Las formalidades de los actos jurídicos en formato digital

Identidad, firma electrónica, sellado de tiempo, conservación de mensajes de datos y eficacia probatoria en el derecho mexicano

Alfredo Bazúa Witte*
Notario 230 de la Ciudad de México

RESUMEN

La transformación digital ha modificado profundamente la forma en que las personas celebran, documentan y prueban actos y negocios jurídicos. La progresiva sustitución del papel por mensajes de datos y de la firma autógrafa por mecanismos electrónicos ha obligado a replantear conceptos jurídicos tradicionales relacionados con la forma escrita, la autenticidad documental y la eficacia probatoria. Si bien la legislación mexicana reconoce desde hace varios años la validez jurídica de los mensajes de datos y de la firma electrónica,[1] la experiencia práctica demuestra que la simple existencia de un documento firmado electrónicamente no garantiza por sí misma la eficacia jurídica ni la fuerza probatoria del acto. El verdadero desafío consiste en demostrar, incluso muchos años después de su celebración, la identidad de los participantes, la integridad del documento, la fecha de su existencia y la conservación inalterada de la evidencia electrónica. El presente trabajo sostiene que la formalidad jurídica en el entorno digital no se satisface exclusivamente mediante la firma electrónica. Se propone que la verdadera formalidad funcional del acto jurídico digital descansa en una cadena de confianza integrada por identidad digital, firma electrónica, sellado digital de tiempo, constancia de conservación de mensajes de datos y capacidad de verificación futura de la evidencia. A partir del análisis de la teoría general del acto jurídico, del principio de equivalencia funcional y

* Egresado de la Facultad de Derecho de la Universidad Panamericana, con maestría en Ciencias Jurídicas por la misma Facultad. Notario 230 de la Ciudad de México desde 1999 y notario del Patrimonio Inmobiliario Federal. Mediador privado certificado por el Centro de Justicia Alternativa. abazua@notaria230.com.mx

1 Ver Código de Comercio, art. 89 bis.

de la evolución de las formalidades documentales, se construyen las bases conceptuales necesarias para comprender el funcionamiento jurídico de la contratación electrónica y los mecanismos tecnológicos que actualmente permiten dotarla de seguridad jurídica.

PALABRAS CLAVE

acto jurídico digital; firma electrónica; mensaje de datos; identidad digital; prueba electrónica; cadena de confianza digital.

ABSTRACT

Digital transformation has profoundly altered the way in which legal acts are entered into, documented, and proved. The replacement of paper by data messages, and of the handwritten signature by electronic mechanisms, has forced a rethinking of written form, documentary authenticity, and evidentiary effectiveness. Although Mexican legislation has long recognized the validity of data messages and electronic signatures, an electronically signed document does not in itself guarantee the probative force of the act: the real challenge is to demonstrate, even years later, the identity of the parties, the integrity of the document, the date of its existence, and the unaltered preservation of the evidence. This paper argues that the functional formality of the digital juridical act rests on a chain of trust comprising digital identity, electronic signature, digital time-stamping, certificates of preservation of data messages, and the capacity for future verification, and it lays the conceptual foundations for understanding electronic contracting and the technological mechanisms that endow it with legal certainty.

KEYWORDS

Digital Juridical Act; Electronic Signature; Data Message; Digital Identity; Electronic Evidence; Digital Chain of Trust.

I. Introducción

Pocas instituciones jurídicas han experimentado una transformación tan profunda durante las últimas décadas como las relacionadas con la documentación y prueba de los actos jurídicos.

Durante siglos, la seguridad jurídica descansó sobre dos pilares fundamentales: el documento escrito y la firma autógrafa. La materialidad del papel proporcionaba permanencia y estabilidad, mientras que la firma manuscrita permitía atribuir el contenido del documento a una persona determinada. La combinación de ambos elementos hizo posible el desarrollo del comercio, la contratación privada y la administración pública moderna.

Sin embargo, el surgimiento de Internet y la masificación de las tecnologías digitales alteraron radicalmente este paradigma. Actualmente, millones de actos jurídicos son celebrados diariamente mediante plataformas electrónicas,

aplicaciones móviles, portales gubernamentales y sistemas automatizados de contratación. En numerosos casos, el documento físico ha desaparecido por completo.

Esta transformación tecnológica generó una preocupación natural en los operadores jurídicos. Si desaparece el papel, ¿cómo se satisface la forma escrita? Si ya no existe una firma manuscrita, ¿cómo puede acreditarse la identidad del firmante? Si los documentos digitales pueden editarse y copiarse indefinidamente, ¿cómo puede garantizarse su integridad? Y quizá la pregunta más importante de todas: ¿cómo podrá probarse un acto jurídico electrónico dentro de diez o quince años cuando surja una controversia judicial?

La respuesta del derecho contemporáneo consistió inicialmente en reconocer el principio de equivalencia funcional.[2] Conforme a este principio, los mensajes de datos pueden cumplir las mismas funciones jurídicas que tradicionalmente desempeñaban los documentos físicos. Sin embargo, la práctica ha demostrado que la equivalencia funcional constituye únicamente el punto de partida del problema.

La verdadera dificultad no consiste en determinar si un documento electrónico es válido, sino en establecer si será probatoriamente eficaz cuando deba ser sometido al escrutinio de un tribunal años después de haber sido generado.

Este trabajo sostiene que la formalidad jurídica digital debe entenderse desde una perspectiva distinta a la utilizada tradicionalmente para los documentos físicos. Mientras que en el mundo analógico la confianza descansaba principalmente en el documento y en la firma autógrafa, en el entorno digital la confianza depende de una infraestructura tecnológica mucho más compleja.

Por ello se propone la noción de *cadena de confianza digital* como una nueva categoría doctrinal destinada a explicar los mecanismos mediante los cuales los actos jurídicos electrónicos adquieren seguridad jurídica y eficacia probatoria.

II. Los actos jurídicos y los negocios jurídicos en el derecho mexicano

La teoría general del acto jurídico[3] constituye el punto de partida obligado para comprender las implicaciones jurídicas de la digitalización.

Tradicionalmente, la doctrina distingue entre hechos jurídicos y actos jurídicos. Los primeros producen consecuencias de derecho independientemente de

2 Ver Código de Comercio, art. 89.

3 Jorge Alfredo DOMÍNGUEZ MARTÍNEZ, *Derecho civil: parte general* (México: Porrúa).

la voluntad humana; los segundos requieren una manifestación consciente de voluntad encaminada precisamente a producir efectos jurídicos.

Dentro de esta categoría, el negocio jurídico representa una construcción doctrinal particularmente relevante. Puede definirse como una declaración o conjunto de declaraciones de voluntad destinadas a crear, transmitir, modificar o extinguir relaciones jurídicas conforme a los fines perseguidos por quienes intervienen en el acto.

La celebración de un contrato de promesa, de prestación de servicios, el otorgamiento de una carta poder, la contratación mercantil o la aceptación de una oferta constituyen ejemplos típicos de negocios jurídicos.

En el sistema jurídico mexicano, para que un acto jurídico exista resulta indispensable la presencia de dos elementos fundamentales:[4]

1. La declaración de la voluntad o el consentimiento

La declaración de la voluntad o el consentimiento representa la manifestación de aquella o la coincidencia de voluntades necesaria para la creación y celebración del acto. Puede manifestarse de manera expresa o tácita, siempre que resulte inequívoca la intención de producir consecuencias jurídicas.

Desde una perspectiva funcional, el consentimiento constituye el elemento que mayores transformaciones ha experimentado como consecuencia de la digitalización. La aceptación que anteriormente se manifestaba mediante una firma autógrafa puede hoy expresarse mediante mecanismos electrónicos de diversa naturaleza.

2. Objeto

Todo acto jurídico requiere una materia sobre la cual recaigan sus efectos. El objeto debe ser posible física y jurídicamente, además de encontrarse dentro del comercio cuando así lo exija la naturaleza del acto.

