BREVE APROXIMACIÓN A LA PROBLEMÁTICA JURÍDICA DEL COMERCIO Y LA CONTRATACIÓN ELECTRÓNICOS Y LA FIRMA ELECTRÓNICA EN PARTICULAR

Isabel DAVARA F. DE MARCOS*

SUMARIO: I. *Planteamiento*. II. *El comercio y la contratación electrónicos*. III. *La firma electrónica*. IV. *Sucintas conclusiones*.

I. PLANTEAMIENTO

Ante la pregunta de la necesidad de la regulación, o, al menos, su primigenia utilidad, especialmente en países de nuestro entorno y tradición jurídicos, parece que la respuesta intuitiva es, además de consideraciones jurídico sociológicas, la búsqueda de seguridad jurídica.

Hablar de seguridad jurídica, en términos generales, es hablar de certeza ante las consecuencias legales de una determinada relación o acto jurídico.[1] La seguridad jurídica, especialmente en países de nuestro entorno sociojurídico, está basada en leyes, en un concepto amplio, que aseguran una específica reacción a una acción concreta.

Comenzamos así esta breve disertación porque no podemos aproximarnos sucintamente al entorno jurídico del comercio, la contratación y

* Doctora en derecho y ciencias económicas empresariales por la Universidad Pontificia Comillas de Madrid (ICAI-ICADE); presidenta del Comité Electrónico para América Latina de la American Bar Association.

1 Profundizando en el estudio del concepto señala Palma Fernández: "La seguridad jurídica en cuanto a las normas se manifiesta en la exigencia de conocer cuáles han de ser las consecuencias jurídicas de una determinada actuación", señalando el autor como características de la seguridad jurídica las siguientes*:* certeza de la norma vigente, claridad del texto de la norma, capacidad reguladora autosuficiente en su ámbito, ausencia de motivaciones pedagógicas y consecuencia de un depurado proceso de elaboración. Véase Palma Fernández, J. L. "La seguridad jurídica ante la abundancia de normas", *Cuadernos y Debates*, Madrid, núm. 68, 1997.

la firma electrónicos en México si no partimos de que esta regulación trae causa de la supuesta incertidumbre ante las consecuencias jurídicas derivadas de la utilización de estos medios.

Por otro lado, pretender analizar la seguridad jurídica en las transacciones electrónicas en casi como hablar de la seguridad jurídica en el comercio tradicional, es decir, inabarcable. Sin embargo, el espíritu de nuestro trabajo era enfrentar el mayor obstáculo que el desarrollo del comercio electrónico, en toda la extensión del concepto, tiene, esto es, la falta de confianza. Y la desconfianza surge inevitablemente de la incertidumbre,[2] de la falta de certeza ante las consecuencias de una determinada acción.[3]

En este sentido, estos recelos y dudas tienen gran parte de fundamento en la supuesta falta de certeza jurídica, en el desconocimiento de las consecuencias jurídicas de una determinada relación jurídica, de cualquier índole. Y, *sensu contrario,* la grandeza y fortaleza de la seguridad y certeza jurídicas hace evadirse, si no completamente sí en gran medida, las incertidumbres generales, funcionando como uno de los mejores antídotos o remedios a dicha inseguridad y falta de confianza.

[2] Tal y como se señala en el Dictamen de las Comisiones Unidas de Justicia y de comercio, con proyecto de decreto por el que se dictaminan diversas reformas y adiciones al Código Civil federal, al Código de Comercio y a la Ley Federal de Protección al Consumidor en materia de comercio electrónico: "En términos generales la legislación actual no reconoce el uso de los medios electrónicos de manera universal, y en caso de un litigio el juez o tribunal tendrán que allegarse de medios de prueba indirectos para determinar que una operación realizada por medios electrónicos es o no válida. Esta situación ha originado que empresas frenen sus inversiones orientadas a realizar transacciones por medios electrónicos, debido a la *incertidumbre legal en caso de controversias*". *Gaceta Parlamentaria*, año III, núm. 500, miércoles 26 de abril de 2000, véase *www.sice.oas.org/e-comm/legislation/mex.asp*, consulta: 18 de agosto de 2007.

