electrónica en el sector público a posibles prescripciones adicionales”. No obstante, hay que recordar, en referencia al artículo 3,2 que, en principio, en referencia a la firma electrónica reconocida, no había problema, en tanto que su contenido era uniforme en todos los Estados de la Unión Europea, pero la firma electrónica avanzada no lo era, lo que suponía una clara incertidumbre difícil de superar. Ante un control y una supervisión *ex post*, como dice la Directiva Europea “hasta que haya recaído la decisión positiva administrativa” (artículo 2,13 de la Directiva 1999/93/CE). Por otro lado, respecto al artículo 3,7 el uso de la firma electrónica en el ámbito público podía quedar supeditada a la cumplimentación de requisitos adicionales, siempre que estos requisitos fueran objetivos, proporcionados, no discriminatorios y solo puedan hacer referencia a características específicas de la aplicación de que se trate.

El ámbito de aplicación en el espacio de las diversas legislaciones nacionales, en materia de firma electrónica, adoptadas en transposición de la Directiva 1999/93/CE, quedaba directamente condicionado por lo dispuesto en el artículo 4.1 de ésta, en lo que se refiere a la prohibición expresa de someter al prestador de servicios de certificación a servicios de autorización previa, ya que realizará sus

funciones en régimen de libre competencia y prohibiendo la imposición de cualquier restricción procedente de cualquier Estado miembro del Espacio Económico Europeo. Dicha prohibición se sustenta en el respeto a los principios del país de origen y reconocimiento mutuo de las legislaciones internas de los Estados miembros, comprendidas en el ámbito normativo, coordinado y consagrado por el legislador comunitario y nacional, en las normas sobre comercio electrónico y firma electrónica.

Asimismo, la Directiva recoge el principio de neutralidad tecnológica, pero da especial importancia a un tipo de firma, la firma electrónica reconocida; haciendo girar la equivalencia formal de los instrumentos en su seguridad; es decir, en su fuerza vinculante y probatoria, situando este principio en un plano superior al del principio de neutralidad tecnológica³.

De esta forma, se deduce que el efecto típico de la firma electrónica avanzada no es otro que el de crear una vinculación segura entre el firmante y el mensaje de datos y la de proteger el mensaje, pero sin que, en ningún caso, pueda equipararse esta firma a una firma manuscrita⁴. A pesar de esto, a las firmas electrónicas simples y avanzadas no se les negarán efectos, o lo que es lo mismo, deben tener efectos jurídicos según el apartado segundo del Artículo 5, pero si se podrán negar efectos si no pueden considerarse suficientemente seguras o si no permiten establecer un vínculo, suficientemente, fiable entre firmante y mensaje firmado. Aunque, es obvio que las causas, por las que se le pueden negar efectos a la firma electrónica avanzada, son inferiores a las casusas de la firma electrónica simple.

Al mismo tiempo, el Artículo 5,1 de la Directiva, recoge una firma electrónica especialmente fiable, la firma electrónica avanzada, basada en un certificado reconocido y creada por un dispositivo seguro de creación de firma, que equivale a la firma manuscrita, lo que se denomina como firma reconocida.

La firma electrónica reconocida se trata de un subtipo de la firma electrónica avanzada, caracterizada por un refuerzo de los requisitos de la firma electrónica avanzada; pues, se basa en un tipo especial de certificado (el reconocido) y necesita que la firma electrónica avanzada haya sido creada empleando un dispositivo seguro de firma electrónica. Al decir un subtipo firma electrónica avanzada, lo hacemos refiriéndonos a aquella generada por una persona física, no la jurídica. Siguiendo al Prof. Madrid Parra⁵, esto es una opción de política legislativa; pues,

3 ILLESCAS ORTIZ, R., *Derecho de la Contratación Electrónica*, Cizur Menor, 2019, p. 31.

4 CNUDMI/UNCITRAL, *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. 15.

5 MADRID PARRA, A., "Contenido esencial de la Ley Modelo de la CNUDMI/UNCITRAL sobre Documentos Transmisibles Electrónicos", *Revista Aranzadi de derecho y nuevas tecnologías*, ISSN 1696-0351, N°. 48, 2018, pp. 1-55.

se sigue el modelo de la firma manuscrita. La persona jurídica actúa a través de personas físicas, pero las consecuencias jurídicas se imputan a las personas jurídicas. Así pues, a efectos fiscales sería más operativo otorgar una firma electrónica a la persona jurídica que tiene su correspondiente código de identificación fiscal. Por ello, la ley española, para este concreto ámbito del derecho público, el legislador contempla la posibilidad de que el firmante sea una persona jurídica.

La aceptación transfronteriza de la firma electrónica solo se aplica al nivel reconocido, ya que el apartado segundo del Artículo 4 de la Directiva establece la libre circulación de los productos de firma electrónica, que se ajustan a lo dispuesto en la Directiva, lo que en la práctica significa ajustarse a los requisitos establecidos en los Anexos. La firma electrónica reconocida es un mecanismo de seguridad jurídica, emplea unas tecnologías que deben ofrecer unas garantías de calidad y seguridad elevadas, que de algún modo son "reconocidas" por los Estados miembros.

De esta manera, aparecen en la Directiva dos visiones diferentes de lo que debe ser la firma electrónica como equivalente de la firma manuscrita; o sea, establece una distinción entre dos tipos de firmas, las reconocidas y las demás, atribuyendo a las primeras unos efectos diferenciados. Por un lado, las firmas electrónicas reconocidas parten del hecho de que cumplen la misma función autenticadora que la firma manuscrita; por otro, las firmas electrónicas no reconocidas, plantean problemas y restricciones jurídicas, técnicas y organizativas. La Directiva define la firma electrónica avanzada de forma muy genérica, por lo que los Estados han utilizado sus Leyes para atribuirles efectos diversos con distintos niveles de seguridad, además, de imponer soluciones nacionales específicas para aplicaciones concretas, creando nuevos obstáculos al uso transfronterizo de la firma electrónica.