La digitalización no ha modificado sustancialmente este elemento, aunque sí ha ampliado significativamente las posibilidades de contratación sobre bienes intangibles y activos digitales.

Una vez satisfechos los elementos de existencia, el acto jurídico debe cumplir determinados requisitos de validez;[5] legalmente se reconocen: i) capacidad legal de las partes; ii) ausencia de vicios del consentimiento; iii) licitud en el objeto, motivo o fin; iv) observancia de la forma exigida por la ley.

---

4 Ver Código Civil Federal, art. 1794.
5 Ver Código Civil Federal, art. 1795.

Es precisamente este último requisito el que ha sufrido la transformación más profunda en la era digital.

III. La función jurídica de las formalidades

Con frecuencia las formalidades jurídicas son percibidas como simples exigencias burocráticas carentes de utilidad práctica. Sin embargo, esta visión desconoce la función esencial que desempeñan dentro del sistema jurídico.

Las formalidades surgieron históricamente como mecanismos destinados a generar certeza respecto de la existencia y contenido de los actos jurídicos. Su finalidad nunca fue obstaculizar la contratación, sino reducir los riesgos derivados de la incertidumbre.[6]

Desde una perspectiva funcional, las formalidades cumplen al menos cinco objetivos fundamentales.

A. Función de exteriorización. La forma permite transformar una voluntad interna en una manifestación objetivamente perceptible. Sin algún mecanismo de exteriorización resultaría imposible distinguir entre una simple intención y una verdadera declaración de voluntad jurídicamente relevante.

B. Función de autenticación. Las formalidades permiten asociar la declaración de voluntad con una persona determinada. Esta función explica históricamente la importancia de la firma autógrafa y, en la actualidad, de los mecanismos de autenticación electrónica.

C. Función de conservación. La forma permite preservar la información jurídica a través del tiempo. Esta función adquiere especial relevancia cuando existe una separación temporal significativa entre la celebración del acto y la necesidad de demostrar su existencia.

D. Función probatoria. Quizá la función más importante de todas consiste en facilitar la acreditación futura del acto jurídico. La forma genera evidencia susceptible de ser presentada ante terceros o autoridades cuando surja una controversia.

E. Función de seguridad jurídica. Finalmente, las formalidades contribuyen a reducir la incertidumbre y los costos de transacción, fortaleciendo la confianza de los participantes en el tráfico jurídico.

Lo relevante para efectos de este trabajo es advertir que ninguna de estas funciones desaparece en el entorno digital. Por el contrario, todas ellas subsisten. Lo que cambia son los mecanismos tecnológicos utilizados para satisfacerlas.

---

6 Rafael ROJINA VILLEGAS, *Derecho civil mexicano: teoría general de las obligaciones* (México: Porrúa).

IV. Actos consensuales, formales y solemnes en la era digital

La doctrina clásica distingue entre actos consensuales, actos formales y actos solemnes.[7]

Los actos consensuales se perfeccionan mediante el simple consentimiento de las partes. La ley no exige una forma específica para su validez.

Los actos formales requieren el cumplimiento de determinadas formalidades establecidas por el legislador. La forma se convierte en un requisito necesario para la eficacia o validez del acto.

Finalmente, los actos solemnes exigen formalidades cuya observancia resulta indispensable para la propia existencia del acto jurídico.

La digitalización no ha eliminado esta clasificación.

Sin embargo, obliga a replantear la manera en que dichas formalidades pueden cumplirse.

Cuando la ley exige que un acto conste por escrito, la pregunta relevante ya no consiste en determinar si existe un documento físico, sino en establecer si el medio utilizado cumple adecuadamente las funciones que históricamente justificaron la exigencia de forma escrita.

Esta reflexión conduce directamente al principio de equivalencia funcional, cuya importancia resulta fundamental para comprender el régimen jurídico contemporáneo de los mensajes de datos.

V. Del papel al mensaje de datos: el principio de equivalencia funcional

Uno de los errores conceptuales más frecuentes en materia de contratación electrónica consiste en identificar la forma escrita con el papel. En realidad, la ley nunca protegió el papel como objeto material. Lo que históricamente ha protegido el ordenamiento jurídico es algo distinto: la posibilidad de conservar información de manera estable, accesible y verificable.

Durante siglos, el papel fue simplemente la tecnología documental más eficiente para cumplir ese propósito.

La aparición de los medios electrónicos obligó a replantear esta concepción tradicional. Para resolver el problema, la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional desarrolló el principio de equivalencia funcional, posteriormente incorporado a numerosas legislaciones nacionales.

---

7 *Ibid.*

Conforme a este principio, los mensajes de datos pueden satisfacer los mismos objetivos jurídicos que los documentos físicos siempre que permitan conservar la información y consultarla posteriormente.

La importancia de esta idea no puede ser subestimada.

Significa que el derecho contemporáneo ha dejado de proteger un soporte documental específico para concentrarse en las funciones que dicho soporte desempeña.

La consecuencia es trascendental: la ley protege la información jurídicamente relevante y no el medio físico que la contiene[8].

Este cambio conceptual constituye el fundamento sobre el cual descansa todo el régimen jurídico de la contratación electrónica moderna y permite comprender por qué los mensajes de datos pueden producir los mismos efectos jurídicos que los documentos tradicionales.

VI. La firma electrónica como mecanismo de atribución jurídica

La firma constituye una de las instituciones jurídicas más antiguas y relevantes dentro de la teoría de la prueba documental. Mucho antes de la aparición de las tecnologías digitales, la firma autógrafa desempeñaba una función esencial: vincular una declaración de voluntad con una persona determinada.

Desde una perspectiva funcional, la firma cumple tres objetivos fundamentales.

En primer lugar, permite identificar al autor de la declaración. En segundo término, acredita la intención de obligarse respecto del contenido del documento. Finalmente, permite atribuir jurídicamente al firmante las consecuencias derivadas del acto celebrado.

Estas funciones permanecen inalteradas en el entorno digital. Lo que cambia es el mecanismo utilizado para satisfacerlas.

La transición tecnológica obliga a abandonar una visión gráfica o caligráfica de la firma para sustituirla por una visión funcional. La pregunta jurídicamente relevante ya no consiste en determinar si existe un trazo manuscrito sobre un soporte físico, sino en establecer si existen elementos suficientes para atribuir de manera confiable la declaración de voluntad a una persona determinada.

Bajo esta perspectiva, la firma electrónica no constituye una categoría excepcional dentro del derecho. Se trata simplemente de un mecanismo tecnológi-

8 Véanse Código de Comercio, arts. 89, 89 bis y 93, así como la *Ley Modelo de Comercio Electrónico* de la CNUDMI de 1996, que incorporó el principio de equivalencia funcional entre documentos físicos y mensajes de datos.

co destinado a cumplir las mismas funciones que históricamente desempeñó la firma autógrafa.

Sin embargo, no todas las firmas electrónicas ofrecen el mismo nivel de certeza.

Por ello resulta indispensable distinguir entre firma electrónica simple y firma electrónica avanzada.

VII. La firma electrónica simple y el problema de la identidad

La legislación mexicana reconoce la validez jurídica de la firma electrónica simple.[9] Esta categoría comprende cualquier conjunto de datos electrónicos utilizados para identificar a una persona y expresar su aceptación respecto de determinada información.

Dentro de esta categoría pueden ubicarse: i) la aceptación mediante clic;[10] ii) los códigos OTP enviados por SMS;[11] iii) las contraseñas;[12] iv) los correos electrónicos;[13] v) determinados mecanismos biométricos;[14] vi) las firmas manuscritas

---

9 Ver Código de Comercio, art. 89.

10 La aceptación mediante clic (click-wrap agreement) consiste en la manifestación expresa de voluntad realizada por el usuario al seleccionar un botón o casilla de aceptación —por ejemplo, «Acepto los términos y condiciones»— dentro de una plataforma electrónica. Su eficacia jurídica no deriva del clic por sí mismo, sino del conjunto de evidencias que permiten acreditar que determinada persona realizó dicha acción, tales como la identificación del usuario, la fecha y hora de la operación, la dirección IP, el identificador de la sesión y los registros de auditoría del sistema. Es el mecanismo de contratación electrónica más utilizado en el comercio electrónico contemporáneo.