[3] En cuanto a las implicaciones que el término seguridad jurídica tiene, Pérez Luño señala: "Partimos a la conquista de una seguridad radical que necesitamos porque, precisamente, lo que por lo pronto somos aquello que nos es dado al sernos dada la vida, es radical inseguridad... El anhelo de seguridad constituye una constante histórica que adquiere especial relieve en el mundo moderno... En la segunda, que representa su faceta subjetiva, se presenta como certeza del derecho, es decir, como proyección en las situaciones personales de la seguridad objetiva. Para ello, se requiere la posibilidad del conocimiento del derecho por sus destinatarios... El sujeto de un ordenamiento jurídico debe poder saber con claridad y de antemano aquello que le está mandado, permitido o prohibido... La certeza representa la otra cara de la seguridad objetiva: su reflejo en la conducta de los sujetos del derecho". Véase Pérez Luño, A. E., *La seguridad jurídica*, Barcelona, Ariel, 1991.

Hemos seleccionado estos temas dentro del amplio espectro de materias afectadas por las tecnologías de la información y las comunicaciones, porque, volviendo a nuestro punto de partida, entendemos que sería de todo punto imposible profundizar en todos los ámbitos jurídicos afectados por las mismas, puesto que, en nuestra opinión, éstas afectan a todos los ámbitos jurídicos imaginables, de modo que se está construyendo, permitiéndonos una licencia jurídica, un "ordenamiento jurídico paralelo", y cualquier disciplina jurídica de las denominadas tradicionales se ve afectada por estos medios.[4]

Consecuencia de lo expuesto, parece imposible, y probablemente poco eficiente, pretender analizar en profundidad todas las áreas expuestas, como igualmente lo sería hacerlo en el entorno tradicional.

Partiendo de la mencionada hipótesis, nuestro trabajo se divide en dos áreas fundamentales en las que hemos entendido conveniente centrar nuestra atención. Así, hablaremos en primer lugar del comercio y la contratación electrónicos y después pasaremos al estudio de la firma electrónica como garante de la seguridad y confianza en el perfeccionamiento de las relaciones electrónicas basadas en documentos electrónicos.

[4] Así, podríamos ir recorriendo cada una de las ramas del derecho e ir viendo su homónima electrónica: el derecho laboral con el derecho laboral electrónico y el tan nombrado teletrabajo, el derecho mercantil con el derecho mercantil electrónico partiendo de las sociedades con única existencia electrónica, el derecho administrativo con el derecho administrativo electrónico y la administración electrónica, el derecho procesal con la administración de justicia electrónica, el derecho civil con la contratación electrónica, etcétera. Además de las innumerables materias que de por sí no constituyen una rama independiente, pero cuya relevancia no se cuestiona, como la publicidad, la propiedad intelectual, el derecho de la competencia, etc. A este respecto, Davara Rodríguez señala: "No se trata, nos dice el profesor Hernández Gil, de que el derecho va a ordenar nuevas realidades, sino que el derecho mismo va a experimentar, en cuanto objeto de conocimiento, una mutación, derivada de un modo distinto de ser elaborado, tratado y conocido". Véase Davara Rodríguez, M. A., "La sociedad de la información y el tratamiento de datos de carácter personal (1997-1998)", *Quince años de encuentros sobre informática y derecho*, en Davara Rodríguez, Miguel Ángel (coord.), Madrid, Universidad Pontificia Comillas, 2002, pp. 20 y ss. Y, además, todo lo anterior sin olvidarnos de un aspecto fundamental: la ética. Así lo señala Davara Rodríguez, en concreta relación a su influencia en el ámbito laboral, pero absolutamente extendible analógicamente a los demás entornos, véase *ibidem* pp. 331 y ss. Véase también, del mismo autor, "Ética de los empresarios y directivos. Reflexiones pseudojurídicas en torno a la utilización de las tecnologías de la información y comunicaciones (TIC)", *Economía ética y bienestar social*, Madrid, Pirámide, 2003, pp. 175 y ss.

