

# *La suplantación de identidad en los contratos electrónicos*

Catherina Gallardo\*

RVDM, nro. XV, 2025, pp. 361-380

**Resumen:** El presente trabajo tiene por objeto estudiar la suplantación de identidad en el ámbito de los contratos electrónicos, primeramente, desde el análisis de la legislación vigente en Venezuela, así como algunas normas modelo a nivel internacional, a los fines de verificar si existen regulaciones y mecanismos para prevenir la suplantación de identidad y establecer mecanismos seguros en la contratación electrónica a estos fines. Asimismo, se realiza un estudio sobre los mecanismos que pueden emplearse para prevenir y hacer frente a posibles casos de suplantación de identidad en el ámbito digital, especialmente orientados hacia el área de contratos electrónicos, así como las diversas leyes, generales o específicas, que nos sirven como marco de actuación en este sentido y, finalmente, los vacíos y áreas grises que las mismas pueden presentar. Finalmente, se hace una breve referencia a la relación entre suplantación de identidad y debida diligencia desde el punto de vista del prestador del servicio, en este caso de caras a España y el sector bancario, para abrir el debate en torno a cómo otros países están manejando políticas de prevención y actuación en este tema.

**Palabras clave:** identidad; suplantación; contratos electrónicos; consentimiento.

## *Identity theft in electronic contracts*

**Abstract:** *This paper aims to study identity theft in the context of electronic contracts, first through an analysis of the current legislation in Venezuela, as well as some international model regulations, in order to determine whether there are rules and mechanisms to prevent identity theft and establish secure contracting processes for these purposes. It also examines mechanisms that can be employed to prevent and address potential cases of identity theft in the digital sphere, particularly focused on electronic contracts, along with the various laws—general or specific—that serve as a framework for action in this regard, and finally, the gaps and gray areas these laws may present. Lastly, a brief reference is made to the relationship between identity theft and due diligence from the perspective of the service provider, in this case with a view toward Spain and the banking sector, to open the debate on how other countries are managing prevention and response policies on this issue.*

**Keywords:** *identity; impersonation; electronic contracts; consent.*

**Recibido:** 18/11/2025

**Aprobado:** 25/11/2025

---

\* Universidad Metropolitana, Venezuela. cgallardo@unimet.edu.ve



# *La suplantación de identidad en los contratos electrónicos*

Catherina Gallardo\*

RVDM, nro. XV, 2025, pp. 361-380

## SUMARIO:

INTRODUCCIÓN. *I. Suplantación de identidad y ordenamiento jurídico venezolano. II. Suplantación de identidad en contratos electrónicos. III. Suplantación de identidad y debida diligencia.* CONCLUSIONES. REFERENCIAS.

## INTRODUCCIÓN

Con el avance de la tecnología y la era digital, el ámbito de la contratación cada vez es visto menos como un proceso formal, escrito, y más como un proceso dinámico, en el cual las nuevas tecnologías adquieren un papel protagónico, en especial en el ámbito transfronterizo.

En este contexto la legislación tradicional, si bien aplicable desde el punto de vista general y sus instituciones jurídicas, resulta insuficiente para regular el ámbito de las operaciones comerciales llevadas a cabo en forma tecnológica, en razón de lo cual el Derecho Digital surge como una rama fundamental dentro de la dinámica actual, y más aún para el futuro, como mecanismo para establecer regulaciones especiales que permitan llevar las instituciones jurídicas contractuales al ámbito digital.

En el presente caso nos encontramos en el ámbito de la contratación por medios electrónicos, en la cual la Ley de Mensajes de Datos y Firmas Electrónicas representa, desde el contexto venezolano, el principal instrumento jurídico que permitirá dar respuestas y soluciones a cómo deben llevarse a cabo estos procesos, para cumplir con los requisitos y elementos fundamentales de los contratos.

Al referirnos a la identidad y su usurpación, nos estamos refiriendo al sujeto contratante y al consentimiento inequívocamente expresado, como mecanismo de validez del contrato e imputación de sus obligaciones y sus consecuencias.

Ello así, pasaremos a analizar este tema de los vicios en el consentimiento y la identidad del contratante y cómo hacerles frente, desde el punto de vista del derecho venezolano, así como las ideas y aportes que nos ofrece el contexto internacional.

---

\* Universidad Metropolitana, Venezuela. cgallardo@unimet.edu.ve

## ***I. Suplantación de identidad y ordenamiento jurídico venezolano***

Cuando se habla de suplantación de identidad se refiere al uso indebido de datos o documentos de otra persona, para hacerse pasar por ella. La identidad va atada a la noción de identificación, la cual es definida en el artículo 2 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de Identificación (2014) como “*el conjunto de datos básicos que individualizan y diferencian a una persona con respecto a otros individuos y que sirven de fuente de información para su reconocimiento*”.

Cabe recordar que la identidad es un derecho humano consagrado no sólo en nuestro país sino en el ámbito internacional, y que su relevancia es tal que la noción de ciudadanía va ligada a su existencia. Respecto a la suplantación de identidad, la misma puede tener lugar en el ámbito físico o en el ámbito digital. En el primer supuesto se da por la firma de documentos en nombre de terceros, el uso de documentos de identificación de otras personas, entre otros. En el ámbito digital se da por el uso de claves de acceso a correos o sistemas que pertenecen a un tercero, el uso de instrumentos de pago y tarjetas de crédito de otra persona, el empleo de una identidad falsa perteneciente a un tercero en correos electrónicos o redes sociales, entre otros, siempre cuando el que usa la identificación que no le es propia pretenda engañar haciéndose pasar por el titular.

Esta suplantación asimismo puede ocurrir tanto en el ámbito contractual como en el no contractual, siendo que a título meramente referencial y solamente para realizar un abrebocas del tema, podemos referirnos a las denuncias realizadas por ejemplo en el mundo de la televisión y el espectáculo, con casos como el de Maite Delgado, quien denunció en el mes de marzo de 2024 que a través del uso de la IA, se estaba utilizando su imagen y su voz para promocionar productos, obteniendo lucro indebido por parte de terceros a través del uso de esta suplantación de identidad<sup>1</sup>.