11 Los códigos OTP (One-Time Password) son claves de autenticación de un solo uso generadas aleatoriamente y enviadas al usuario por un canal previamente asociado con su identidad, como mensajes SMS, correo electrónico o aplicaciones autenticadoras. Su finalidad consiste en incorporar un segundo factor de autenticación que permita incrementar el grado de certeza respecto de la identidad del usuario. Desde la perspectiva jurídica, el OTP no constituye por sí mismo una firma electrónica avanzada, sino un mecanismo complementario de autenticación que fortalece la atribución de la declaración de voluntad.

12 Las contraseñas (passwords) constituyen uno de los mecanismos de autenticación electrónica más utilizados en los sistemas informáticos. Consisten en una secuencia de caracteres conocida únicamente por el usuario y el sistema informático, cuya finalidad es acreditar que quien pretende acceder a una cuenta o realizar una determinada operación conoce un secreto previamente establecido. Desde la perspectiva jurídica, la contraseña no constituye por sí misma una firma electrónica avanzada, sino un mecanismo de autenticación que puede formar parte de una firma electrónica simple cuando es utilizada para manifestar electrónicamente la voluntad del usuario. Su eficacia probatoria dependerá de las evidencias adicionales que permitan atribuir razonablemente su utilización a una persona determinada, tales como registros de acceso, direcciones IP, identificadores del dispositivo, sellos de tiempo, bitácoras de auditoría y demás elementos tecnológicos generados durante la operación.

13 El correo electrónico puede constituir un mecanismo válido de manifestación de voluntad

digitalizadas;[15] vii) las aceptaciones realizadas mediante aplicaciones móviles.[16]

La autenticación multifactor (Multi-Factor Authentication, MFA) consiste en exigir al usuario la acreditación simultánea de dos o más categorías independientes de autenticación antes de permitir la celebración del acto jurídico. Estos factores pueden pertenecer a tres categorías: (i) algo que el usuario conoce, como una contraseña; (ii) algo que posee, como un teléfono móvil o un token criptográfico; y (iii) algo que es, como una característica biométrica. La utilización de múltiples factores incrementa significativamente el grado de certeza respecto de la identidad del usuario y fortalece la eficacia probatoria de la firma electrónica simple.

La principal ventaja de estos mecanismos consiste en su simplicidad operativa.

Sin embargo, su principal debilidad aparece cuando surge una controversia.

En tales casos, la pregunta fundamental es:

¿Cómo demostrar que efectivamente fue determinada persona quien realizó la acción correspondiente?

La experiencia demuestra que el verdadero problema de la contratación electrónica no es un problema de firma. Es un problema de identidad. La validez jurídica de una aceptación electrónica rara vez es cuestionada. Lo que normal-

---

cuando del contenido del mensaje y de las circunstancias que lo rodean sea posible identificar razonablemente al remitente y acreditar su intención de obligarse. Su fuerza probatoria dependerá de elementos adicionales como encabezados (headers), registros del servidor, autenticación de la cuenta, historial de comunicaciones y demás evidencia tecnológica que permita atribuir el mensaje a una persona determinada.

14 Los mecanismos biométricos utilizan características físicas o conductuales propias de una persona para efectos de autenticación, tales como huellas dactilares, reconocimiento facial, reconocimiento del iris, geometría de la mano, reconocimiento de voz o patrones de escritura. En la contratación electrónica, estos mecanismos generalmente no sustituyen a la firma electrónica avanzada, sino que funcionan como factores adicionales de autenticación destinados a fortalecer la atribución de identidad del firmante.

15 La firma manuscrita digitalizada consiste en la reproducción electrónica de una firma autógrafa mediante escaneo, fotografía o captura sobre dispositivos electrónicos, como tabletas digitalizadoras. A diferencia de la firma electrónica avanzada, este mecanismo no incorpora necesariamente procesos criptográficos destinados a proteger la integridad del documento ni la identidad del firmante. Su eficacia probatoria dependerá del conjunto de evidencias que acompañen al documento y de las circunstancias particulares de cada caso.

16 Diversas aplicaciones móviles permiten celebrar actos jurídicos mediante la autenticación previa del usuario y la posterior confirmación de su voluntad a través de botones de aceptación, validaciones biométricas, códigos OTP o mecanismos equivalentes. Jurídicamente, la manifestación de voluntad no deriva de la aplicación en sí misma, sino de la combinación de evidencias tecnológicas generadas durante la operación, tales como registros de autenticación, identificadores del dispositivo, direcciones IP, geolocalización, sellos de tiempo y bitácoras de auditoría.

mente se discute es si efectivamente fue realizada por la persona a quien se atribuye.

Es importante advertir que ninguno de estos mecanismos constituye una categoría jurídica autónoma. Todos son técnicas de autenticación o de manifestación electrónica de la voluntad cuyo valor probatorio dependerá del conjunto de evidencias tecnológicas que permitan atribuir razonablemente el acto a una persona determinada. En consecuencia, la diferencia entre una firma electrónica simple y una firma electrónica avanzada no radica en el dispositivo utilizado por el usuario, sino en el nivel de confianza jurídica y técnica que la infraestructura subyacente es capaz de proporcionar.

Esta observación resulta particularmente importante porque permite comprender que la evolución tecnológica de las firmas electrónicas ha estado dirigida fundamentalmente a resolver problemas de atribución de identidad.

En otras palabras, la historia de la firma electrónica es esencialmente la historia de la construcción de mecanismos cada vez más robustos de identificación digital.

VIII. La firma electrónica avanzada y la construcción de la identidad digital

La firma electrónica avanzada representa el nivel más sofisticado de atribución jurídica disponible actualmente en los sistemas de contratación electrónica.[17] A diferencia de la firma electrónica simple, su funcionamiento no depende exclusivamente de evidencias circunstanciales. Descansa sobre procedimientos criptográficos matemáticamente verificables.

Su principal finalidad consiste en reducir significativamente la posibilidad de que una persona niegue posteriormente haber intervenido en una determinada operación.

Desde una perspectiva jurídica, la firma electrónica avanzada permite acreditar simultáneamente tres circunstancias:

Primera, que una persona determinada intervino en la operación.

Segunda, que el contenido del documento no fue modificado después de la firma.

Tercera, que la evidencia asociada puede ser verificada objetivamente por terceros.

La importancia de este mecanismo no radica únicamente en la seguridad informática que proporciona. Su verdadera trascendencia consiste en que permite

17 Ley de Firma Electrónica Avanzada, arts. 2, 7, 8 y correlativos.

construir una identidad jurídica digital verificable.

Durante siglos la identidad jurídica descansó en elementos físicos: i) presencia personal; ii) documentos oficiales; iii) reconocimiento de firmas; iv) testimonios.

La firma electrónica avanzada traslada esos mecanismos al entorno digital mediante procedimientos criptográficos. La identidad deja de depender exclusivamente de la percepción humana y pasa a sustentarse en evidencia matemáticamente verificable.

IX. Infraestructura de clave pública (PKI)

La firma electrónica avanzada resulta incomprensible sin entender previamente la infraestructura tecnológica que la hace posible. Dicha infraestructura es conocida internacionalmente como Public Key Infrastructure o PKI.[18] La PKI constituye un sistema destinado a administrar identidades digitales mediante mecanismos criptográficos. Su funcionamiento descansa sobre la existencia de dos claves matemáticamente relacionadas:

Clave privada. La clave privada permanece bajo el control exclusivo del titular. Su función consiste en generar firmas electrónicas. Debe mantenerse confidencial en todo momento.

Clave pública. La clave pública puede ser conocida por cualquier tercero. Su función consiste en verificar las firmas generadas mediante la clave privada correspondiente.