Por consiguiente, este estatus puede llevar a los Estados miembros, que solo están obligados a no negar efectos legales a la firma electrónica avanzada por el hecho de estar en formato electrónico, a gozar de un mayor margen de apreciación, en cuanto a la solución de firma electrónica avanzada, o simple, y a su aceptación o no. En definitiva, el reconocimiento legal de las firmas electrónicas, que no satisfacen los requisitos del Artículo 5,1 de la Directiva, dependerán de que se llegue a probar la fiabilidad y/o la seguridad del sistema de firma electrónica utilizado, mientras queda garantizado el reconocimiento de eficacia legal a la firma electrónica, que cumpla las exigencias enunciadas en el mencionado Artículo.

Las firmas electrónicas, contempladas en el Artículo 5,1, serán siempre equiparadas a las firmas manuscritas, cuyo juicio se ha realizado *ex ante* por el legislador. Por el contrario, la eficacia de las restantes firmas estará sometidas a un juicio *ex post*, que habrán de realizar los propios Tribunales a la espera de

determinar, si son suficientemente fiables atendidas las circunstancias y si garantizan la autenticidad e integridad del mensaje de datos o documento electrónico.

La Directiva ya venía asumiendo que los Estados limitarían la eficacia jurídica y formal por el hecho de no ser lo suficientemente segura. La Directiva en su Artículo 5,2 pide a los Estados que revisen sus Ordenamientos jurídicos, para que no se niegue la eficacia jurídica a la firma electrónica por el hecho de ser electrónica, porque no se base en certificado reconocido. Es este el motivo por el que no pide a los Estados que revisen su Derecho de contratos, y es que el Artículo 5 no puede entrar en cada uno de los supuestos en los que se exige la firma, supuestos que no son uniformes en las regulaciones europeas.

Por otro lado, la firma electrónica reconocida es el instrumento, a través del cual se intenta conseguir la homogeneidad necesaria, para la utilización de firmas electrónicas en negocios de tracto internacional; así como, la configuración de un servicio uniforme de prestación de servicios de certificación. De esta forma, se conjuga como el equivalente pleno de la firma manuscrita a nivel europeo, incluyendo exigencias capaces de asegurar las comunicaciones electrónicas. Esta firma sirve de equivalente de la firma para legislaciones más estrictas, las medidas de seguridad que implica exceden de la propia equivalencia funcional respecto de la firma tradicional, para constituirse en garante de las comunicaciones electrónicas.

Sin embargo, el uso de las firmas electrónicas reconocidas plantea problemas similares a los ya esbozados para las firmas no reconocidas, si bien la situación es mucho más compleja para las no reconocidas. La firma electrónica reconocida tiene un estatus jurídico dentro de la Directiva inequívoco y se espera con ella un uso transfronterizo claro, lo que se demuestra con la presunción de equivalencia con la firma manuscrita y la obligación jurídica de los Estados miembros de reconocer mutuamente los certificados reconocidos.

2. Evolución del Modelo Normativo.

Con la Directiva 1999/93/CE se aprecia que los mecanismos de firma electrónica típicamente utilizados en el ámbito del comercio electrónico, prácticamente, no fueron objeto de atención legislativa, así como que otros posibles mecanismos tecnológicos relevantes, para aportar seguridad al comercio electrónico, quedaron al margen de ese régimen legal. Asimismo, se observaron dificultades de aplicación o el carácter innecesario de ciertos requisitos legales, la inadecuación de algunas de las limitaciones previstas, o el carácter inviable de ciertos elementos básicos de la Directiva 1999/93/CE y de sus normas de transposición.

Por otro lado, se veían ciertas lagunas como la obligación no definida de la supervisión nacional de los proveedores de servicios. Además, se hizo hincapié

en que todos los países de la UE tenían marcos jurídicos para la firma electrónica, pero distintos lo que imposibilitan las transacciones electrónicas transfronterizas. Y lo mismo cabe decir respecto de los servicios de confianza, antiguos Prestadores de Servicios de Certificación, de las marcas de tiempo electrónicas, de las ventas y servicios de entrega electrónica y de la autenticación electrónica, que carecía de interoperabilidad europea.

Todo ello, entre otras cosas, motivó una profunda transformación del modelo previo, mediante la adopción del Reglamento (UE) nº 910/2014, de 23 de julio de 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.

El origen para su establecimiento debemos situarlo en el Tratado de Lisboa, firmado en esta ciudad, el 13 de diciembre de 2007, que entró en vigor el 1 de diciembre 2009, por el que se modifican el Tratado de la Unión Europea y el Tratado Constitutivo de la Comunidad Europea, y que, en gran parte, reproduce las innovaciones contenidas en el “fallido” Tratado que establecía una Constitución para Europa.

El Tratado de Lisboa sitúa la libertad, la justicia y la seguridad entre sus prioridades más importantes. Con ello, se quiere poner en práctica políticas en diversos campos: crecimiento económico y competitividad, desarrollo del empleo y las condiciones sociales, aumento de la seguridad personal y colectiva, fomento del medio ambiente y las condiciones sanitarias, desarrollo de la cohesión y la solidaridad entre los Estados miembros, en cuanto a progreso científico y tecnológico, además de mejorar su capacidad de actuación en la escena internacional⁶.

De modo más concreto, en el Tratado de Lisboa encontramos tres disposiciones legales que podrían invocarse para sostener la acción legal de la UE en el ámbito de la identificación electrónica, que son:

- a) Artículo 77 del Tratado de Funcionamiento de la Unión Europea (TFUE), que recoge la posibilidad de que la UE, en referencia a las políticas de fronteras, asilo, inmigración, etc. pueda establecer, con arreglo a un procedimiento legislativo especial, disposiciones relativas a los pasaportes, documentos de identidad, permisos de residencia o cualquier otro documento asimilado.
- b) Artículos 20 a 25 TFUE, en el que se recoge lo que podríamos denominar como el derecho de la ciudadanía europea. En efecto, la ciudadanía de la

6 MERCHÁN MURILLO, A., *Firma electrónica: funciones y problemática*, Pamplona, 2016, p. 212.

Unión se añade a la ciudadanía nacional sin sustituirla, lo que presupone la necesidad de crear un sistema de identificación dentro de la zona europea.