No obstante, y a pesar de que, por las razones previamente expuestas hemos tenido que limitar nuestro estudio a estas dos materias, no queremos dejar siquiera de mencionar aquí otras tantas involucradas, como la especialmente relevante protección de datos de carácter personal (considerado como derecho fundamental de tercera generación independiente y autónomo),[5] la propiedad intelectual e industrial, el teletrabajo, la administración electrónica, o los delitos informáticos. Cada uno de ellos *per se* daría lugar a otro extenso trabajo de investigación, y, como nuestro ámbito no lo permite, sirva este planteamiento únicamente como constancia de su relevante existencia, sin pretender abarcar más que un mero apunte recordatorio. Nuestro estudio finaliza con unas concisas reflexiones a modo de conclusión.

II. El comercio y la contratación electrónicos

Podríamos decir que es comercio toda aquella actividad que tenga por objeto realizar una operación comercial, y que es electrónico cuando ese comercio se lleva a cabo utilizando la herramienta electrónica de forma que tenga o pueda tener alguna influencia en la consecución del fin comercial, o en el resultado de la actividad que se está desarrollando.

[5] Como decíamos, materia especialmente relevante y atractiva, máxime teniendo en cuenta que este trabajo, se encuadra dentro de una obra homenaje al constitucionalista Héctor Fix-Zamudio. La mayoría de los textos constitucionales internacionales están reconociendo este derecho fundamental de tercera generación que faculta al titular de los datos para decidir quién, cómo, dónde, cúando y para qué se trata la información personal que le concierne (partiendo del reconocido principio a la autodeterminación informativa). El legislador mexicano se encuentra rezagado. Existen numerosas iniciativas en ambas Cámaras inexplicablemente paralizadas. No obstante, el 20 de julio de 2007 se publicó en el *Diario Oficial de la Federación*, en sus páginas 2 y 3, el Decreto por el que se adiciona un segundo párrafo con siete fracciones al artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, donde se hace una referencia explícita a la protección de datos personales, si bien dentro del artículo destinado al derecho de acceso a la información. Aunque resulta de alabar que dicha referencia se haga en un texto constitucional, no debe hacerse exclusivamente, al menos sin realizar una interpretación profunda y casi diríamos extensiva, como un límite al derecho de acceso a la información, puesto que se trata de dos derechos fundamentales independientes entre sí, más complementarios que excluyentes, en su caso. En cuanto al contenido de la reforma, y reiterando que no se trata de una reforma de protección de datos en sí (que entendemos y esperamos que venga en camino en el artículo 16 de la Constitución respecto del que conocemos, y participamos, en dicha reforma), todavía adolece de algunas lagunas, reiterando, de nuevo, nuestra complacencia acerca de la referencia constitucional.

Es decir, el medio electrónico es tan sólo eso, el medio,[6] la forma de concreción, aunque tiene una relevancia esencial. En este sentido, intentando enumerar qué actividades podríamos encontrar dentro de la idea del comercio electrónico, podemos mencionar tanto la compra de productos o servicios por Internet, la transferencia electrónica de datos entre operadores de un sector en un mercado, el intercambio de cantidades o activos entre entidades financieras, la consulta de información (con fines comerciales) a un determinado servicio, o un sinfín de actividades de similares características realizadas por medios electrónicos (nótese que no se circunscribe a Internet);[7] pero, para no perdernos en ambigüedades, entenderemos, como apuntábamos, en un sentido amplio[8] que comercio es toda aquella actividad que tenga por objeto o fin realizar una operación comercial y que es electrónico cuando ese comercio se lleva a cabo utilizando la herramienta electrónica de forma que tenga o pueda tener alguna influencia en la consecución del fin comercial, o en el resultado de la actividad que se está desarrollando.[9]

La contratación electrónica, por su parte, en gran medida se encuadra dentro del comercio electrónico,[10] pero su relevancia es tal que merece al

6 No obstante, no podemos desconocer la dimensión cuantitativa del fenómeno, que, además, da lugar a toda esta regulación e innovación. El comercio electrónico constituye, cuando menos, un nuevo sector de la economía.