La seguridad del sistema depende precisamente de la imposibilidad práctica de reconstruir la clave privada a partir de la clave pública. Esta característica permite generar sistemas de confianza escalables y verificables.

18 RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile*.

X. La función hash[19]: la identidad criptográfica del documento

Con frecuencia se afirma que la firma electrónica consiste en «firmar un documento». Técnicamente esto no es exacto. Lo que realmente se firma es la huella digital del documento.

Dicha huella se obtiene mediante funciones criptográficas conocidas como funciones hash.[20]

Un hash puede definirse como un resumen matemático único generado a partir del contenido de un documento. Entre los algoritmos más utilizados actualmente destacan: SHA-256, SHA-384 y SHA-512.[21]

---

19 Una función hash es un algoritmo criptográfico que transforma un conjunto de datos de cualquier tamaño en una secuencia alfanumérica de longitud fija, denominada huella digital (hash, digest o message digest). esta huella constituye una representación matemática única del contenido del documento. entre los algoritmos más utilizados actualmente se encuentran SHA-256, SHA-384 y SHA-512, desarrollados conforme al estándar FIPS 180-4 del national institute of standards and technology (NIST). las funciones hash poseen cuatro propiedades esenciales para el derecho: (i) determinismo, pues un mismo documento siempre genera la misma huella; (ii) extrema sensibilidad, ya que la modificación de un solo bit produce una huella completamente distinta (efecto avalancha); (iii) resistencia a la preimagen, que impide reconstruir el documento original a partir de su hash; y (iv) resistencia a las colisiones, que hace computacionalmente inviable encontrar dos documentos distintos que produzcan la misma huella. desde una perspectiva jurídica, el hash no protege el contenido del documento, sino su integridad, ya que permite verificar objetivamente que el documento presentado en un momento posterior es exactamente el mismo que existía cuando se generó la huella criptográfica.

20 National Institute of Standards and Technology (NIST), FIPS PUB 180-4, *Secure Hash Standard*.

21 SHA (Secure Hash Algorithm) es una familia de funciones hash criptográficas desarrollada por la National Security Agency (NSA) de los Estados Unidos y estandarizada por el National Institute of Standards and Technology (NIST) mediante la publicación FIPS PUB 180-4, Secure Hash Standard (SHS). Los algoritmos pertenecientes a la familia SHA-2 son actualmente los más utilizados en aplicaciones jurídicas, financieras y gubernamentales para garantizar la integridad de documentos electrónicos. par SHA-256 genera una huella criptográfica de 256 bits (32 bytes), representada habitualmente mediante una cadena hexadecimal de 64 caracteres. Es el algoritmo de uso más extendido en plataformas de firma electrónica, infraestructura de clave pública (PKI), certificados digitales, sellos digitales de tiempo, conservación de mensajes de datos, blockchain y protocolos de seguridad en Internet, debido a que ofrece un elevado nivel de seguridad con un costo computacional relativamente bajo. par SHA-384 produce una huella de 384 bits (48 bytes), representada mediante 96 caracteres hexadecimales. Se utiliza principalmente en aplicaciones que requieren un mayor margen de seguridad criptográfica o que operan bajo estándares de seguridad reforzada. par SHA-512 genera una huella de 512 bits (64 bytes), representada mediante 128 caracteres hexadecimales. Es el algoritmo con mayor longitud de salida dentro de la familia SHA-2 y se emplea en infraestructuras críticas, sistemas gubernamentales, militares y financieros donde se requiere el máximo nivel de resistencia frente a ataques criptográficos actualmente conocidos.

Estas funciones poseen características extraordinariamente relevantes desde una perspectiva jurídica:

Unicidad práctica. La probabilidad de que dos documentos distintos generen la misma huella resulta extraordinariamente baja.

Irreversibilidad. A partir del hash no es posible reconstruir el contenido original del documento.

Sensibilidad absoluta. La modificación de un solo carácter genera una huella completamente distinta. Esta última característica convierte al hash en una herramienta excepcional para proteger la integridad documental.

Desde una perspectiva jurídica, la diferencia entre estos algoritmos no radica en que uno sea «más válido» que otro, sino en el nivel de seguridad criptográfica que proporcionan. Todos cumplen la misma función: generar una identidad matemática única del documento que permita verificar objetivamente su integridad. En la actualidad, SHA-256 constituye el estándar predominante en la mayoría de los sistemas de firma electrónica avanzada, sellado digital de tiempo y conservación de mensajes de datos utilizados en México.

Estos algoritmos no generan simplemente una cadena de caracteres; generan la identidad criptográfica irrepetible del documento.

Considere que una modificación aparentemente insignificante —como agregar una coma, un espacio o cambiar una sola letra— produce una huella criptográfica completamente distinta. Esta propiedad, conocida como «efecto avalancha», constituye el fundamento técnico que permite utilizar las funciones hash como mecanismo de verificación objetiva de la integridad documental.

Así podemos afirmar que el hash funciona como una especie de ADN digital del documento. Si la huella coincide, puede concluirse razonablemente que el documento permanece íntegro. Si la huella cambia, puede afirmarse que el documento fue modificado.

XI. Certificados digitales y atribución de identidad

La existencia de una clave pública y una clave privada no resulta suficiente para construir confianza jurídica. Todavía subsiste una pregunta fundamental:

¿Cómo puede un tercero saber que determinada clave pública pertenece realmente a determinada persona?

La respuesta se encuentra en los certificados digitales. Un certificado digital es un documento electrónico emitido por una entidad de confianza (como el Prestador de Servicios de Certificación) que vincula una identidad jurídica con una clave pública específica. Desde una perspectiva funcional, el certificado cumple en el entorno digital una función similar a la que desempeñan los documentos oficiales de identidad en el mundo físico. Permite que terceros confíen

razonablemente en que determinada clave pública pertenece efectivamente a determinada persona.

Por ello, los certificados constituyen uno de los pilares fundamentales de toda infraestructura de confianza digital. Sin ellos, las firmas electrónicas avanzadas carecerían de un mecanismo robusto de atribución de identidad.

XII. Los prestadores de servicios de certificación como terceros de confianza digital

La contratación electrónica moderna requiere la intervención de actores especializados cuya función consiste en generar confianza dentro del ecosistema digital. En México, ese papel corresponde a los Prestadores de Servicios de Certificación (PSC). Desde una perspectiva jurídica, los PSC no certifican la validez del acto jurídico. Tampoco sustituyen la voluntad de las partes. Su función es diferente: Los PSC certifican evidencia tecnológica.

Esta distinción resulta fundamental para comprender su verdadera naturaleza jurídica. La intervención del PSC permite incorporar al acto digital una capa adicional de confianza basada en evidencia verificable por terceros. Entre las actividades que habitualmente realizan destacan: i) validación de identidad; ii) emisión de certificados de firma electrónica avanzada; iii) validación de dichos certificados; iv) sellado digital de tiempo; v) generación de constancias de conservación de mensajes de datos; vi) administración de bitácoras; y vii) la más importante para nuestro tema, la preservación de evidencia tecnológica.

El PSC no conserva únicamente documentos. Conserva la capacidad de demostrar que dichos documentos permanecen íntegros. Esta afirmación constituye una de las ideas centrales de este trabajo.

La verdadera utilidad de un PSC *no aparece el día en que se firma el documento. Aparece años después, cuando surge una controversia. En ese momento, los registros conservados por el* PSC *permiten reconstruir objetivamente la evidencia tecnológica original.*

XIII. Hacia una teoría de la identidad digital verificable

La doctrina jurídica tradicional construyó gran parte de sus mecanismos de confianza sobre la presencia física de las personas.

La digitalización obliga a sustituir progresivamente esa confianza presencial por mecanismos de confianza verificable. La identidad digital verificable puede definirse como el conjunto de evidencias técnicas y jurídicas que permiten atribuir razonablemente una determinada actuación electrónica a una persona específica. La firma electrónica avanzada constituye una herramienta funda-

mental para alcanzar este objetivo. Sin embargo, la identidad digital no depende exclusivamente de la firma. También intervienen: i) procedimientos de identificación; ii) certificados digitales; iii) bitácoras de autenticación; iv) evidencias biométricas; v) registros de actividad; vi) mecanismos de conservación.