- c) Artículo 16 TFUE, donde se consagra que el derecho a la protección de datos de carácter personal, afirmando que las comunicaciones electrónicas y la protección de los datos personales se encuentran íntimamente conectadas.

Además, el Artículo 114 TFUE se refiere a la adopción de normas a fin de eliminar los obstáculos que dificultan el funcionamiento del mercado interior. A través de este precepto, se pretende que los ciudadanos, empresas y administraciones puedan beneficiarse del reconocimiento y la aceptación mutua de la identificación, autenticación y la firma electrónica y otros servicios de confianza través de las fronteras cuando resulte necesario para el acceso y la realización de procedimientos o transacciones electrónicos.

El citado Reglamento se presentó sobre la base de una propuesta emitida por la Comisión fundamentada en el citado Artículo 114 del TFUE, que se refiere a la adopción de normas a fin de eliminar los obstáculos que dificultan el funcionamiento del mercado interior. De esta manera, se considera que un Reglamento es el instrumento jurídico más apropiado. La aplicabilidad directa de un Reglamento en virtud del artículo 288 del TFUE reducirá la fragmentación jurídica y aportará mayor seguridad jurídica.

Con este Reglamento se viene a plantear un mercado único de la firma electrónica y los servicios de confianza en línea afines, más allá de las fronteras, asegurando que esos servicios funcionen y gocen del mismo estatuto jurídico que los trámites tradicionales en papel, dándose pleno efecto a los posibles ahorros propiciados por la contratación electrónica. Por otro lado, se pretende respetar los sistemas de identificación nacionales, así como las preferencias de los Estados miembros que no tienen sistemas nacionales de identificación, permitiendo a los países que si tienen sistemas de identificación electrónica optar por quedar fuera del sistema paneuropeo. Si un Estado miembro notifica que desea sumarse a este sistema deberá ofrecer el mismo acceso a los servicios públicos mediante la identificación electrónica que a sus propios ciudadanos. Así, se trata de dar un reconocimiento recíproco a las identificaciones electrónicas nacionales, a la vez que se quiere establecer normas comunes sobre los servicios de confianza y la firma electrónica. De esta forma, se pretende profundizar en la mejora de la legislación existente y en la ampliación del reconocimiento y la aceptación mutua, dentro de la Unión Europea, de los sistemas de identificación electrónica y otros servicios de confianza electrónicos conexos.

No obstante, no se obliga a los Estados miembros de la UE a introducir (ni a los individuos a obtener) documentos nacionales de identidad, tarjetas electrónicas de identidad u otras soluciones de identificación electrónica, ni introduce una identificación electrónica europea ni ninguna especie de base europea de datos, ni permite ni requiere que se comparta información personal con otras partes⁷.

Se aprecia así, el respeto de la soberanía nacional, al no imponer la obligación de que todos los ciudadanos de la UE tengan una identificación electrónica, aunque habría que considerar, como ha puesto el Comité Económico y Social Europeo, los beneficios de un sistema universal de identificación electrónica europea. Todo ello, con el objetivo de que los ciudadanos puedan disfrutar de una igualdad de oportunidades dentro de la UE.

Por ello, es importante asegurar la interoperabilidad transfronteriza en el seno de la UE de las identificaciones nacionales, así como el reconocimiento y aceptación mutuos entre los Estados miembros de los medios de identificación electrónica, para la ejecución de operaciones electrónicas sin fisuras que dependan de la identificación electrónica y la prestación de los servicios de confianza⁸.

El Reglamento parte de tres cuestiones fundamentales:

- 1) Mejorar el marco jurídico de la firma electrónica sustituyendo la Directiva vigente sobre la firma electrónica, impone una mayor responsabilidad por la seguridad y establece normas claras y estrictas para la supervisión de la firma electrónica y servicios relacionados
- 2) Imponer el requisito del reconocimiento mutuo entre diversos sistemas nacionales de identificación electrónica (artículo 6 del Reglamento).
- 3) Incluir los servicios de confianza, dejando claro el marco jurídico estableciendo a unos sólidos organismos de supervisión para los prestadores de servicios relacionados con ventas electrónicas, marcas de tiempo, aceptabilidad electrónica de documento, servicios de entrega electrónica y autenticación electrónica.

De esta forma, se promueve el uso de estándares de firma electrónica, tratando de centrarse en un área de aplicación menos compleja y, por tanto, más accesible. Estas recomendaciones son las de promover: la interoperabilidad entre Estados miembros de la UE, el reconocimiento legal de la aplicación de la firma

7 MADRID PARRA, A., "Seguridad, pago y entrega en el comercio electrónico", *Revista de Derecho Mercantil*, núm. 241, 2001, pp. 1189-1264.

8 SULLIVAN, C.: "Digital identity – From emergent legal concept to new reality," *Computer Law & Security Review*, 2018, vol. 34, núm. 4, pp. 723-731.

electrónica simple de acuerdo con la Directiva y un desarrollo sencillo en cualquier contexto empresarial. Unas aplicaciones accesibles son una condición *sine qua non* para su adopción⁹. Las aplicaciones para el uso de las firmas electrónicas deben cumplir con unos criterios de utilización estrictos, que los usuarios deberán ser capaces de usar, a través de su firma electrónica, sin complejidad.

3. Desarrollo normativo final

La profunda transformación del modelo previo destaca, en primer lugar, por el abandono como instrumento normativo de la Directiva y su sustitución por un Reglamento, al considerarse que un Reglamento es el instrumento jurídico más apropiado.

La aplicabilidad directa de un Reglamento, en virtud del artículo 288 del TFUE, reduce la fragmentación jurídica y aporta mayor seguridad jurídica, mediante la introducción de un conjunto armonizado de normas básicas, que contribuirán al buen funcionamiento del mercado interior. Todo ello, teniendo presente que el objetivo fundamental es mejorar la legislación existente y ampliarla, incluyendo el reconocimiento y la aceptación mutua, dentro de la UE, de los sistemas de identificación electrónica notificados y otros servicios de confianza electrónicos conexos esenciales

De esta forma, con la elección de este marco normativo, se trata de evitar la multitud de problemas causados por la Directiva, de reforzar la seguridad jurídica, de estimular la coordinación de la supervisión nacional, de garantizar el reconocimiento y la aceptación mutuos de los regímenes de identificación electrónica y de incorporar servicios de confianza conexos. Especial importancia tiene la identificación; pues, con el Reglamento se trata de suprimir los problemas de armonización causados por los diferentes sistemas nacionales de identificación electrónica.