7 Davara & Davara, *Factbook sobre comercio electrónico*, 3a. ed., Pamplona, Aranzadi Thomson, 2004, pp. 74 y ss.

8 Véase, entre otras, la Guía para la Incorporación de la Ley Modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional en su párrafo 7.

9 Como decimos, es un tema amplísimo y las clasificaciones también múltiples. Por ejemplo, podemos dar varias clasificaciones de comercio electrónico, según el criterio de clasificación escogido. Así, podemos hablar, desde el punto de vista del canal o canales utilizados, en un comercio electrónico directo u *on line* (en el que todas las fases del comercio se realizan electrónicamente, sin tener que recurrir a ningún medio o mecanismo tradicional) y en comercio electrónico indirecto u *off line* (en el que alguna de las fases del perfeccionamiento de la relación se realizan por medios no electrónicos, típicamente la entrega de los bienes y servicios). Por otro lado, desde el punto de vista de los sujetos intervinientes, podemos hablar de tres tipos de ellos: administraciones, empresas y consumidores, pudiendo a su vez subdividirse todos estos sujetos en muchos más según infinidad de particularidades. Véase Davara & Davara, *Factbook sobre comercio electrónico*, *cit.*, nota 7, pp. 75 y ss.; y Davara & Davara, *Guía práctica de comercio electrónico para las PYME*, Madrid, Dafema, 2003, pp. 45 y ss.

10 Si bien no todos los contratos son actos de comercio, lo cierto es que la gran parte de los mismos lo son en el entorno electrónico, en especial en Internet, salvo, probable-

menos una referencia individual, y de ahí el epígrafe bajo el que denominanos esta parte del trabajo.

Respecto a ella, se predica igualmente lo anterior, máxime en un ordenamiento de marcado carácter espiritualista como el nuestro,[11] donde la forma o el medio por el que se llega a un convenio no es lo esencial, pues, según el artículo 1794 del Código Civil,[12] los elementos para la existencia de toda contratación sólo son el consentimiento[13] y el objeto,[14] aunque la doctrina señala, asimismo, como especialmente relevante en cuanto a la validez el fin del mismo.[15]

Una vez situados los términos por utilizar, y adentrándonos en la cuestión normativa, tenemos que decir que en México no existe una ley espe-

mente, algunos de los realizados "entre pares", o *peer to peer,* es decir, entre iguales, en los que ni el objeto ni el sujeto haga posible catalogarlos como actos comerciales. Por otro lado, la mayoría de las legislaciones eximen de su ámbito competencial la regulación de gran parte de los contratos civiles. Véase artículo 9.2 D, de la Directiva Europea de Comercio Electrónico y título IV de la LCE española, por ejemplo, respecto de aquellos contratos que se refieran al derecho de familia y sucesiones; los que la ley acuerde para su validez o para la producción de determinados efectos la forma documental pública o los que requieran la intervención de órganos jurisdiccionales, notarios, registradores de la propiedad y mercantiles o autoridades públicas.

11 Así, dice el Código Civil en su artículo 1832: "En los contratos civiles cada uno se obliga en la manera y términos que aparezca que quiso obligarse, sin que para la validez del contrato se requieran formalidades determinadas, fuera de los casos expresamente designados por la ley", que, además, se aplica supletoriamente en el ámbito commercial en virtud de lo dispuesto en el artículo 2o. del Código de Comercio.

12 Artículo 1794 del Código Civil: "Para la existencia del contrato se requiere: I. Consentimiento; II. Objeto que pueda ser materia del contrato".