La identidad digital surge de la combinación de todos estos elementos.

Precisamente por ello, el estudio de la firma electrónica no puede realizarse de manera aislada. Debe analizarse como parte de una infraestructura más amplia de confianza digital.

Y es precisamente esa infraestructura la que será objeto de estudio en los capítulos siguientes al abordar los sellos digitales de tiempo, la NOM-151, la conservación de mensajes de datos y el problema de la prueba del acto jurídico digital.

XIV. Los sellos digitales de tiempo y la construcción de la fecha cierta electrónica

La firma electrónica avanzada responde a una pregunta fundamental: ¿Quién firmó?

Sin embargo, la seguridad jurídica de un acto digital exige responder una segunda interrogante igualmente relevante: ¿Cuándo existía exactamente el documento firmado?

En el mundo físico esta función era cumplida tradicionalmente por diversos mecanismos de fecha cierta. La protocolización notarial, la ratificación de firmas, el registro público o incluso la simple existencia material de un documento en determinada fecha permitían generar evidencia temporal relativamente confiable.

En el entorno digital la situación es distinta. La fecha que aparece impresa dentro de un documento electrónico carece por sí misma de valor técnico suficiente para demostrar que dicho documento existía efectivamente en ese momento. Cualquier usuario podría modificarla posteriormente. Por esta razón surgieron los sistemas de sellado digital de tiempo.

A. Fundamento tecnológico: Los sellos digitales de tiempo se encuentran regulados internacionalmente por el estándar RFC 3161.[22] Su funcionamiento es relativamente sencillo desde una perspectiva conceptual. Cuando una persona firma electrónicamente un documento, el sistema genera primero una huella digital o hash del archivo. Esa huella es enviada a una Autoridad de Sellado de Tiempo (Time Stamping Authority o TSA), que en el caso mexicano es un

22 C. ADAMS *et al.*, RFC 3161, *Internet X.509 Public Key Infrastructure Time-Stamp Protocol*.

Prestador de Servicios de Certificación acreditado para ello por la Secretaría de Economía. La TSA incorpora una referencia temporal obtenida de fuentes confiables y genera un token criptográfico firmado digitalmente. El resultado es una evidencia técnicamente verificable de que una determinada huella digital existía en una fecha y hora específicas.

Lo importante es advertir que la TSA no recibe necesariamente el documento completo. Recibe únicamente la huella digital. Por ello puede certificar la existencia temporal del documento sin conocer su contenido.

B. Fundamento jurídico:[23] Desde una perspectiva jurídica, el sello digital de tiempo constituye probablemente el mecanismo tecnológico más cercano a la noción tradicional de fecha cierta. No acredita quién firmó. No acredita la validez del acto. No acredita la capacidad de las partes. Lo que acredita es algo distinto:

Que una determinada evidencia documental existía en un momento específico.

Esta función resulta extraordinariamente relevante cuando transcurren varios años entre la celebración del acto y su eventual presentación en juicio.

XV. La conservación de mensajes de datos, la NOM-151 y la preservación de la identidad criptográfica del documento

La principal contribución de la NOM-151-SCFI-2016 ha sido frecuentemente malinterpretada. En numerosos foros jurídicos se afirma que la NOM-151 constituye un requisito para la validez de los actos jurídicos digitales. A juicio de este autor, esa afirmación es incorrecta. La validez de un acto jurídico continúa dependiendo de los elementos tradicionales establecidos por el derecho civil y mercantil: i) consentimiento; ii) objeto; iii) capacidad; iv) ausencia de vicios; v) licitud; vi) forma cuando esta sea exigida.

La NOM-151 no interviene en ninguno de esos elementos.[24] Su función es distinta. La NOM-151 constituye un mecanismo de preservación de evidencia. Su objetivo principal consiste en fortalecer la eficacia probatoria de los mensajes de datos mediante procedimientos técnicos destinados a garantizar: i) integridad; ii) disponibilidad; iii) accesibilidad; iv) trazabilidad; v) verificabilidad.

Por ello puede afirmarse que la NOM-151 no resuelve un problema de validez. Resuelve un problema de prueba. Esta distinción resulta fundamental para comprender correctamente su función dentro del sistema jurídico mexicano.

---

23 Ver Código de Comercio, art. 89.

24 La NOM-151 regula procedimientos de conservación y digitalización documental. Su incumplimiento puede afectar la fuerza probatoria de la evidencia digital, pero no necesariamente la existencia o validez intrínseca del acto jurídico celebrado.

La verdadera función de las constancias de conservación

Con frecuencia se piensa que una constancia de conservación sirve para almacenar documentos. En realidad, su función es mucho más sofisticada. La constancia no conserva una copia. Conserva la capacidad de verificar. La diferencia es enorme. Almacenar una copia permite recuperar un archivo. Conservar la evidencia criptográfica permite demostrar que dicho archivo permanece íntegro respecto de una versión previamente existente. Desde una perspectiva jurídica, esta segunda función es mucho más importante que la primera.

Desde la perspectiva de la prueba electrónica, el hash puede entenderse como la identidad criptográfica del documento. Así como las personas físicas poseen una identidad jurídica que permite distinguirlas de las demás, cada documento electrónico posee una identidad matemática única representada por su huella criptográfica. La conservación de esa identidad permite verificar, incluso muchos años después de celebrado el acto jurídico, que el documento ofrecido como prueba permanece íntegro respecto del documento originalmente firmado.

Lo verdaderamente importante no es conservar una copia del documento, sino preservar su identidad criptográfica. Mientras la huella digital originalmente generada permanezca verificable, será posible demostrar objetivamente que el documento presentado en juicio corresponde al mismo acto jurídico que fue firmado electrónicamente.

Principio de identidad criptográfica del documento. Todo documento electrónico susceptible de producir efectos jurídicos posee una identidad criptográfica única, representada por su función hash, cuya preservación permite verificar objetivamente la integridad del documento a lo largo de todo su ciclo de vida y constituye el fundamento técnico de su eficacia probatoria.

Nuestro tema, complementa perfectamente la tesis que proponemos más adelante sobre la cadena de confianza digital: la cadena garantiza la confianza; el hash proporciona la identidad criptográfica del documento; y el PSC, mediante el Sello Digital de Tiempo (SDT) y la Constancia de Conservación de Mensajes de Datos (CCMD), preserva esa identidad desde el instante mismo del nacimiento del acto jurídico para que pueda ser verificada cuando, años después, deba producir efectos en juicio.

XVI. El problema del *delay* probatorio

La experiencia demuestra que el verdadero desafío de los actos jurídicos digitales no aparece el día de la firma. Aparece años después. Un contrato puede celebrarse hoy y llegar a juicio dentro de: cinco, diez o quince años; incluso más.

Este fenómeno puede denominarse *delay* probatorio. La separación temporal entre la celebración del acto y su acreditación judicial genera una serie de interrogantes fundamentales: i) ¿Quién firmó?, ii) ¿Cuándo se firmó?, iii) ¿El documento sigue siendo el mismo?, iv) ¿Fue modificado? v) ¿Los certificados continúan siendo verificables? vi) ¿La evidencia tecnológica sigue existiendo?

En el mundo físico estas preguntas suelen resolverse mediante inspección documental, reconocimiento de firmas o prueba pericial caligráfica.

En el entorno digital el problema adquiere una dimensión completamente distinta. La prueba depende de elementos tecnológicos que pueden desaparecer, corromperse o volverse inaccesibles con el paso del tiempo. Precisamente por ello la preservación de evidencia adquiere una relevancia central. De ahí que propongamos lo que hemos denominado la «*cadena de confianza digital*» y el «*expediente probatorio autocontenido*».