En nuestro ordenamiento jurídico no existe una norma específica que tipifique y sancione la suplantación de identidad en el ámbito digital. En efecto, la norma específica contentiva de este delito, que forma parte del Decreto con Rango, Valor y Fuerza de Ley Orgánica de Identificación (2014), únicamente hace referencia a la obtención de acta de nacimiento, cédula de identidad, pasaporte o documento de viaje mediante datos falsos o documentos de otra persona, sin que en ningún caso esta norma pueda tener alcance en el ámbito digital.

---

<sup>1</sup> (<https://www.instagram.com/reel/C4yVhtSP10m/>).

Asimismo, el Código Penal (2005)<sup>2</sup> establece como delito “*apropiarse de documentos oficiales para usurpar una identidad distinta a la suya*” (art. 319); atestar falsamente ante un funcionario público o en un acto público (art 320); falsificar o alterar *papeles* de carácter privado, haciendo uso de los mismos en perjuicio público o de particulares (art. 321); el uso de licencias, pasaportes, itinerarios y permisos de residencia pertenecientes a terceros (art.326) o cuando haga uso de documentos de este tipo atribuyéndose una falsa identidad (art. 327) y presentar como propios certificados pertenecientes a terceros, en materia de buena conducta, indigencia, empleos públicos, entre otros (art. 333). Todos estos delitos guardan relación directa o indirecta, o pueden constituirse en mecanismos, para materializar suplantación de identidad.

Respecto a las disposiciones aplicables en materia de derecho digital, y en particular respecto a contratos electrónicos es de interés y ayuda lo dispuesto en el mencionado Código Penal (2005),<sup>3</sup> en su artículo 320, cuando expresa que “*el que en títulos o efectos de comercio ateste falsamente su propia identidad o la de un tercero, será castigado con prisión de tres a seis meses*”.

Del mismo modo, en materia de usurpación de identidad y posibles normas aplicables al ámbito digital, encontramos las disposiciones contenidas en la Ley Especial Contra los Delitos Informáticos (2001),<sup>4</sup> de las cuales pueden ser de utilidad en la materia las siguientes:

- i. El artículo 6, que tipifica y sanciona el acceso y uso indebido de sistemas “*sin la debida autorización o excediendo la que hubiere obtenido*”.
- ii. El artículo 12, relativo a la falsificación de documentos, que conlleva tanto la creación de documentos incorporados a sistemas que utilizan tecnologías de la información, la modificación o eliminación de datos de estos, o la incorporación a dichos sistemas de documentos inexistentes.
- iii. Asimismo, el artículo 13, devenido de la materialización de hurtos a través del empleo de tecnologías de la información, accediendo, interceptando, interfiriendo, manipulando o usando sistemas o medios de comunicación para apropiarse de bienes tangibles o intangibles, sustrayéndolos de su tenedor. Ello ocurre, por ejemplo, cuando ocurre phishing bancario (el caso concreto cuando llega un correo que presuntamente es del banco y te roban los datos para acceder a tu cuenta y robarse los fondos), así como el uso de algún *Malware* que hurta los datos de acceso a bancos, con los mismos fines.

---

<sup>2</sup> Código Penal de la República Bolivariana de Venezuela (2005) Asamblea Nacional. Gaceta Oficial Nro 5.768 ( E ) del 13/04/2005

<sup>3</sup> *Ejusdem*.

<sup>4</sup> Ley Especial Contra los Delitos Informáticos (2001) Gaceta Oficial Nro. 37.313 del 30/10/2001.

- iv. Artículo 14, que dispone el delito de fraude, cuando se haga uso indebido de data o información contenida en sistemas, insertándose instrucciones falsas o fraudulentas como lo sería, por ejemplo, un acceso no autorizado a un banco (en línea) para sacar fondos desde la cuenta de la víctima, en beneficio propio o a un tercero.
- v. Artículo 15, que consagra la utilización de tarjeta inteligente ajena o instrumento destinado a los mismos fines o cuando se empleen TIC para obtener bienes o servicios sin erogar las contraprestaciones o pagos correspondientes. Ello ocurriría cuando uso la tarjeta de crédito de un tercero para hacer una compra, haciéndome pasar por el mismo, y no honrando el compromiso de pago asumido sino dejándolo en cabeza del titular de la tarjeta.
- vi. Finalmente, el artículo 16, que dispone el fraude por la alteración, duplicación, etc. de la información contenida en tarjetas inteligentes o la duplicación, alteración, etc. de data para incorporar usuarios, cuentas, registros o consumos inexistentes, norma que resulta aplicable en los casos de clonaciones de tarjetas bancarias, por ejemplo.

El reconocimiento de la identidad y los controles y mecanismos para evitar el uso indebido de la misma no sólo constituyen garantías del derecho humano a la identidad, sino que a su vez son garantía de la seguridad jurídica en materia de contratos y, en general, de las relaciones jurídicas en el ámbito digital, ya que determinan la confiabilidad en quién realiza la contratación y el consentimiento expresado ya que, de no garantizarse el mismo, las operaciones comerciales resultan anulables y, en general, los actos pudieran ser anulados y no tener efectos jurídicos.

## ***II. Suplantación de identidad en contratos electrónicos***

Primeramente, se debe hacer un breve recordatorio de qué es un contrato y cuándo estamos ante la presencia de contratos electrónicos. El artículo 1133 del Código Civil (1982)<sup>5</sup> define el contrato como “*una convención entre dos o más personas para constituir, reglar, transmitir, modificar o extinguir entre ellas un vínculo jurídico*”, partiendo siempre de la existencia de un acuerdo de voluntades, y la necesaria existencia de una oferta y una aceptación (art. 1137 CC), debiendo además estar presente los tres elementos de existencia del contrato: consentimiento, objeto y causa lícita (art. 1141).