Dicho lo anterior, tenemos presente que la naturaleza transnacional del Reglamento exige una acción de la UE. Con arreglo al principio de subsidiariedad (artículo 5, apartado 3, del TUE), la Unión sólo debe intervenir en caso de que los objetivos perseguidos, no puedan ser alcanzados de manera suficiente por los Estados miembros por sí solos, para que puedan alcanzarse mejor, debido a la dimensión o a los efectos de la acción pretendida, a escala de la Unión.

En cualquier caso, para entender el desarrollo emprendido del Reglamento 910/2014, hay que tener presente que no existe un mercado único digital; es decir, preexisten de 28 mercados digitales individuales, divididos y, hasta la fecha,

⁹ ALAMILLO DOMINGO, I, *Identificación, firma y otras pruebas electrónicas: la regulación jurídico-administrativa de la acreditación de las transacciones electrónicas*. Pamplona, 2019, p. 120.

no armonizados. No obstante, estos 28 mercados, como sabemos, son sistemas jurídicos aproximados, más aún, en la materia que tratamos, gracias a la Directiva.

Así, a la luz de estos problemas, se consideró, como decimos que, por sí solos, los Estados miembros no pueden mitigar los problemas que se plantean, en la situación actual, especialmente, los debidos a la fragmentación de las legislaciones nacionales. Por tanto, existe una necesidad específica de establecer un marco armonizado y coherente, con la intención de alcanzar los objetivos y metas fijadas en la *estrategia Europa 2020*¹⁰.

Asimismo, la Comisión consideró que la UE es la que está en mejores condiciones para garantizar de forma efectiva y coherente la interoperabilidad de la firma electrónica; pues, como sabemos, las medidas nacionales han creado barreras *de facto* a la citada interoperabilidad de la firma electrónica en la UE, y están teniendo, actualmente, el mismo efecto sobre la identificación electrónica, la autenticación electrónica y los servicios de confianza conexos, por lo que es necesaria la creación de un marco, que permita abordar la interoperabilidad transfronteriza y mejorar la coordinación, de los regímenes nacionales de supervisión¹¹.

Por lo anterior, se ha dotado a la Comisión de la potestad de adoptar actos delegados (artículo 47 del Reglamento) y de ejecución (artículo 52, b) y c) del Reglamento). Asimismo, A la hora de adoptar actos delegados o actos de ejecución, la Comisión debe tener en cuenta las normas y especificaciones técnicas elaboradas por organizaciones y organismos de normalización europeos e internacionales, en particular, el Comité Europeo de Normalización (CEN), el Instituto Europeo de Normas de Telecomunicación (ETSI), la Organización Internacional de Normalización (ISO) y la Unión Internacional de Telecomunicaciones (UIT), con vistas a garantizar un elevado nivel de seguridad e interoperabilidad, de los servicios de identificación electrónica y de confianza.

El procedimiento de ejecución de estos actos se contiene en el artículo 48, intitulado "Procedimiento de comité", que remite al Reglamento (UE) n° 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión, que establece las normas y principios generales, que regulan los mecanismos aplicables, en los casos en que un acto jurídicamente

10 ALAMILLO DOMINGO, I., "Firma y sello electrónicos: el porqué y el cómo de la implantación del nuevo reglamento europeo", *Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones*, N° 74, 2016, págs. 28-29.

11 CNUDMI/UNCITRAL, *Proyecto de disposiciones sobre el reconocimiento transfronterizo de sistemas de gestión de la identidad y servicios de confianza*, Nueva York, 5 a 9 de abril de 2021, p. 2.

vinculante de la Unión determine la necesidad de condiciones uniformes de ejecución y requiera que la adopción de actos de ejecución, por la Comisión esté sometida al control de los Estados miembros.

Estos actos van destinados a garantizar la disponibilidad de normas organizativas y técnicas, gestionar la información notificada por los Estados miembros, y, en particular, mantener la información relacionada con las listas de confianza, sensibilizar acerca de las ventajas de la utilización de la identificación, autenticación y firma electrónicas y los servicios de confianza conexos e iniciar conversaciones con terceros países con vistas a conseguir la interoperabilidad a nivel mundial en este ámbito.

En este sentido, puede decirse sé que se trabaja en la creación de un “espacio de confianza transfronterizo”¹² que signifique una combinación de condiciones jurídicas, organizativas y técnicas recomendadas por la propia UE. Todo ello con el objetivo de promover la investigación y cooperación, que permitan el uso eficaz de datos y software, en particular documentos y operaciones electrónicos, incluidos medios electrónicos de autenticación, el mejoramiento de los métodos de seguridad y, además, promover la confianza en un entorno electrónico en todo el mundo alentando las corrientes de información transfronterizas seguras, incluidos los documentos electrónicos y las actividades encaminadas a ampliar y reforzar la Infraestructura de la Información.

No obstante, si bien esos actos pueden ser necesarios, desde la perspectiva estatal, pueden provocar incertidumbre e inseguridad; pues, como se establece en el artículo 290 del Tratado de Funcionamiento de la Unión Europea y el Acuerdo Común del Parlamento Europeo: “el Parlamento Europeo o el Consejo podrán decidir revocar la delegación”, si lo consideran necesario.

Dicho lo anterior, decir que, con fecha 3 de junio de 2021, la Comisión Europea ha elaborado una Propuesta de Reglamento por el que se modifica el Reglamento eIDAS en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea, al considerarse que el Reglamento actual no consigue dar respuesta a estas nuevas demandas del mercado debido a las escasas posibilidades que tienen los prestadores privados en línea para conectarse al sistema, a la disponibilidad insuficiente de soluciones de identidad electrónica en todos los Estados miembros y a la falta de flexibilidad del sistema para admitir diversos tipos de casos de uso¹³.