1. La insuficiencia de la firma electrónica aislada

Una de las ideas fundamentales que este trabajo pretende demostrar consiste en que la firma electrónica avanzada, por sí sola, no resuelve completamente el problema probatorio.

La firma acredita identidad. Pero no necesariamente garantiza la conservación futura de la evidencia. Puede existir una firma perfectamente válida sobre un documento cuya trazabilidad documental resulte imposible de reconstruir años después.

Por ello la firma constituye únicamente uno de los elementos de una infraestructura probatoria mucho más amplia.

2. Del documento electrónico simple al documento probatoriamente robusto

Uno de los errores más frecuentes en materia de contratación electrónica consiste en asumir que todos los documentos digitales poseen la misma eficacia probatoria. En realidad, existe una diferencia sustancial entre la validez jurídica de un documento y su fortaleza probatoria.

Puede existir un documento jurídicamente válido cuya capacidad de acreditación futura resulte limitada. Desde esta perspectiva, es posible distinguir al menos cuatro niveles de robustez documental.

Nivel 1. Documento electrónico simple. Ejemplo: PDF[25] enviado por correo. Permite demostrar un indicio de su existencia. Difícil atribución.

---

25 PDF corresponde a Portable Document Format (Formato de Documento Portátil), un formato de archivo desarrollado por Adobe Systems en 1993, con la finalidad de preservar la apariencia y estructura de un documento con independencia del sistema operativo, software o dispositivo utilizado para visualizarlo.



DIAGRAMA 1. El problema probatorio del documento firmado electrónicamente y su solución.

Nivel 2. Documento firmado electrónicamente. Ejemplo: OTP. - correo validado. Mejor atribución. Integridad limitada.

Nivel 3. Documento firmado mediante firma electrónica avanzada. Permite: identificación robusta; integridad criptográfica; no repudio.

Nivel 4. Documento probatoriamente robusto. Integra: firma electrónica avanzada; sello digital de tiempo; constancia de conservación NOM-151; evidencia de autenticación; registros auditables; todo con la intervención de un Prestador de Servicios de Certificación.

Este último nivel representa el estándar óptimo de protección jurídica en el entorno digital.

XVII. La tesis 2031573 y el nacimiento de un nuevo paradigma probatorio para los actos jurídicos digitales

La tesis aislada identificada con el registro digital 2031573[26] representa uno de los criterios judiciales más importantes emitidos recientemente en materia de prueba electrónica.

Una lectura superficial de la tesis podría llevar a pensar que únicamente resuelve una cuestión procesal relativa al desechamiento de una demanda.

Formalmente, la resolución sostiene que una persona juzgadora no puede determinar mediante una simple revisión visual si un documento electrónico cumple con los requisitos técnicos establecidos por la NOM-151.

Sin embargo, un análisis sistemático permite advertir que el Tribunal reconoce implícitamente diversos principios que redefinen la forma de entender la prueba de los actos jurídicos digitales.

A continuación, se reproduce la tesis:

”Tesis Registro digital: 2031573

Instancia: Tribunales Colegiados de Circuito Tesis: I.11o.C.99 C (11a.) Duodécima Época

26 Tesis I.11o.C.99 C (11a.), Décimo Primer Tribunal Colegiado en Materia Civil del Primer Circuito, amparo directo 698/2024, Uvi Tech, S.A.P.I. de C.V., registro digital 2031573.

Fuente: Semanario Judicial de la Federación. Publicación: viernes 12 de diciembre de 2025 10:24 h

Materia(s): Civil Tipo: Aislada

DOCUMENTOS DIGITALES ACOMPAÑADOS A LA DEMANDA EN EL JUICIO ORAL MERCANTIL. EN EL AUTO INICIAL LA PERSONA JUZGADORA NO PUEDE, MEDIANTE UNA SIMPLE LECTURA VISUAL, VERIFICAR SI CUMPLEN CON LOS REQUISITOS ESTABLECIDOS EN LA NORMA OFICIAL MEXICANA NOM-151-SCFI-2016.

Hechos: Una persona moral demandó en un juicio oral mercantil el vencimiento anticipado de un contrato de compraventa a plazos con interés con reserva de dominio y, derivado de ello, el pago de diversas prestaciones. La persona juzgadora le requirió que exhibiera los documentos que describía en los hechos y en el capítulo de pruebas, así como la copia certificada del instrumento con el que acreditaba su personalidad. Desahogada esa prevención nuevamente la previno para que exhibiera la constancia de conservación del contrato y el pagaré, pues dada la forma electrónica en que se signaron esos documentos no tuvo por satisfecho ese requisito con el registro de consentimiento que exhibió la actora, al no reunir los requisitos previstos en la Norma Oficial Mexicana NOM-151 SCFI-2016. En cumplimiento la actora exhibió el dispositivo USB que contenía el documento requerido. La persona juzgadora estimó que la documentación digital no satisfacía los requisitos de la referida Norma Oficial y, por ende, desechó la demanda. Contra esa resolución se interpuso amparo directo.

Criterio jurídico: Este Tribunal Colegiado de Circuito determina que en el auto inicial la persona juzgadora no puede verificar mediante una simple lectura visual si los documentos digitales acompañados a la demanda en el juicio oral mercantil cumplen con los requisitos establecidos en la Norma Oficial Mexicana NOM-151-SCFI-2016.

Justificación: La referida Norma Oficial Mexicana establece los requisitos necesarios para la conservación de mensajes de datos al momento de firmar documentos electrónicos y los esenciales al digitalizar documentos que originalmente se encuentran en formato físico. Asimismo, define a la constancia de conservación de mensajes de datos como una serie de sellos digitales emitidos por un prestador de servicios de certificación, que permiten verificar la fecha y hora de firma del documento electrónico y acreditar ante cualquier tercero o autoridad la integridad del documento desde el momento en que se generaron dichos sellos, es decir, comprueba que el documento no ha sido modificado después de haber sido firmado por las partes. Para tal efecto, el prestador de servicios de certificación formará una constancia siguiendo el formato ASN.1 del RFC 3161 que se conformará de uno o más sellos digitales de tiempo. Cada sello debe constar con una versión de sello digital de tiempo, un identificador de objeto, y

su contenido debe corresponder a la versión del documento de las políticas de emisión de sellos digitales de tiempo. Las huellas digitales electrónicas se obtendrán con la solicitud. Así, los mensajes de datos pueden conservarse y almacenarse a través de los propios prestadores de servicios de certificación que ofrecen el servicio de almacenamiento de mensajes de datos, quienes cuentan con medios tecnológicos suficientes para garantizar que la información bajo su control podrá ser ulteriormente consultada en cualquier tiempo y expedir constancia de conservación de mensajes que permiten acreditar ante cualquier tercero o autoridad, la integridad desde el momento en que se generaron, con lo cual se cumple la obligación establecida en el artículo 49 del Código de Comercio. De todo lo anterior se advierten como principios aplicables a los mensajes de datos, que les dan certeza y valor probatorio ante terceros, los siguientes: 1) la información en ellos contenida siempre habrá de estar disponible; 2) el mensaje de datos ha de mantenerse íntegro en el tiempo, es decir, sin posibilidad de modificación; y 3) cuando se requiera firma, ésta ha de realizarse a través de la firma electrónica avanzada. En ese sentido, la determinación sobre si un contrato digital cumple o no con los requisitos técnicos establecidos por la NOM-151-SCFI-2016 es un aspecto de naturaleza especializada y técnica que, en su caso, corresponde controvertir a la parte demandada mediante el ofrecimiento y desahogo de una prueba pericial técnica, pues no es posible establecerlo mediante una simple lectura visual de un documento, por lo que implica la participación de personal especializado de diversas dependencias de la administración pública federal y organismos competentes. Por tanto, no puede sostenerse válidamente que la persona juzgadora al analizar el desahogo de la prevención realizada a la actora al presentar la demanda determine que los documentos digitales no cumplen con la mencionada Norma Oficial únicamente con base en una revisión superficial o documental, porque dicha autoridad no tiene la experticia en materia informática.