Cuando se habla de contratos electrónicos se alude as referimos a aquellos en los cuales una parte o la totalidad de la operación (negociación, oferta y aceptación, acuerdo definitivo, suscripción y almacenamiento) se ha realizado en el entorno di-

---

<sup>5</sup> Código Civil (1982) Gaceta Oficial ( E ) Nro 2.990 del 26/07/1982.

gital, sea cual sea el medio utilizado (documentos avalados por certificados y firmas electrónicas, correos electrónicos, formularios web, etc.), siendo lo indispensable que el acuerdo definitivo devenga de medios electrónicos, al margen de si la fase previa, la negociación, etc., han sido efectuadas en forma analógica.

Interrelacionar el tema de los contratos electrónicos con la suplantación de identidad va orientada principalmente al elemento consentimiento como elemento del contrato, sin el cual el mismo carece de validez. Asimismo, va ligado a los mecanismos de seguridad y las formas de determinar la identidad de la persona que, en el ámbito digital, está realizando la contratación.

Sobre este respecto debemos señalar primeramente que, en Venezuela, lo relacionado a la usurpación o suplantación de identidad en materia relacionada a contratos electrónicos ha sido estudiado principalmente a nivel de sanciones, en el ámbito penal, que pudieran ser aplicables a estos casos, a las cuales hicimos referencia en el punto anterior y que están contenidas en el Código Penal (2005) y en la Ley Especial Contra los Delitos Informáticos (2001).

Ahora bien, en torno a la formación del contrato, incluyendo la oferta, aceptación y el acuerdo propiamente dicho, se entiende que los mismos, cuando son emitidos en forma electrónica, constituyen “mensajes de datos”, en los términos del artículo 2 de la Ley de Mensajes de Datos y Firmas Electrónicas <sup>6</sup>(en lo adelante LMDFE, 2001), disponiendo la propia Ley, en su artículo 15, que la oferta y la aceptación pueden ser realizadas por mensajes de datos. Asimismo, a los fines de determinar su emisor, el artículo 9 de la LMDFE dispone que se entiende que el mensaje es emitido por el emisor, salvo acuerdo en otros términos entre las partes, cuando se den alguna de las tres circunstancias siguientes: a) El mensaje devenga del propio emisor; b) El mensaje haya sido emitido por una persona autorizada para actuar en nombre del emisor respecto de ese mensaje; o c) Cuando el mensaje fuere emitido por un sistema de Información programado por el emisor, o bajo su autorización, para que opere automáticamente.

Asimismo, el mensaje puede contener a su vez una firma electrónica, dentro de su cuerpo o asociada a él, la cual tiene la misma validez que la firma autógrafa y permite atribuir la autoría del mensaje (identidad del remitente), siempre y cuando se cumplan los siguientes requisitos: a) Se garantice que los datos utilizados para su generación puedan producirse sólo una vez, y se pueda asegurar, razonablemente, su confidencialidad; b) Pueda ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento; y c) No se altere la integridad del mensaje de datos (artículo 16 LMDFE, 2001).

---

<sup>6</sup> Ley de Mensajes de Datos y Firmas Electrónicas (2001) Gaceta Oficial Nro 37.148 del 28/02/2001.

Las firmas electrónicas pueden certificarse por un Proveedor de Servicios de Certificación, siendo que en este caso el titular tendrá, además, como responsabilidades extras: a) Actuar con diligencia para evitar el uso no autorizado de su Firma Electrónica; y b) Notificar a su Proveedor de Servicios de Certificación que su Firma Electrónica ha sido controlada por terceros no autorizados o indebidamente utilizada, cuando tenga conocimiento de ello (artículo 19 *ejusdem*). Asimismo, algunos de los deberes del Proveedor de Servicios de Certificación son “*adoptar las medidas necesarias para determinar la exactitud de los Certificados Electrónicos que proporcionen y la identidad del Signatario*” (artículo 35 numeral 1 LMDFE) y “*verificar la información suministrada por el Signatario para la emisión del Certificado Electrónico*” (artículo 35 numeral 3), lo cual refuerza (más no garantiza en cien por ciento) la identidad de la parte. Del mismo modo, tienen el deber que “*garantizar la adopción de las medidas necesarias para evitar la falsificación de Certificados Electrónicos y de las Firmas Electrónicas que proporcionen*” (artículo 35 numeral 8), lo cual implica no sólo el deber de verificar la información para la emanación de documentos, sino también garantizar la fiabilidad de los documentos emitidos. Tan es así que la propia Ley dispone que “*el Certificado Electrónico garantiza la autoría de la Firma Electrónica que certifica, así como la integridad del Mensaje de Datos*” (2001, art. 38 LMDFE).

Esta Ley encontró su fundamento principal en la Ley Modelo de la Comisión de las Naciones Unidas sobre el Derecho Mercantil Internacional (en lo adelante CNUDMI) sobre Comercio Electrónico (1996)<sup>7</sup>, la cual, si bien es cierto no es un instrumento vinculante, tiene una importancia fundamental no sólo en nuestro país, sino en el contexto internacional. El mismo contiene una serie de disposiciones de interés, muchas de ellas recogidas en la prenombrada Ley. Una de ellas es la regulación del principio de equivalencia funcional, cuando dispone que cuando se requiera la firma (de un documento), dicho requisito queda satisfecho si el mensaje de datos “*...utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos...*”, así como si el método es fiable y apropiado para los fines para los que se *generó y comunicó* el mensaje (art. 7).

Un aspecto interesante de esta Ley Modelo guarda relación con la forma de determinar que el mensaje proviene de una determinada persona. En este sentido, el artículo 13 señala que debe entenderse que el mensaje de datos ha sido enviado por la persona no sólo si es remitido directamente por la misma, sino también cuando es emitido por alguna persona facultada para actuar en su nombre o por un sistema de información programado para actuar automáticamente en su nombre, lo cual coincide con el artículo 9 de la LMDFE; sin embargo, también dispone que el destinatario no

---

<sup>7</sup> ONU 1996. Ley Modelo de la Comisión de las Naciones Unidas sobre el Derecho Mercantil

debe dar valor al mensaje de datos cuando “*sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el mensaje de datos no provenía del iniciador*”.