13 Artículo 1796 del Código Civil: "Los contratos se perfeccionan por el mero consentimiento; excepto aquellos que deben revestir una forma establecida por la ley. Desde que se perfeccionan obligan a los contratantes no sólo al cumplimiento de lo expresamente pactado, sino también a las consecuencias que, según su naturaleza, son conforme a la buena fe, al uso o a la ley". Véase Pombo, F., "Contratación electrónica", *Régimen jurídico de Internet*, Madrid, La Ley, 2002, pp. 1163 y ss.

14 Artículo 1825 del Código Civil: "La cosa objeto del contrato debe: 1o. Existir en la naturaleza. 2o. Ser determinada o determinable en cuanto a su especie. 3o. Estar en el comercio". Artículo 1827 del Código Civil: "El hecho positivo o negativo, objeto del contrato, debe ser: I. Posible; II. Lícito". Artículo 1830 Código Civil: "Es ilícito el hecho que es contrario a las leyes de orden público o a las buenas costumbres". Véase Barriuso Ruiz, C., *La contratación electrónica*, Madrid, Dykinson, 1998.

15 Artículo 1831 del Código Civil: "El fin o motivo determinante de la voluntad de los que contratan, tampoco debe ser contrario a las leyes de orden público ni a las buenas costumbres".

cífica reguladora del comercio electrónico, o de la presencia en Internet, al contrario de lo que se da en otras naciones, especialmente en el entorno europeo.[16]

Por el contrario, para introducir estas reglas se optó por añadir disposiciones específicas a las diversas normas ya existentes, pero no se modificaron leyes menores, sino las codificaciones más importantes y generales, lo que, por otro lado, nos da una idea de la importancia y relevancia de las consecuencias jurídicas derivadas del uso de estos medios. Estas reformas tuvieron lugar mediante, principalmente, el Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en materia común y para toda la República en materia federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor, del 23 de mayo de 2000, y el Decreto por el que se realizan posteriores reformas y adiciones al Código de comercio en materia de firma electrónica de agosto de 2003.[17]

Dichas reformas se basaron, en gran parte, en las Leyes Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) sobre comercio electrónico y otros medios conexos de comunicación de datos y sobre firmas electrónicas.[18]

16 Por ejemplo, como norma marco en toda la Unión Europea se aplica la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, del 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior, publicada en el *Diario Oficial* núm. L 178 de 17/07/2000 (en adelante, Directiva sobre el Comercio Electrónico) y, en concreto, en el caso de España, la transposición de esa Directiva se hace mediante la Ley 34/2002, del 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, publicada en el *Boletín Oficial del Estado* núm. 166, del 12 de julio, pp 25 388 y ss. (en adelante, LCE española).

17 Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor (*DOF* del 29 de mayo de 2000); Decreto por el que se reforman y adicional diversas disposiciones del Código de Comercio en Materia de Firma Electrónica (*DOF* del 29 de agosto de 2003).

18 Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) sobre Comercio Electrónico y otros medios conexos de comunicación de datos, que fue aprobada por la Asamblea General de las Naciones Unidas en el vigésimo noveno periodo de sesiones, en su 605a. sesión, celebrada el 12 de junio de 1996, siendo aprobada por la Asamblea General el 16 de diciembre de ese mismo año en

Como apunte general, antes de entrar a analizar someramente dichas reformas, a los distintos cuerpos legislativos, queremos mencionar aquí unos concretos principios generales, especificados con carácter general en el artículo 89 del reformado Código Civil, en su aplicación e interpretación: neutralidad tecnológica,[19] autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del mensaje de datos en relación con la información documentada en medios no electrónicos, y la firma electrónica en relación con la firma autógrafa.[20]

1. *Reformas al Código Civil Federal*

Comienza el reformado artículo 1803 del citado Código Civil Federal señalando que el consentimiento se considerará expreso cuando se manifieste por medios electrónicos, ópticos o por cualquier tecnología.