12 CNUDMI: A/CN.9/WG.III/ WP.136 - *Solución de controversias en línea en las operaciones transfronterizas de comercio electrónico. Documento presentado por la Federación de Rusia*, Viena, 30 de noviembre a 4 de diciembre de 2015, págs. 3 y ss.

13 ALAMILLO DOMINGO, I., “El uso de los sistemas de identidad auto-soberana en el sector público español y de la unión europea”, *Blockchain intelligence*, 2019, pp. 1-22.

Entre las novedades del citado proyecto, se pretende desarrollar un Marco para una Identidad Digital Europea, mediante el uso de las de las tecnologías de registro distribuido (TRD), lo que será objeto de estudio más adelante, con el fin de crear un marco seguro para la identificación electrónica, para que todos las personas, físicas o jurídicas, puedan controlar sus propias interacciones, así como su presencia en línea.

III. EL MARCO NORMATIVO PARA LA DETERMINACIÓN DE LA COMPETENCIA Y LA LEY APLICABLE

Debe tenerse en cuenta que vamos a encontrarnos con cadenas de proveedores y otros agentes, tales como proveedores de infraestructuras o de comunicaciones, por lo que resulta necesario disponer de directrices concretas, para identificar y distinguir los derechos y obligaciones correspondientes de los controladores, conectores y procesadores que trabajan para los proveedores de servicios en la nube, los agentes de la cadena de valor, etc.¹⁴; pues, todo va a plantea cuestiones sobre competencia judicial internacional y sobre ley aplicable en caso de infracción, en supuestos de materia contractual o extracontractual, ya que el lugar de establecimiento pertinente de un prestador de servicios será difícil de determinar, 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 supuesto. Ante esto, el uso de los servicios va a plantear un riesgo importante, que consiste en ver cómo la responsabilidad se puede diluir 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.

En relación con el derecho preexistente serán relevantes los acuerdos atributivos de competencia incluidos en el contrato, en la medida en que sean eficaces conforme a las reglas de nuestro sistema de Derecho internacional privado, en este caso, centrémonos en los establecido en el Reglamento 1215/2012, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil.

Al margen de esas transacciones de las transacciones con consumidores, habrá que observarse la eventual incidencia de reglas especiales como la del artículo 25,2 Reglamento 1215/2012 con respecto a la forma escrita en la contratación electrónica;

¹⁴ 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, pág. 2 y 3.

pues, nos viene a indicar que “se considerará hecha por escrito toda transmisión efectuada por medios electrónicos que proporcione un registro duradero del acuerdo”, por lo que da un presupuesto de la eficacia de los acuerdos atributivos de competencia¹⁵. En este sentido, habrá que tener presente la posibilidad de aplicación del foro del artículo 7,1 del citado Reglamento, en relación con el foro especial en materia de contratos, pudiendo ser controvertida; pues, como indica el Prof. De Miguel Asensio¹⁶, habrá que determinar en qué medida la automatización de ciertas prestaciones condiciona la determinación del lugar de cumplimiento de la obligación a los efectos de esa norma¹⁷; pues, precisar esa cuestión no va a ser tarea sencilla ya que tendríamos que acudir al “método analítico distributivo”¹⁸, que ha sido precisado por el TJUE en muchas de sus sentencias, que en definitiva consiste en que es competente para conocer del litigio contractual el tribunal del lugar del Estado miembro en el que hubiere sido o debiera ser cumplida la obligación que sirve de base a la demanda, que será la obligación incumplida y para conectar el lugar de cumplimiento de dicha obligación debe aplicarse la Ley que regula el contrato según las normas de Derecho internacional privado vigentes en el Estado miembro cuyos tribunales conocen del asunto.

La complicación va a venir porque, en resumen, el original del contrato se reemplaza por su manifestación digital: un “token”; es decir, un “ficha” que tiene por función facilitar la efectividad de las transacciones y minimizar sus costos, sin que su naturaleza jurídica esté clara y/o determinada aún¹⁹. No obstante, habrá que determinar para cada caso si estamos ante tokens de pago (sinónimos de criptomonedas), tokens de utilidad (destinados a proporcionar acceso digital a una aplicación o servicio) o tokens de activos (representan activos, como la participaciones en compañías, un derecho a dividendos, etc.).

Siguiendo 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 entre las partes. Como no puede ser de otra manera, la base debemos asentarla en el Reglamento 593/2008 del Parlamento Europeo y del Consejo, de 17 de junio de 2008, sobre la ley aplicable a las

15 RODRÍGUEZ BENOT, A., “Acuerdos para la determinación del lugar de ejecución de las obligaciones contractuales y acuerdos atributivos de competencia en los convenios de Bruselas y de Lugano” en *La revisión de los Convenios de Bruselas de 1968 y Lugano de 1988 sobre competencia judicial y ejecución de resoluciones judiciales en materia civil y mercantil: una reflexión preliminar española. Seminario celebrado en Tarragona 30-31 de mayo de 1997*, Ed. Marcial Pons, Barcelona, pp. 165-197.

16 DE MIGUEL ASENSIO, P. A., *Derecho Privado de Internet*, Ed. Civitas, Madrid, 2015, pág. 445; DE MIGUEL ASENSIO, P. A.: *Blog de Derecho internacional privado*, Disponible en: <http://pedrodemiguelasensio.blogspot.com/search/label/Comercio%20electr%C3%B3nico>

17 CALVO CARAVACA, A. L., Carrascosa González, J., *Derecho Internacional Privado*, vol. II, 18ª ed., Comares, Granada, 2018, p. 908.

18 CALVO CARAVACA, A. L., Carrascosa González, J., *Derecho Internacional Privado*, cit., pp. 929-931.

19 SAVELYEV, A., *Some risks of tokenization and blockchainization of private law*, *Computer Law & Security Review*, vol. 34, Agosto, 2018, pp. 863-869.

obligaciones contractuales (Roma I), donde nos vamos a encontrar la problemática de determinar, si no hay acuerdo entre las partes la determinación de la Ley aplicable.