Asimismo, tiene importancia y es un referente en la materia a nivel internacional la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (2001), la cual, en sintonía con el texto previamente analizado, atribuye valor a las firmas electrónicas en mensajes de datos cuando la misma resulte *fiable y apropiada* para los fines para los cuales se *generó o comunicó* ese mensaje. A estos fines, señala los elementos que deben estar presentes para considerar fiable la firma electrónica:

- a) los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;
- b) los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;
- c) es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y
- d) cuando uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, es posible detectar cualquier alteración de esa información hecha después del momento de la firma.” (art. 6)

Asimismo, dispone en su artículo 7 que las autoridades (públicas) de cada Estado deberán determinar qué firmas electrónicas cumplen con dichos requisitos. Del mismo modo, establece la responsabilidad del titular de la firma de actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma; y de notificar al prestador de los servicios de certificación y a los terceros que puedan tener interés, cuando los datos de creación de la firma hayan quedado o puedan quedar en entredicho, teniendo responsabilidad en caso de no cumplir con esta carga. Asimismo, dispone en su artículo 9 que el prestador de los servicios de certificación debe proporcionar a quien confía en el certificado, en el cual está contenida la firma, entre otros aspectos, medios que le permitan determinar el método empleado para comprobar la identidad del firmante. (art.8)

Siguiendo con ello, en el artículo 10 establece algunos requisitos para determinar si los sistemas de certificación son fiables, incluyendo: (i) *la calidad de los sistemas de equipo y programas informáticos*; (ii) *los procedimientos para la tramitación del certificado y las solicitudes de certificados, y la conservación de registros*; (iii) *la disponibilidad de información para los firmantes nombrados en el certificado y para las partes que confíen en éste*; entre otros. El artículo 11, por su parte, dispone que es responsabilidad de quien confía en el certificado, verificar la fiabilidad de la firma y la validez del certificado. Por último, dentro de los instrumentos internacionales de

importancia en la materia y a pesar de no estar ratificada por Venezuela, consideramos de interés a la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (2007)<sup>8</sup>, la cual dispone, en su artículo 9, que cuando se requiera de la firma por una de las partes del contrato, debe garantizarse la identidad de la persona y su consentimiento, así como asegurarse que el método empleado en la comunicación sea *fiable y apropiado*.

Ahora bien, si se remite a las Notas Explicativas de la Secretaría de la CNUDMI sobre esta Convención, las cuales además son en su mayoría replicadas en las Notas Ley Modelo de la Comisión de las Naciones Unidas sobre el Derecho Mercantil Internacional (en lo adelante CNUDMI) sobre Comercio Electrónico, llama poderosamente la atención a que sobre esta norma comenta que su aplicación (criterio de equivalencia funcional) no debe imponer “...*normas de seguridad más estrictas (con los costos que acarrear) que a los usuarios de un documento sobre papel...*”. Sin embargo, al explicar el requisito de fiabilidad previamente referido, sí hace referencia a la complejidad técnica de los equipos empleados en las comunicaciones, los procedimientos de autenticación, el empleo de dispositivos de seguridad de alto nivel, etc., dependiendo del tipo de operación comercial, su carácter eventual o no y la envergadura de la misma. Asimismo, al pronunciarse sobre la fiabilidad, señala que “...*no debe inducir a un tribunal o a un verificador de los hechos a invalidar la totalidad del contrato por estimar que la firma electrónica no es debidamente fiable si no hay ninguna disputa acerca de la identidad de la persona firmante o del hecho de que ha firmado...*”, ya que permitiría a cualquier parte eludir sus obligaciones negando la validez de su firma.

También es importante analizar qué sucede cuando en la contratación participan sistemas automatizados de mensajes, en los cuales la máquina actúa sin la intervención humana, y cómo se expresa el consentimiento en estos casos y a su vez, se evita la suplantación de identidad (art 12). Sin embargo, la convención solamente se limita a tomar como válidas estas contrataciones, sin entrar al análisis de estos aspectos.

Se puede ver entonces, que en los contratos electrónicos en los cuales simplemente estemos en presencia de un mensaje de datos, sin una firma electrónica o con una firma electrónica simple, no reportan una garantía en torno a su emisor y, por tanto, respecto a la identidad de la persona que está contratando, ya que bien pudiera una persona crear un correo electrónico con el nombre, datos personales o incluso fotografía de otra persona y contratar en nombre de la misma, en especial si las comunicaciones electrónicas son realizadas a través de correos electrónicos o de sistemas automatizados.

---

<sup>8</sup> ONU. 2007. Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales.

Ahora bien, si se utiliza la figura de la firma electrónica certificada, que vaya avalada por un proveedor de servicios regulado, se generan unas garantías adicionales para evitar la suplantación de identidad, como lo son el deber de dicho proveedor de verificar la identidad del signatario de la firma, así como verificar la información suministrada para la emisión del certificado, lo cual incluye los datos personales e identidad del solicitante, así como el deber posterior de evitar la falsificación de los certificados (por ejemplo, a través de la modificación de los datos del firmante y hacerse pasar por parte del contrato un tercero que no lo es), ello no garantiza en cien por ciento que la identidad que dice tener la persona no sea usurpada, por ejemplo, si al cargar la solicitud de documento electrónico se emplea una cédula, pasaporte o documento de identificación bien de un tercero, bien forjado.