El estudio del consentimiento en derecho es una cuestión crucial, especialmente en la contratación, pues es uno de los elementos de existencia de la misma como ya hemos visto. Por un lado, en cuanto a la forma en la que se puede otorgar el consentimiento, con carácter general, cabe distinguir entre consentimiento tácito y expreso.[21] En cualquiera de los

su sesión plenaria 85, añadiéndose, en 1998, durante el trigésimo primero período de sesiones de la Comisión, un nuevo artículo 5 bis (en adelante, Ley Modelo sobre Comercio Electrónico). Y Ley Modelo sobre firmas electrónicas de la CNUDMI, así como su guía de incorporación, fue aprobada mediante resolución aprobada por la Asamblea General (sobre la base del informe de la Sexta Comisión), durante la 85a. sesión plenaria celebrada el 12 de diciembre de 2001 (en adelante, Ley Modelo sobre firmas electrónicas).

19 Las normas de "nuevas tecnologías" y en general las técnicas, no suelen imponer la utilización de una tecnología en concreto por claras razones de obsolescencia técnica y de competencia en el mercado. Sin embargo, lo que sí marcan son necesarios objetivos a cumplir con las herramientas que se utilicen, y, en ocasiones, se remiten a publicaciones oficiales que enumeran las tecnologías que en el momento cumplen esos requisitos. Así, cuando el reformado artículo 89 del Código de Comercio se refiere a "cualquier otra tecnología" (al igual que en repetidas ocasiones más) pretende abarcar no sólo las técnicas conocidas en el momento, sino también la posibilidad de adaptación a las futuras técnicas de comunicación.

20 Asimismo, Mateu de Ros también señala la importancia del antiformalismo total en la contratación electrónica. Véase Mateu de Ros, R., "Principios de la nueva Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (2001-2002)", en Davara Rodríguez, Miguel Ángel (coord.), *Quince años de encuentros sobre informática y derecho*, Madrid, Universidad Pontificia Comillas, 2002, pp. 794-795.

21 También la doctrina y jurisprudencia menciona en algún momento un denominado "consentimiento presunto". Por otro lado, el consentimiento expreso puede ser verbal o

casos señalados, la cuestión se centra en la prueba de la obtención del consentimiento, puesto que, tanto en el consentimiento tácito, principalmente, como en el expreso que no sea por escrito, parece que hay que implementar procedimientos estandarizados de recogida de dicho consentimiento para que luego se pueda probar su obtención, recayendo la carga de la prueba en quien solicita el consentimiento.

Por otro lado, de las características que conforman el consentimiento se pueden destacar las siguientes: libre (que haya sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por las leyes, es decir, que no esté viciado);[22] específico, informado e inequívoco (no se puede deducir el consentimiento de los meros actos realizados por el afectado —el llamado *consentimiento presunto*—, sino que es preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento).

Además, en dicho artículo 1803 se señala de forma indirecta la inmediatez de la contratación por medios electrónicos, como Internet, superando las clásicas discusiones doctrinales acerca de si la contratación electrónica debe considerarse entre ausentes[23] o entre presentes.[24] Lo importante en este tipo de contratación es que la oferta y la aceptación pue-

escrito (en este sentido, y, aunque no parece necesario volver a recalcarlo, en un trabajo dedicado al derecho de las tecnologías de la información y las comunicaciones, el concepto de escrito no puede circunscribirse al soporte papel).

22 Artículo 1812 del Código Civil: "El consentimiento no es válido si ha sido dado por error, arrancado por violencia o sorprendido por dolo". Artículo 1795 del Código Civil: "El contrato puede ser invalidado: I. Por incapacidad legal de las partes o de una de ellas. II. Por vicios del consentimiento. III. Porque su objeto, o su motivo o fin sea ilícito. IV. Porque el consentimiento no se haya manifestado en la forma que la ley establece".

23 En este sentido, mucho se discute sobre la definición de contratación entre ausentes referida a la contratación electrónica, y más por Internet, ya que la distancia es física, pero la inmediatez en la contratación se produce en la mayor parte de los casos, igual que en la contratación telefónica, por lo que las categorías y las reglas aplicables a la tradicional contratación a distancia tienen que cambiar aquí, pues la mencionada inmediatez hace que la contratación se parezca en muchas ocasiones a una contratación entre presentes, como una presencia diferente, a pesar de la separación espacial. En definitiva, los procesos de contratación, especialmente los que basan la aceptación en el "click" que da lugar al perfeccionamiento del contrato, son contratos inmediatos, que difieren sustancialmente de los procesos por carta, fax, telégrafo, etcétera, tradicionales.