En este sentido, como decimos, 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).

Por otro lado, si las partes no han realizado cláusula de elección, habrá que tener en cuenta el tipo de contrato, que dependiendo del Estado en el que nos situemos puede llegar a calificarse de distinta forma e, incluso podremos encontrar distintos tipos de acuerdos de licencia de usuario final, términos de servicio y otros documentos similares que forman la base del marco contractual y que se han convertido en una parte integral de cualquier servicio o sitio web de Internet. Dichos contratos se utilizan principalmente para administrar los servicios, de uso del software, de despliegue, de condiciones de pago, etc. Resultando contratos mixtos o de cualquier otro tipo.

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? Cuestiones complejas ante la situación altamente tecnológica que se nos presenta. 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 relación a la cuestión procesal, por la *lex fori*²⁰, que también conlleva una problemática aparejada y cuyo debate excede este trabajo.

Además, es posible que debamos tener en cuenta el criterio de origen de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), en relación a que, como se indica en el Considerando 22 “El control de los servicios de la sociedad de la información debe hacerse en el origen de la actividad para garantizar que se protegen de forma eficaz los intereses generales” en relación con los aspectos contractuales incluidos en el ámbito coordinado.

Asimismo, habrá que tener en cuenta la capacidad para contratar y, por supuesto, no debemos olvidarnos de la protección de datos²¹, muy especialmente, todo lo relativo al régimen aplicable en materia de protección de datos personales²², en el que habrá que estar a lo dispuesto a los artículos 79,2 y 3 2016/679, 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. Ahora bien, habrá que observarse obligatoriamente una serie de cuestiones que, en ocasiones, no será fácil de determinar: que la accesibilidad de los servicios en el territorio de un Estado determinado pueda ser suficiente para aplicar el Reglamento; que la nacionalidad o la residencia del sujeto de los datos o de las partes contratantes, en especial del responsable de los datos, puedan dar lugar a la aplicación de la ley del sujeto de los datos o de alguna de las partes; y que la ley del lugar en que se originó la actividad (por ejemplo, la ubicación del equipo o el nodo) o a la que se orienta la actividad con fines de lucro haga que se aplique la ley de ese lugar. En este contexto, no debemos perder de vista 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, ya que va a tener una gran relevancia, como veremos más adelante para determinar la identidad electrónica como un criterio de conexión.

20 DE MIGUEL ASENSIO, P. A., *Derecho Privado de Internet*, cit., Cit., p. 464.

21 Debe hacerse una observación importante en relación con esta cuestión, pues son objeto de una protección legal especial en muchas jurisdicciones. La legislación aplicable al procesamiento de dichos datos puede ser diferente a la que se aplica al contrato y, en ese caso, invalidará las cláusulas contractuales no conformes con dicha legislación.

22 CARRASCOSA GONZALEZ, J., “La Directiva 95/46/CE: Entre la protección de la intimidad y la libre transferencia internacional de datos personales automatizados”, *Economist-Jurist*, enero / febrero, 1997, pp. 30-35

IV. LA APLICABILIDAD DE LA CONVENCION SOBRE LA UTILIZACION DE LAS COMUNICACIONES ELECTRONICAS EN LOS CONTRATOS INTERNACIONALES COMO ASPECTO RELEVANTE

Ante la posibilidad de que distintos operadores que se sitúan en el contexto electrónico de Blockchain y la IA, sin perder de vista, la computación en nube, puedan operar en el foro debemos tener presente la Convención sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales en 2005, que en su artículo 20 de la Convención, intitulado "Comunicaciones intercambiadas en el marco de otros instrumentos internacionales", dispone que la Convención se aplique también al empleo de comunicaciones electrónicas, relacionadas con la formación o ejecución de un contrato, que venga regido por una de las Convenciones que el propio Artículo determina en su apartado segundo.

Este artículo ofrece soluciones que tropieza el comercio electrónico en los instrumentos internacionales existentes, de forma que se evite la necesidad de enmendar los distintos Tratados internacionales²³. De esta forma, se produce una situación atípica en dos sentidos²⁴:

Se delimita el ámbito de aplicación de una Convención en función de la aplicación de otras Convenciones.

Estas resultan indirectamente modificadas, ya que, sin modificación formal, se permite incluir supuestos, en principios no contemplados, en referencia al uso de las comunicaciones electrónicas.

La Convención se aplica al modo de empleo de las comunicaciones electrónicas en relación con la formación y/o cumplimiento de un contrato (artículo 1,1); es decir, formación y ejecución de un contrato (no a las comunicaciones electrónicas bursátiles o financieras, etc. excluidas en el artículo 2,2), sin tener en cuenta la nacionalidad ni el carácter mercantil o civil de las partes del contrato.

Partiendo del ámbito de aplicación de la Convención, hemos de hacer dos precisiones: por un lado, la Convención se aplica a las partes cuyos establecimientos estén en distintos Estados; estos es, mensajes electrónicos intercambiados entre partes cuyos establecimientos estén en Estados contratantes diferentes, aun cuando

23 OLIVA BLÁZQUEZ, F., "Análisis de la Convención de las Naciones Unidas sobre la utilización de las comunicaciones electrónicas en los contratos internacionales", *Revista de Derecho Patrimonial*, 2007-2, núm. 19, pp. 45-88.

24 MADRID PARRA, A., "El derecho uniforme de la contratación electrónica", en *Comercio electrónico: estructura operativa y jurídica*, Ed. Hammurabi, Buenos Aires, 2010, pp. 221-295.

uno de esos Estados no sea contratante²⁵, en la medida que la Ley de un Estado contratante fuese aplicable a la operación de que se trate; por otro, la Convención de 2005 permite a los Estados contratantes expandir sus disposiciones a otros instrumentos internacionales en los que el Estado contratante sea o no parte del mismo (artículo 20), lo que lleva a que tengan que ser aplicados e interpretados conforme a la Convención de 2005, facilitándose la aplicación de lo previsto en los Convenios internacionales, en un entorno electrónico, al que no siempre se encuentran acomodados.