Cabe recordar que la función principal del certificado “*es vincular la identidad del firmante a una clave pública*” de modo que es tarea fundamental del prestador del servicio de certificación velar porque “*el solicitante sea el presunto firmante y ejerza el control de la clave privada correspondiente a la clave pública indicada en el certificado*” (Comisión de las Naciones Unidas para el Derecho Mercantil Internacional: Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas, 2009)<sup>9</sup>. Al respecto, en dicho documento, se señalan tres ejemplos de posibles casos en que se materializaba la usurpación de identidad a través de estos certificados, a saber:

Los propios empleados o contratistas del prestador de servicios de certificación podrían confabularse para expedir certificados erróneos utilizando la clave de firma de éste para atender a solicitudes indebidas del impostor. Esas personas podrían actuar con negligencia y expedir un certificado erróneo, ya sea aplicando indebidamente los procedimientos de validación establecidos por el prestador de servicios de certificación al examinar la solicitud del impostor o utilizando la clave de firma del prestador de servicios de certificación para crear un certificado que no ha sido aprobado. Por último, un malhechor podría hacerse pasar por el firmante utilizando documentos de identificación falsificados, aunque aparentemente auténticos, y convencer al prestador de servicios de certificación, aun cuando éste se adhiera cuidadosamente a sus normas establecidas y no actúe con negligencia, a extenderle un certificado.

Asimismo, se pudiera hackear el sistema empleado para su creación y empleo del certificado o la firma, o pudiera también accederse a la clave privada<sup>10</sup> del autor de la firma si el mismo no guarda la debida diligencia para impedir el acceso por terceros

<sup>9</sup> Comisión de las Naciones Unidas para el Derecho Mercantil Internacional: Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas, 2009, p. 101.

<sup>10</sup> En materia de certificados electrónicos, existen claves públicas y privadas, las cuales se interrelacionan y van ligadas a los documentos. El autor divulga la clave pública, que permite a los terceros validar la existencia y contenido del documento, pero conserva la clave privada, que sólo él maneja y que es la que le permite acceder y crear las firmas electrónicas.

o en los casos en que el mismo divulgue o comparta dicha clave. Sobre este aspecto nuestra legislación también consagra el deber del titular de la firma de asegurarse que la misma no sea utilizada por terceros, siendo que en el supuesto de que ello ocurriera, el titular tiene el deber de informar de inmediato al proveedor de servicios.

En Europa, en particular en España, este tema ha sido tomado muy en serio, en particular desde el punto de vista de la prevención, pudiendo hacerse referencia a la labor desarrollada por la Agencia Española de Protección de Datos, quien en diversas materias ha realizado seguimiento y auditoría en torno al funcionamiento de los sistemas a través de los cuales se realizan contrataciones electrónicas, pudiendo mencionarse el caso particular de telecomunicaciones y energía. En el informe de auditoría publicado en el año 2020 y reseñado por la propia Agencia, refiere a la necesidad de que las empresas, en sus procesos de autenticación de identidad, de que se adopte un *modelo de información por capas o niveles*, que implique la validación de preguntas de seguridad a través de dos o más elementos independientes, que sólo conoce y posee el usuario, de manera que si existe una vulneración en los datos de uno de los elementos, el sistema a través del segundo o tercer elemento, pueda determinar la existencia de irregularidades y bloquear el proceso de contratación<sup>11</sup>

Asimismo, la Agencia elaboró unas Recomendaciones en la Contratación a Distancia de Servicios de Telecomunicaciones y Energía, dirigidas a los usuarios, que expresan entre las mismas: que los usuarios se aseguren de estar ingresando a la página del proveedor del servicio; utilización de contraseñas seguras, que no incluyan datos fáciles de averiguar (como fecha de nacimiento, cédula de identidad, etc.); cerrar las sesiones al momento de terminar las operaciones realizadas en las mismas; incluir mecanismos adicionales de seguridad en los dispositivos electrónicos como teléfonos y Tablet, como la autenticación vía huella digital y reconocimiento facial; entre otras.

Estas son las garantías para evitar la suplantación de identidad dispuestas en nuestra legislación, respecto a los certificados y firmas electrónicas, que son los mensajes de datos regulados por la misma y que, aún a pesar de esta regulación, vemos que la misma resulta insuficiente, en la práctica, para evitar la suplantación de identidad. Ello sin adentrarse en temas más profundos, como aquellos que pudieran devenir del uso de la Inteligencia Artificial para generar perfiles falsos y documentación forjada, que burle los sistemas de seguridad y códigos empleados por los proveedores de servicios de certificación (en nuestro país o en el extranjero) y permitan generar certificados y firmas electrónicas a personas creadas con IA o a perfiles falsos o modificados a través del empleo de esta tecnología.

---

<sup>11</sup> (<https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/aepd-publica-resultados-auditoria-contratacion-telecomunicaciones-energia>)

Ahora bien, estas garantías y estos niveles de verificación resultan aplicables en nuestro país a los certificados electrónicos y las firmas electrónicas, más la práctica que se da que en el día a día, en el comercio nacional e internacional, no deviene en su mayoría de certificados y firmas electrónicas avanzadas o cualificadas, sino del simple envío de correos electrónicos, con el nombre de la persona remitente, lo cual es empleado como mecanismo válido de identidad y compromiso de las partes en una operación mercantil, dada la complejidad y costos asociados a las firmas electrónicas, más para su empleo en operaciones cotidianas. Siendo ello así, estas garantías reforzadas no están siquiera presentes y basta con que en un correo electrónico por ejemplo: yo indique “mi nombre es Pedro Pérez y mi ID es xxx,” para entablar un proceso de negociación de contrato por vía electrónica, que pudiera llevar a suplantación de identidad o fraude y que, en el caso de que el contratante no cumpla, resultará muy difícil, por no decir imposible, lograr la ejecución forzosa de las obligaciones contraídas.

El tema clave para evitar la suplantación de identidad, de cara a los privados, es la prevención. En efecto, no publicar datos personales y documentos como la cédula de identidad en perfiles públicos, restringir la privacidad a datos personales y proteger las contraseñas de los correos electrónicos, son elementos que evitan que la información sensible, que pueda ser empleada para suplantación de identidad, pueda ser accedida por terceros inescrupulosos. Asimismo, ser cuidadosos en la apertura de correos electrónicos, enlaces, etc., para evitar el phishing, es otro elemento base de la prevención.