DÉCIMO PRIMER TRIBUNAL COLEGIADO EN MATERIA CIVIL DEL PRIMER CIRCUITO.

Amparo directo 698/2024. Uvi Tech, S.A.P.I. de C.V. 15 de julio de 2025. Unanimidad de votos. Ponente: Fernando Rangel Ramírez. Secretario: Hernán Arturo Pizarro Balmori.

Esta tesis se publicó el viernes 12 de diciembre de 2025 a las 10:24 horas en el Semanario Judicial de la Federación"

A juicio de este autor, la importancia de la tesis no radica únicamente en afirmar que el juzgador carece de conocimientos técnicos para verificar visualmente una constancia de conservación.

Su verdadero aporte consiste en reconocer la existencia de una infraestructura tecnológica de confianza cuya finalidad es preservar la eficacia probatoria de

los actos jurídicos electrónicos durante todo su ciclo de vida.

El Tribunal reconoce que la prueba del acto jurídico digital es dinámica. En los documentos físicos la prueba suele concentrarse en el propio documento. En cambio, los documentos digitales distribuyen su fuerza probatoria entre múltiples componentes tecnológicos. No basta el contrato, también deben considerarse: i) la firma electrónica; ii) el certificado digital; iii) los sellos digitales de tiempo; iv) la constancia de conservación de mensaje de datos; v) los registros del PSC; vi) los metadatos; vii) las bitácoras de autenticación. Todos estos elementos integran una infraestructura probatoria.

La tesis reconoce esta realidad implícitamente al señalar que la verificación exige conocimientos especializados. El verdadero problema no es verificar el documento, es verificar la evidencia: en realidad, el juez no verifica el PDF, sino que lo que debe verificarse es la evidencia asociada al PDF; la prueba ya no reside únicamente en el documento sino además en la infraestructura criptográfica que lo debe acompañar.

Y aquí se introduce un problema más, el «*delay*» entre la firma del documento y la incorporación de los sellos de tiempo y la constancia de conservación de mensajes de datos.

La mayoría de las plataformas, ayudan a firmar electrónicamente; muy pocas preservan la evidencia criptográfica.

El instante de la firma constituye el momento de mayor valor probatorio de un acto jurídico digital; es precisamente en ese momento cuando deben incorporarse todos los mecanismos destinados a preservar la evidencia electrónica antes de que el transcurso del tiempo deteriore su capacidad probatoria, y es aquí cuando el papel del PSC adquiere la mayor relevancia.

XVIII. El papel del prestador de servicios de certificación en la preservación de evidencia

El Prestador de Servicios de Certificación inmoviliza criptográficamente la evidencia. ¿Cómo lo hace?

Tratándose de los Sellos Digitales de Tiempo: 1) Se genera el hash de la firma electrónica del firmante; 2) Firma el hash con el certificado digital que le otorga la Secretaría de Economía; 3) Obtiene del Centro Nacional de Metrología la hora exacta del firmado; 4) Conserva los elementos anteriores para una futura verificación.

Tratándose de Constancias de Conservación de Mensajes de Datos: 1) Se genera el hash del documento firmado; 2) Firma el hash con el certificado digital que el otorga la Secretaría de Economía; 3) Conserva los elementos anteriores para una futura verificación.

Desde una perspectiva probatoria la intervención del Prestador de Servicios de Certificación debe producirse de manera simultánea con la firma del documento, porque si el sellado ocurre horas o días después... ya apareció el «*delay*», ya existe una ventana temporal y esa ventana puede ser utilizada para cuestionar la integridad del documento. La sincronización entre la plataforma de firma electrónica y el PSC constituye uno de los elementos más importantes de la cadena de confianza digital.

La verdadera utilidad de los Prestadores de Servicios de Certificación aparece cuando transcurre el tiempo. El día de la firma, la intervención del PSC puede parecer invisible para los usuarios. Sin embargo, años después se convierte en un elemento crítico. Cuando una plataforma de firma electrónica opera vinculada con un PSC, pueden realizarse simultáneamente diversos procesos: i) generación del hash documental; ii) validación de identidad; iii) sellado digital de tiempo; iv) emisión de constancias de conservación; v) almacenamiento de evidencia criptográfica; vi) generación de registros auditables.

La consecuencia jurídica es extraordinariamente relevante. El PSC conserva la posibilidad de cotejar la evidencia futura contra la evidencia original. Por ello puede afirmarse que el PSC no conserva únicamente documentos. Conserva la capacidad de demostrar la integridad de los documentos. Esta diferencia constituye uno de los pilares conceptuales de la cadena de confianza digital.

XIX. El expediente probatorio autocontenido

La evolución natural de los sistemas de contratación electrónica parece dirigirse hacia la creación de documentos capaces de transportar su propia evidencia. En el futuro, los actos jurídicos digitales tenderán a incorporar expedientes probatorios autocontenidos mediante archivos XML embebidos que concentrarán la totalidad de la evidencia criptográfica necesaria para su validación.

Bajo este modelo, el documento firmado incorporaría un expediente técnico autocontenido mediante un archivo XML embebido o asociado.[27]

En el contexto de los actos jurídicos digitales, un XML embebido consiste en un archivo XML incorporado dentro del propio documento electrónico o vinculado inseparablemente a éste, cuya finalidad es contener los metadatos y eviden-

27 XML corresponde a las siglas de eXtensible Markup Language (Lenguaje Extensible de Marcado), un estándar desarrollado por el World Wide Web Consortium (W3C) para estructurar, organizar e intercambiar información entre distintos sistemas informáticos mediante etiquetas descriptivas. A diferencia de un documento PDF, cuyo objetivo principal es representar visualmente un documento, un archivo XML está diseñado para almacenar datos estructurados que pueden ser interpretados automáticamente por aplicaciones informáticas.



DIAGRAMA 2. El expediente probatorio autocontenido.

cias técnicas asociadas al acto jurídico. Dependiendo de la plataforma utilizada, dicho XML puede almacenar, entre otros elementos, la huella criptográfica (hash) del documento, los certificados digitales del firmante y de la autoridad certificadora, los sellos digitales de tiempo, las constancias de conservación de mensajes de datos, los identificadores únicos de la transacción, las evidencias de autenticación (OTP, biometría, direcciones IP, identificadores del dispositivo, geolocalización cuando exista), así como las bitácoras de auditoría generadas durante el proceso de firma.

Desde una perspectiva jurídica, el XML embebido puede entenderse como un expediente probatorio electrónico autocontenido, ya que concentra en un solo conjunto estructurado de datos la evidencia técnica necesaria para verificar la autenticidad, integridad, temporalidad y trazabilidad del acto jurídico, facilitando su validación futura por las partes, por los Prestadores de Servicios de Certificación, por peritos especializados o por las autoridades jurisdiccionales.

La principal ventaja de este esquema consiste en que gran parte de la verificación podría realizarse automáticamente. El documento no sería únicamente un instrumento jurídico. Sería simultáneamente un contenedor de evidencia verificable.

Reducción de la dependencia pericial

La tesis 2031573 parte de la premisa de que la verificación de determinados elementos técnicos requiere conocimientos especializados. Sin embargo, la evolución tecnológica podría permitir que una parte importante de esa verificación se realizara de manera automatizada mediante validadores conectados con los PSC correspondientes. En consecuencia, la prueba pericial quedaría reservada para aquellos casos en que exista una controversia real respecto de la autenticidad de la evidencia.

Ello reduciría significativamente los costos y complejidades asociados al litigio electrónico.

XX. Hacia una teoría de la cadena de confianza digital

La evolución de las formalidades jurídicas demuestra que la confianza siempre



DIAGRAMA 3. La cadena de confianza digital.

ha constituido el verdadero objetivo de la forma. En el mundo físico, esa confianza descansaba en: i) el papel; ii) la firma autógrafa; iii) la presencia física; iv) los registros públicos; v) los terceros de confianza.