De esta forma, la regla contenida dentro del artículo 20 debe interpretarse de forma conjunta con el artículo 1, referente al ámbito de aplicación, con el fin de evitar la más que probable crítica a la suerte de la unilateralidad, que supondría el planteamiento contrario. Podemos decir que no se imponen reglas de un Convenio a otro Estado que no forme parte de él, sino que tan solo se auto delimita el ámbito de aplicación de la Convención, en tanto que integrante del ordenamiento nacional señalado aplicable, por el sistema de Derecho internacional privado del Estado del foro, a determinadas situaciones mercantiles internacionales.

Este planteamiento no es automático, pues según se indica en la Nota Informativa de la Secretaría de la CNUDMI²⁶: “Los párrafos 1 y 2 presuponen que todo Estado Contratante incorporará a su Derecho interno una disposición que ordene a sus órganos judiciales que recurran al régimen de la Convención para resolver toda cuestión jurídica suscitada por el empleo de mensajes de datos en el contexto de otros convenios internacionales”.

Por consiguiente, no se trata de enmendar o modificar ningún convenio, tratado o acuerdo internacional, con independencia de si figura o no en la lista del párrafo 1, ni tampoco se trata de dar una interpretación auténtica del texto de ninguno de esos instrumentos, sino que se trata de eliminar obstáculos jurídicos que el texto actual de los convenios internacionales pudieron imponer al comercio electrónico, lo que resulta lógico conforme a lo dispuesto en el derecho internacional público y en el Convenio de Viena de los Tratados de 1969. No lo hace, porque si se enmendara o modificara un convenio podrían contrariar en alguna medida el objeto y el fin del convenio o tratado, de tal forma que su conclusión y su aplicación haría incurrir a los Estados parte en un acuerdo *inter se* en responsabilidad internacional frente a los demás Estados parte²⁷.

25 PERALES VISCASILLAS, M^o P., “Publicidad y Formación del contrato: Convención de UNCITRAL sobre la utilización de las comunicaciones electrónicas en los contratos internacionales, 2005”, *Revista Electrónica de la Contratación*, núm. 72, junio 2006, pp. 3-45.

26 Cndmi/Uncitral, *Nota explicativa de la Secretaría de la CNUDMI* cit., pág. 54.

27 MONCAYO, G., VINUESA, R., GUTIERREZ POSSE, A., *Derecho Internacional Público*, Tomo I, Ed. Zaida, Buenos Aires, 1990, p. 126.

A la Convención se le da una aplicación de carácter general y transversal, ofreciendo soluciones prácticas para problemas, que se sustancian en el uso de los medios electrónicos de comunicación en la celebración de contratos internacionales. Y lo hace proyectándose sobre la plantilla resultante de la Convención de Viena de 1980 y con los principios cardinales de la Ley Modelo sobre Comercio Electrónico (1996) y la Ley Modelo sobre Firmas Electrónicas (2001)²⁸.

Así, teniendo en cuenta que una convención o tratado internacional supone una cierta unidad, relativamente cerrada y suficiente en sí misma, al margen de la relación de normativa necesaria, hay supuestos en los que se establece entre unos y otros acuerdos una concatenación fáctica. Así, esta Convención, como la Convención de Viena de 1980, recurre en ocasiones al criterio de "acuerdos que regulan la misma materia"; es decir, que además de la conexión formal establecida, hay otras que necesariamente surgen de la identidad del objeto entre acuerdos, que pueden ser formalmente distintos.

El estudio del proceso de integración comunitaria europea enseña que, aunque haya acuerdos comunitarios todo recibe una unidad en el derecho comunitario y, en su caso, consiste uno de los refinamientos de la unidad de esta técnica de integración. La Jurisprudencia de la Haya reconoce, que el principio de interpretación de una regla internacional debe ser interpretada en contemplación de las circunstancias que concurrieron en su constitución y los efectos jurídicos deben ser medidos por el entorno jurídico vigente en el momento de su aplicación. En consecuencia, la Convención se inserta en un marco normativo y sus distintos elementos evolucionan, acompasadamente, de tal modo que la mutación que se produzca repercute a los demás, por lo que esa expansión, en principio, no produce problemas.

Ahora bien, el empleo de Internet, como medio para la celebración de contratos internacionales, no modifica, normalmente, la determinación de la ley aplicable. Sin embargo, las peculiares características de la contratación por Internet hacen que la localización de las relaciones jurídicas en un ordenamiento estatal, con base a los criterios típicos empleados por las reglas de conflicto en la materia, como el lugar de celebración del contrato, lugar de ejecución de las obligaciones, el domicilio de alguna de las partes, etc. pueden resultar inapropiados, de tal forma que la falta de adecuación de estos criterios puede generar una dificultad en su concreción²⁹, por ejemplo, en términos de perfección del contrato a través de medios electrónicos es internacionalmente aceptado que la oferta es aceptada desde el momento en que la aceptación es recibida por el oferente sin que sea necesario conocimiento de la misma. Asimismo, hay ordenamientos que aceptan

28 MADRID PARRA, A., "El derecho uniforme", cit., pp. 221-295

29 MIGUEL ASENSIO, P.A., *Derecho Privado de Internet*, cit., p. 419.

el recurso de la vía electrónica, en el marco de ciertas categorías de operaciones, imponiendo requisitos especiales para su empleo, como puede ser el tipo de firma electrónica utilizada, mientras en otros países adoptan un enfoque más liberal, por razón de la cual, puede suceder que ciertas materias puedan estar sujetas a requisitos especiales o, incluso, excluidas en algunos países, mientras que en otros países no lo están.

Hemos de tener en cuenta que, el planteamiento del Artículo 20 a los instrumentos de derecho internacional privado comunitario resulta compleja si no imposible: una interpretación literal de este Artículo excluye del ámbito de aplicación material instrumentos supraestatales que no tengan carácter convencional (con independencia de su denominación), siendo los Reglamentos y Directivas de la Unión Europea técnicamente actos de Derecho comunitario europeo y no Convenios internacionales. Ahora bien, si las partes, en virtud de la autonomía de la voluntad (Artículo 3 de la Convención de 2005) declararan aplicable a los contratos internacionales que se celebren bajo el paraguas de la Convención de 2005, sin que los Estados fuesen parte de este, ¿qué pasaría en tal caso si la normativa aplicable no está adecuada para la celebración del contrato a través de medios electrónicos?