Asimismo, el mecanismo ideal de caras a los particulares, en particular en nuestro caso, es el empleo de firmas electrónicas que posean certificados electrónicos, debidamente otorgados por una empresa acreditada a estos fines (en el caso de Venezuela, por la Superintendencia de Servicios de Certificación Electrónica – SUSCERTE), como mecanismos para la contratación digital, en especial cuando se refiera a operaciones comerciales recurrentes o grandes contratos, que van más allá de una simple compra venta a través de un portal web.

En estos casos, los costos y cargas que puedan conllevar las firmas y certificados electrónicos se deben sopesar con la garantía de la efectividad de las operaciones comerciales y de la posibilidad de hacer cumplir las obligaciones a través de la jurisdicción competente en caso de que se produzca un incumplimiento por alguna de las partes, lo cual constituye un riesgo de las operaciones de comercio electrónico y contratos electrónicos, siendo por tanto conveniente para las partes garantizar la identidad del contratante y su contraparte.

Puede verse como en algunos países ya se está buscando la masificación del acceso a mecanismos seguros como las firmas electrónicas, para que sean usadas en el día a día de las personas. Un ejemplo de ello es Bélgica, país en el cual se ha dotado a las

personas con tarjetas de identidad física contentivas de un chip que contiene los datos que necesita el ciudadano para producir una firma digital <sup>12</sup>.

Ahora bien, en los casos en que ya se hubiere materializado una suplantación de identidad, y cuando la misma devenga de que usen en forma indebida los datos de una persona para hacerse pasar por ella y comprometerla, por ejemplo, para la adquisición de un crédito, y esa persona quede obligada al pago de las cuotas e intereses por el dinero otorgada a un tercero, es muy importante tener presente que la mayoría de las veces, cuando se conozca de la suplantación, en particular por la persona cuya identidad haya sido usada inescrupulosamente, el contrato falso ya se habrá consumado, y la forma como el sujeto se entera es porque le llegue un correo electrónico o alguna comunicación, en formato físico o digital, solicitando el pago de una obligación que no ha contraído, o porque reciba notificaciones de plataformas en las cuales nunca se ha registrado, o cuando se le bloqueen los accesos a alguna plataforma o servicio financiero que antes era utilizado con normalidad.

Una vez detectado un posible caso de suplantación de identidad, es importante recopilar y guardar todos los soportes que constituyan las posibles pruebas. A este respecto se debe recordar que estando en presencia de pruebas electrónicas, la simple impresión de los soportes de las mismas no resulta suficiente, sino que es necesaria la conservación de cada uno de los documentos y pruebas en su formato digital, para luego poder ser incorporadas a cualquier juicio, de ser necesario, por la vía del documento electrónico y la constatación y experticia informática de dichos soportes, ya que se trata de mensajes de datos, equiparables a los documentos escritos pero diferentes a ellos.

Asimismo, existen otros elementos que pueden ser usados para demostrar la suplantación de identidad, entre los que podemos mencionar, sólo a título de ejemplo:

- Si se usaron documentos de identificación cargados a sistemas o plataformas, verificar la veracidad de estos. Si fuera el caso de Venezuela y por ejemplo, se empleó una cédula que se había perdido, consignar la denuncia de pérdida del documento de identidad.
- Revisión de las IP y las identificaciones de los equipos web desde los que se realizaron los accesos a los portales o desde donde se enviaron los correos electrónicos y demás mensajes de datos que soportan el proceso de contratación, para demostrar que los mismos no pertenecen ni fueron accedidos por la parte suplantada.

---

<sup>12</sup> Comisión de las Naciones Unidas para el Derecho Mercantil Internacional: Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas, 2009, p. 34

- Que la persona cuya identidad fue usurpada haya sido víctima de phishing, *malware* u otros mecanismos de robo de datos, lo cual resultará perfectamente demostrable en los casos en que hayan existido denuncias ante las autoridades competentes pero que, en caso de no haberse presentado, requerirán de pruebas electrónicas para demostración de estos dichos.
- Demostrar que no se cumplieron con protocolos *suficientes* para garantizar la identidad de las partes, lo cual resulta bastante idóneo si existía un protocolo o procedimiento a seguir para identificar a las partes, pero no sería tan idóneo, por ejemplo, en los casos en que la oferta y/o la aceptación o la contratación en sí misma se realicen a través de mensajes de datos como correos electrónicos.

En los casos en que existan firmas o certificados electrónicos, la prueba podrá devenir del momento inicial de creación de los mismos, para determinar si se cumplieron a cabalidad los mecanismos de verificación de identidad de sus suscriptores o, en los casos de que fueron utilizados datos falsos, la demostración de esta suplantación; o podrá devenir de la falsificación de las firmas o certificados ya emitidos, lo cual puede demostrarse a través de experticias informáticas en los certificados o a través de la validación por el propio proveedor del servicio de certificación.

En todos los casos, las pruebas estarán centradas en el ámbito técnico, para demostrar el uso indebido o inescrupuloso de las identidades de las partes supuestamente vinculadas en los procesos de contratación. Por último, sobre el tema de la prueba en los procesos de contratación, se debe precisar que las manifestaciones de voluntad no necesariamente tuvieron que devenir de un documento escrito ni de la prueba escrita. En efecto, al hablar de lo electrónico o digital, cabe englobar dentro de este concepto no sólo los documentos intercambiados vía electrónica, los sistemas y los emails, sino también el intercambio vía celulares, las reuniones vía conferencia o teleconferencia, entre otros. Sin embargo, algunos doctrinarios han aclarado que al margen de que la oferta sea verbal, escrita o de otra naturaleza, al realizarse a través de un mensaje electrónico o de datos, su forma es “oferta electrónica”, con la eficacia probatoria que ello conlleva, en los términos dispuestos en la Ley de Mensajes de Datos y Firmas Electrónicas<sup>13</sup> Es decir, siempre deviene de un “mensaje de datos”, cuya prueba se basará en la evacuación vía prueba libre, conforme a lo dispuesto en el artículo 4 de la mencionada Ley.