En el entorno digital, esas funciones son desempeñadas por mecanismos diferentes. Por ello puede afirmarse que la verdadera formalidad funcional del acto jurídico digital descansa sobre una cadena integrada por cinco elementos inseparables:

Identidad. ¿Quién intervino?

Firma. ¿Qué aceptó?

Temporalidad. ¿Cuándo existía el documento?

Conservación. ¿Cómo se preservó su integridad?

Verificabilidad. ¿Cómo puede demostrarse todo lo anterior en el futuro?

La ausencia de cualquiera de estos elementos debilita significativamente la eficacia probatoria del acto jurídico digital.

A partir de las consideraciones anteriores, este trabajo propone formalmente la siguiente tesis doctrinal:

La formalidad jurídica en el entorno digital no se satisface exclusivamente mediante la existencia de un documento firmado electrónicamente. La verdadera formalidad funcional del acto jurídico digital descansa en una cadena de confianza integrada por identidad digital, firma electrónica, sellado de tiempo, conservación verificable de mensajes de datos y capacidad de verificación futura de la evidencia.

Esta cadena de confianza cumple en el entorno electrónico las mismas funciones que históricamente desempeñaron: i) el documento físico; ii) la firma autógrafa; iii) los mecanismos de fecha cierta; iv) los registros documentales; v) y diversos terceros de confianza.

Desde esta perspectiva, la evolución tecnológica no ha modificado los objetivos esenciales del derecho. Lo que ha cambiado son las herramientas utilizadas para alcanzarlos.

Por ello la cadena de confianza digital constituye la evolución contemporánea de las formalidades jurídicas tradicionales y representa, en última instancia, la infraestructura que permite trasladar la seguridad jurídica del mundo físico al entorno electrónico.

XXI. Conclusiones

La transformación digital no ha eliminado las formalidades jurídicas. Lo que ha hecho es sustituir los mecanismos mediante los cuales tradicionalmente se cumplían las funciones de identificación, conservación, autenticación y prueba.

Durante siglos, el documento físico y la firma autógrafa constituyeron los instrumentos predominantes para dotar de seguridad jurídica a las relaciones privadas. Sin embargo, la progresiva sustitución del papel por mensajes de datos ha obligado a replantear conceptos jurídicos que parecían inmutables.

A partir del análisis desarrollado en este trabajo pueden formularse las siguientes conclusiones:

Primera. La forma jurídica no debe confundirse con el soporte documental. La ley nunca protegió el papel como objeto material. Lo que históricamente ha protegido es la posibilidad de exteriorizar, conservar y acreditar una declaración de voluntad jurídicamente relevante.

Por ello, la sustitución del documento físico por mensajes de datos resulta plenamente compatible con la función histórica de la forma escrita.

Segunda. La firma electrónica constituye un mecanismo de atribución jurídica y no un simple recurso tecnológico. Su función esencial continúa siendo la misma que desempeñó históricamente la firma autógrafa: identificar al autor de la declaración, manifestar su voluntad y vincularlo jurídicamente con el contenido del documento.

Tercera. El principal desafío de la contratación electrónica no consiste en la validez de la firma. El verdadero problema jurídico consiste en la construcción de identidad digital verificable. La experiencia demuestra que la mayoría de las controversias relacionadas con documentos electrónicos no giran en torno a la existencia formal de una firma, sino a la posibilidad de acreditar que determinada persona intervino efectivamente en la operación.

Cuarta. La firma electrónica avanzada representa actualmente el mecanismo más robusto de atribución de identidad disponible en el derecho privado contemporáneo. Su fortaleza deriva de la utilización de infraestructura criptográfica basada en certificados digitales, claves asimétricas y funciones hash matemáticamente verificables.

Quinta. Los Prestadores de Servicios de Certificación desempeñan una función esencial dentro de la construcción de confianza digital. Su importancia no radica únicamente en la emisión de certificados o en la prestación de servicios tecnológicos. Su verdadero valor consiste en conservar la capacidad de verificar la integridad y autenticidad de la evidencia electrónica a través del tiempo. Por ello puede afirmarse que los PSC no conservan únicamente documen-

tos. Conservan la capacidad de demostrar que dichos documentos permanecen íntegros.

Sexta. Los sellos digitales de tiempo constituyen el equivalente funcional más cercano a la fecha cierta en el entorno digital. Su función consiste en demostrar que una determinada evidencia documental existía en una fecha y hora específicas. La temporalidad verificable constituye uno de los elementos fundamentales de toda infraestructura moderna de confianza digital.

Séptima. La NOM-151-SCFI-2016 no debe entenderse como un requisito de validez de los actos jurídicos electrónicos. Su verdadera función consiste en fortalecer la eficacia probatoria de los mensajes de datos mediante mecanismos destinados a preservar su integridad, disponibilidad y verificabilidad. En consecuencia, la NOM-151 resuelve fundamentalmente un problema de prueba y no un problema de validez.

Octava. La tesis con registro digital 2031573 representa uno de los criterios judiciales más relevantes emitidos recientemente en materia de prueba electrónica. El Tribunal reconoce que la prueba del acto jurídico digital es dinámica. En los documentos físicos la prueba suele concentrarse en el propio documento. En cambio, los documentos digitales distribuyen su fuerza probatoria entre múltiples componentes tecnológicos. No basta el contrato, también deben considerarse: i) la firma electrónica; ii) el certificado digital; iii) los sellos digitales de tiempo; iv) la constancia de conservación de mensaje de datos; v) los registros del PSC; vi) los metadatos; vii) las bitácoras de autenticación. Todos estos elementos integran una infraestructura probatoria.

Novena. La principal dificultad de los actos jurídicos digitales no aparece al momento de la firma. Aparece años después. La separación temporal entre la celebración del acto y su eventual presentación en juicio genera lo que este trabajo ha denominado *delay* probatorio. La necesidad de preservar evidencia verificable durante largos periodos de tiempo constituye uno de los desafíos centrales del derecho digital contemporáneo.

Décima. La evolución tecnológica permite vislumbrar la posibilidad de crear documentos electrónicos acompañados de expedientes probatorios autocontenidos integrados mediante XML embebidos o mecanismos equivalentes. Estos expedientes podrían contener la totalidad de los elementos necesarios para verificar identidad, integridad, temporalidad y conservación, reduciendo significativamente la necesidad de pruebas periciales complejas.

Décima Primera. La cadena de confianza digital como nueva formalidad funcional del acto jurídico electrónico. La formalidad jurídica en el entorno digital no se satisface exclusivamente mediante la existencia de un documento firmado electrónicamente. La verdadera formalidad funcional del acto jurídico digital descansa en una cadena de confianza integrada por identidad digital, firma

electrónica, sellado de tiempo, conservación verificable de mensajes de datos y capacidad de verificación futura de la evidencia.

Bibliografía

ADAMS y LLOYD. *Understanding* PKI.

BROWN, Ian. *Electronic Signatures and Electronic Evidence*.

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI). *Ley Modelo sobre Comercio Electrónico*. Nueva York: Naciones Unidas, 1996.

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI). *Ley Modelo sobre Firmas Electrónicas*. Nueva York: Naciones Unidas, 2001.

DE LA MADRID ANDRADE, Mario. *Derecho del comercio electrónico*. México: Oxford University Press.

DOMÍNGUEZ MARTÍNEZ, Jorge Alfredo. *Derecho civil: parte general*. México: Porrúa.

MASON, Stephen. *Electronic Evidence*. Institute of Advanced Legal Studies.

México. Código Civil Federal.

México. Código de Comercio.

México. Ley de Firma Electrónica Avanzada.

Norma Oficial Mexicana NOM-151-SCFI-2016, Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos.

ROJINA VILLEGAS, Rafael. *Derecho civil mexicano: teoría general de las obligaciones*. México: Porrúa.

STALLINGS, William. *Cryptography and Network Security*.

Suprema Corte de Justicia de la Nación. Tesis I.11o.C.99 C (11a.). *Semanario Judicial de la Federación*. Registro digital 2031573.

* * *