Las partes, en virtud de la autonomía de la voluntad, tan usada en el derecho internacional, para la configuración del contenido obligacional del contrato, son libres para pactar la aplicación al acuerdo de las reglas que tengan por conveniente (Aplicación indirecta).

Ante esto, el Artículo 19, I – b) de la Convención de 2005, prevé una limitación eventual del ámbito de aplicación de la Convención, de tal forma que todo Estado podrá declarar que solo aplicará la Convención a determinados contratos si las partes, en dicho contrato, han convenido que su régimen será aplicable a las comunicaciones electrónicas que vayan a intercambiar. Con ello, se reduce la aplicabilidad de la Convención y se priva a todo Estados, que se valiera de ella, de un régimen supletorio uniforme aplicable a las comunicaciones electrónicas intercambiadas entre partes en un contrato internacional, cuyo texto no prevea todos los pormenores que están resueltos en el régimen de la Convención³⁰.

V. CONCLUSIONES

Internet es la máxima expresión del comercio internacional, donde se producen nuevas formas de comunicación, información y comercialización. Ante

30 Cndmi/Uncitral, *Nota explicativa de la Secretaría de la CNUDMI*, cit., pág. 56.

esta situación resulta necesaria la introducción de normas, en los ordenamientos jurídicos existentes.

Hasta ahora, cada Estado miembro había traspuesto la Directiva 1999/93/CE, sobre firma electrónica, aunque en algunos aspectos, de manera divergente y, al mismo tiempo, se constataba en esta norma un vacío que provocaba barreras al comercio electrónico creando incertidumbres en torno a la firma electrónica, en cuanto a la ausencia de seguridad jurídica, debida a la heterogeneidad de las disposiciones nacionales y a la falta de interoperabilidad de los sistemas de firma electrónica establecidos a nivel nacional. Situación que va acompañada de la falta de confianza derivada de los ciudadanos en los propios sistemas electrónicos.

En este contexto nace el Reglamento 910/2014, con el objetivo de mejorar la legislación existente y ampliarla, incluyendo el reconocimiento y la aceptación mutuos a nivel de la UE, de los sistemas de identificación electrónica notificados y otros servicios de confianza electrónicos conexos esenciales.

el Reglamento, va más allá, incluyendo aspectos relacionados con la identificación: función identificativa y una la función de autenticación de la identificación; esto es, establecer un nivel de aseguramiento universal, confiable para la unión de identidades, con el fin de establecer credenciales aceptables en cualquier país.

Algo de vital de vital importancia, si se tiene en cuenta que la integridad del contenido del documento electrónico y la firma se basa en la capacidad de identificar al firmante o al remitente del documento de manera real y confiable.

Sin un estándar de aseguramiento de identidad electrónica uniforme, que esté alineado con las diversas leyes de firmas nacionales, aún en desarrollo por el progreso normativo del propio Reglamento europeo, todas partes presentes en la transacción se enfrentan a la necesidad de poseer varios tipos de credenciales electrónicos.

BIBLIOGRAFÍA

ALAMILLO DOMINGO, I., "El uso de los sistemas de identidad auto-soberana en el sector público español y de la unión europea", *Blockchain intelligence*, 2019, pp. 1-22.

ALAMILLO DOMINGO, I., "Firma y sello electrónicos: el porqué y el cómo de la implantación del nuevo reglamento europeo", *Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones*, N°. 74, 2016, págs. 28-29.

ALAMILLO DOMINGO, I., *Identificación, firma y otras pruebas electrónicas: la regulación jurídico-administrativa de la acreditación de las transacciones electrónicas*. Pamplona, 2019.

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

CARRASCOSA GONZÁLEZ, J., "La Directiva 95/46/CE: Entre la protección de la intimidad y la libre transferencia internacional de datos personales automatizados", *Economist & Jurist*, enero / febrero, 1997, pp. 30-35

CARRASCOSA GONZÁLEZ, J.: "Protección de la intimidad y tratamiento automatizado de datos personales en Derecho internacional privado", en *Revista Española de Derecho Internacional*, 1992-I, vol. XLIV, pp. 417-442

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

Cnudmi/Uncitral, *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

Cnudmi/Uncitral, *Aspectos contractuales de la computación en la nube*, Nueva York, 24 a 28 de abril de 2017

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

DE MIGUEL ASENSIO, P. A., *Derecho Privado de Internet*, Ed. Civitas, Madrid, 2015.

DIAGO DIAGO, Mª. P., "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, pág. 2.

MONCAYO, G., VINUESSA, R., GUTIERREZ POSSE, A, *Derecho Internacional Público*, Tomo I, Ed. Zaida, Buenos Aires, 1990

OLIVA BLÁZQUEZ, F., "Análisis de la Convención de las Naciones Unidas sobre la utilización de las comunicaciones electrónicas en los contratos internacionales", *Revista de Derecho Patrimonial*, 2007-2, núm. 19, pág. 45-88.

PERALES VISCASILLAS, M^a P., "Publicidad y Formación del contrato: Convención de UNCITRAL sobre la utilización de las comunicaciones electrónicas en los contratos internacionales, 2005", *Revista Electrónica de la Contratación*, núm. 72, junio 2006, págs. 3-45.

RODRÍGUEZ BENOT, A., "Acuerdos para la determinación del lugar de ejecución de las obligaciones contractuales y acuerdos atributivos de competencia en los convenios de Bruselas y de Lugano" en *La revisión de los Convenios de Bruselas de 1968 y Lugano de 1988 sobre competencia judicial y ejecución de resoluciones judiciales en materia civil y mercantil: una reflexión preliminar española. Seminario celebrado en Tarragona 30-31 de mayo de 1997*, Ed. Marcial Pons, Barcelona, págs. 165-197.