---

<sup>13</sup> V. Guidón Guerrero: Breve análisis sobre la formación del contrato por la vía electrónica en Venezuela, 2018, p. 298 y ss

Por último, y para destacar que siempre los procedimientos de contratación electrónica serán más convenientes y seguros (más no infalibles) en la medida en que se usen mecanismos de seguridad agravados como las firmas electrónicas y los certificados electrónicos, queremos llamar la atención sobre que la “firma digital”, que cumple con todos los estándares para su elaboración y certificación, pero que tiene un contenido más amplio que el sólo valor de la firma por parte de la persona, con los vínculos respectivos respecto a la identidad de la misma, siendo que también se señala respecto a las mismas que:

*la tecnología de la firma digital “no determina simplemente el origen o la integridad respecto de personas como es necesario a efectos de firma, sino que también puede autenticar, por ejemplo, servidores, sitios de Internet, programas informáticos, o cualesquiera otros datos que se distribuyan o almacenen de forma digital”, lo que confiere a las firmas digitales “una utilización mucho más amplia que la de alternativa electrónica de las firmas manuscritas”*<sup>14</sup>

### ***III. Suplantación de identidad y debida diligencia***

Adicional al tema de la suplantación de identidad propiamente dicha y el fraude y demás delitos, devenidos de la utilización de datos de terceros, como propios, en los procesos de contratación electrónica, consideramos interesante la reflexión sobre temas de debida diligencia que se han venido abriendo debate en España y las medidas que deben ser adoptadas por las partes contratantes para garantizar la identidad y, por tanto, el consentimiento, de las personas que están siendo parte de un proceso de contratación electrónico.

En este país el Tribunal Supremo, en particular su Sala de lo Contencioso - Administrativo, Sección Tercera, dictó sentencia Nro. 1.456/2021, en fecha 13 de diciembre de 2021, caso Dineo Crédito, S.L., con ponencia de Eduardo Calvo Rojas, en la cual estableció la responsabilidad en materia de protección de datos de la empresa contratante en un proceso electrónico, de garantizar a través de la debida diligencia que “quien solicita el crédito es precisamente quien dice ser”.

Este caso tiene su fundamento en la contratación de un micro crédito, vía telemática, presuntamente por un señor llamado Eusebio, por el importe de 100 euros, a través de la entidad bancaria Dineo Crédito S.L, crédito que no fue realmente solicitado por este ciudadano y en el cual, en el proceso de contratación, no se realizó la debida validación de su identidad, en carácter de contratante, haciendo el análisis sobre la base de la necesidad del *consentimiento inequívoco y necesario*, que no admita duda o equivo-

---

<sup>14</sup> Comisión de las Naciones Unidas para el Derecho Mercantil Internacional: Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas, p. 16

cación, señalando que Dineo Crédito, S.L. “...no adoptó las medidas que la diligencia impone al objeto de acreditar la identidad de la persona que contrata con ella y para garantizar que quien facilita como suyos datos personales es su verdadero titular...”.

En efecto, del análisis del caso se evidencia que la institución bancaria no adoptó mecanismos suficientes para realizar la verificación de identidad de dicho ciudadano, ya que a pesar de solicitarse una serie de datos, como DNI (equivalente a la cédula de identidad en Venezuela), teléfonos y correos electrónicos, no existen mecanismos de validación de que los mismos pertenecen a la persona que los indica como suyos, ya que el proceso de verificación, por ejemplo respecto al teléfono, se limita a remitir un código a dicho número, que debe ser cargado en la plataforma; respecto al DNI, la verificación deviene de un algoritmo que determina que el DMI es real y válido pero no que pertenece a la persona; respecto a la cuenta bancaria, solo se valida que está abierta y activa, usándose para la transferencia de los recursos provenientes del crédito; entre otros de los aspectos analizados, siendo que del debate probatorio evacuado en el caso se determinó que ni el número telefónico empleado en la solicitud de crédito, ni la cuenta a la que fueron depositados los fondos, pertenecían al señor Eusebio.

En efecto, la sentencia concluye ratificando la decisión de condena a Dineo Crédito, S.L., concluyendo que, si bien el mismo no tenía la responsabilidad de impedir la comisión del hecho ilícito, es decir, la utilización fraudulenta del DNI del señor Eusebio, si tenía la responsabilidad de debida diligencia para asegurar el consentimiento y la identidad de la persona que estaba realizando el negocio jurídico.

Este criterio debe ser analizado de cara a las nuevas tendencias en *compliance* y debida diligencia, para determinar cuál es la actuación deseada por parte de los actores económicos que realizan contratos por medios digitales, en especial de caras a sectores regulados (lo que en Derecho Administrativo algunos autores denominan Ordenamientos Sectoriales), como lo pudieran ser banca, seguros, telecomunicaciones, e incluso ámbitos en los cuales pudiera estar incluso inmersa la noción del débil jurídico como sucedería en materia de educación.

## CONCLUSIONES

Como pudo verse a lo largo del presente artículo, la suplantación de identidad en el ámbito comercial y contractual viene dada cuando una persona se hace pasar por otra para realizar una negociación, haciendo nugatorias las posteriores exigencias hacia el presunto obligado, especialmente de pago. Esta suplantación afecta el consentimiento, como elemento de existencia del contrato, así como la identidad misma del suscriptor o parte del compromiso contractual.

A pesar de no existir una norma expresa en nuestro ordenamiento jurídico que regule la suplantación de identidad en el ámbito digital, y siendo que además la Ley de Mensajes de Datos y Firmas Electrónicas a pesar de señalar las regulaciones respecto a cuándo debemos considerar que un mensaje de datos fue enviado por el emisor, poco dispone en torno a mecanismos para evitar la suplantación de identidad, más allá del señalamiento de que, en caso de Certificados Electrónicos, el emisor deberá garantizar la constatación de la identidad del signatario, así como la información dada para su emisión (artículo 35 numerales 1 y 3), supuesto que solamente aplicará en la medida en que el instrumento utilizado para la contratación goce de esta formalidad.

A este respecto, se pudo ver cómo los contratos electrónicos pueden ser realizados por el simple acuerdo de voluntades, sin mayor formalidad, o pueden también realizarse mediante el uso de firmas o certificados electrónicos, supuestos en los cuales nos encontramos frente a firmas electrónicas calificadas o certificadas, dependiendo del caso, lo cual les dará un mayor grado de confiabilidad en torno al empleo de mecanismos de certificación de la identidad de los firmantes, pero confiabilidad que no resulta absoluta sino más bien “*iuris tantum*”, ya que pueden haberse empleado mecanismos para subvertir los sistemas de seguridad y mecanismos de certificación de identidad empleados para la emisión de estas firmas y certificados.

A nivel internacional, son ilustrativas para este tema y llaman la atención las disposiciones de la Ley Modelo de la Comisión de las Naciones Unidas sobre el Derecho Mercantil Internacional (en lo adelante CNUDMI) sobre Comercio Electrónico (1996), que expresa que el destinatario no debe dar valor al mensaje de datos cuando “*sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el mensaje de datos no provenía del iniciador*”. Asimismo, la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (2001) nos establece en su artículo 10 algunos requisitos para determinar si los sistemas de certificación son fiables, incluyendo *la calidad de los sistemas de equipo y programas informáticos; los procedimientos para la tramitación del certificado y las solicitudes de certificados y la disponibilidad de información para los firmantes nombrados en el certificado y para las partes que confíen en éste*, así como consagra, en su artículo 11, que quien confía en el certificado tiene la responsabilidad de verificar la fiabilidad de la firma y la validez del mismo. Del mismo modo, la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (2007) dispone, en su artículo 9, que cuando se requiera de la firma por una de las partes del contrato, debe garantizarse la identidad de la persona y su consentimiento, así como asegurarse que el método empleado en la comunicación sea *fiable y apropiado*.

Es importante, en cualquier operación de contratación, en especial cuando las mismas se hagan a través de sistemas, programas o formularios web, cuando se refieran a contratos transfronterizos o cuando existan importantes cargas u onerosidades de por medio, que se establezcan mecanismos especiales de seguridad para verificar la identidad de las personas. Estas pueden devenir de preguntas especiales de seguridad que sólo puede responder el usuario y que no son verificables por el simple uso de sus documentos de identidad, que puedan conllevar identificación biométrica, empleo de equipos y sistemas de seguridad de alto nivel, empleo de sistemas de seguridad por capas o niveles, entre otros. Asimismo, es importante la seguridad que los propios usuarios puedan tener respecto al uso de sus contraseñas, documentos y datos personales, así como el ingreso a sitios web para evitar hackeos, phishing o suplantaciones.

Otro elemento de interés, que ya se encuentra regulado en España más no así en Venezuela, es la obligación de debida diligencia que aplica a los sujetos contratantes en determinados ámbitos económicos, como el bancario, donde es el prestador del servicio en los casos de servicios públicos, por ejemplo, el que tiene la carga y el deber de constatar la identidad del contratante del servicio, so pena de imposición de sanciones por el no cumplimiento de debida diligencia, elemento que perfectamente pudiera ser trasladable a Venezuela, en sectores regulados como la banca, seguros y telecomunicaciones, por sólo mencionar algunos.

Finalmente, a la presente fecha, la vía para atacar estos supuestos de usurpación de identidad en Venezuela vendría dada tanto por la solicitud de nulidad del contrato, en principio en la jurisdicción civil (pero pudiera ser en otras áreas, por ejemplo, en el caso de servicios públicos, prestados por el Estado, donde correspondería a la jurisdicción contencioso administrativa), y por la vía penal, conforme a las disposiciones del Código Penal y la Ley Especial Contra los Delitos Informáticos.

## REFERENCIAS

Agencia Española de Protección de Datos <https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/aepd-publica-resultados-auditoria-contratacion-telecomunicaciones-energia>

Código Civil, G.O. Nro. 2.990 Extraordinario del 26/07/1982.

Código Penal, G.O. Nro. 5.768 Extraordinario del 13/04/2005.

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional: Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas, 2009: [https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/08-55701\\_ebook.pdf](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/08-55701_ebook.pdf)

Decreto con Rango, Valor y Fuerza de Ley Orgánica de Identificación, G.O. Nro. 6.155 Extraordinario del 19/11/2014.

Guidón Guerrero, Víctor (2018) Breve análisis sobre la formación del contrato por la vía electrónica en Venezuela, en Revista Venezolana de Legislación y Jurisprudencia Nro. 11. Consultada en <https://rvlj.com.ve/wp-content/uploads/2019/01/RVLJ-11-293-315.pdf>

Instagram (2024) <https://www.instagram.com/reel/C4yVhtSP10m/>

Ley de Mensajes de Datos y Firmas Electrónicas, G.O. 37.148 del 28/02/2001.

Ley Especial Contra los Delitos Informáticos, G.O. Nro. 37.313 del 30/10/2001.

Ley Modelo de la Comisión de las Naciones Unidas sobre el Derecho Mercantil Internacional sobre Comercio Electrónico (1996).

Ley Modelo de la Comisión de las Naciones Unidas sobre el Derecho Mercantil Internacional sobre las Firmas Electrónicas (2001).

Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (2007).

Recomendaciones en la Contratación a Distancia de Servicios de Telecomunicaciones y Energía. Agencia Española de Protección de Datos. <https://www.aepd.es/infografias/infografia-contratacion-telecos-energia.pdf>

Sentencia del Tribunal Supremo de España, Sala en lo Contencioso, 13 de diciembre de 2021, caso Dineo Crédito, S.L. vs. Administración General del Estado. Consultada en <http://maz.es/Publicaciones/MAZ%20Informa/20220408-01.pdf>