24 Así lo dice Julià-Barceló, aunque apunta algunos obstáculos a este principio general. Véase Julià-Barceló, R., "Contratos electrónicos B2B: creación de un marco jurídico «a la carta»", *Régimen jurídico de Internet*, *cit*., nota 13, pp. 554-557.

dan realizarse de manera inmediata,[25] y no tanto la distancia física entre las partes, cuestión que era absolutamente relevante anteriormente en las contrataciones tradicionales[26] que carecían de esta inmediatez cuando no se daba esta presencia física de las partes (el correo tradicional, el telégrafo, etcétera). De este modo dice el artículo 1805:

> Artículo 1805. Cuando la oferta se haga a una persona presente, sin fijación de plazo para aceptarla, el autor de la oferta queda desligado si la aceptación no se hace inmediatamente. La misma regla se aplicará a la oferta hecha por teléfono o a través de cualquier otro medio electrónico, óptico o de cualquier otra tecnología que permita la expresión de la oferta y la aceptación de ésta en forma inmediata.

En todo caso, además de la cuestión del momento de perfeccionamiento del contrato, lo que parece subyacer, y en nuestra opinión es aún más importante en este tema, es, como decíamos, la cuestión del consentimiento prestado por medios electrónicos, y más todavía en el caso de las aceptaciones automáticas en las que no interviene voluntad humana alguna, por lo que cabría preguntarse si las máquinas tienen esa voluntad, o si dicha voluntad debe adjudicarse a la aceptación y ra-

25 La doctrina distingue tres momentos fundamentales en la vida de un contrato: su generación, la perfección del mismo, y su consumación. Véase Benavides del Rey, J. L. "Celebración de contratos internacionales por medios electrónicos. Formación de contratos", *La validez de los contratos internacionales negociados por medios electrónicos*, Madrid, CECO, pp. 74 y ss.

26 El concepto de documento es una cuestión absolutamente relevante en derecho, y así lo es igualmente en el entorno electrónico de las transacciones. El documento electrónico está totalmente admitido en nuestro ordenamiento jurídico, y actualmente nadie duda ya de la validez de dichos documentos, a pesar de que su introducción, además de haber requerido esfuerzo, está aún lejos de su implantación general, por la tan consabida y repetida falta de confianza por el usuario (y no sólo en nuestro ordenamiento, como señala, por ejemplo, la guía para la incorporación de la Ley Modelo sobre comercio electrónico de la CNUDMI en sus párrafos 3 y 48, entre otros). Pero esta falta de confianza no influye en nada para su admisibilidad en derecho, es decir, su equiparación jurídica, en los casos en los que no existan requisitos, normalmente formales, que lo impidan, a los documentos tradicionales, es, podríamos decir, casi plena, y más aun en los últimos tiempos, sin importar a estos efectos la preferencia del usuario por los documentos tradicionales. No obstante, no podemos olvidar la supremacía que ha tenido la utilización del papel durante siglos en la constancia por escrito. Véase Davara Rodríguez, M. A. "La contratación por medios informáticos (1990-1991)", en Davara Rodríguez, Miguel Ángel (coord.), *Quince años de encuentros sobre informática y derecho*, *cit.,* nota 4, 2002, pp. 127 y ss.

tificación por dicha persona de las operaciones realizadas de manera automática, y, en consecuencia, de todo el perfeccionamiento electrónico de los contratos.

Por otro lado, un paso esencial en las regulaciones en comercio y contratación electrónicos reside en la automatización en el uso y consecuente validez de estas técnicas.[27] Así, de igual modo que las partes no tienen que acordar sobre la validez del uso del papel en la celebración de acuerdos tradicionales, el Código que analizamos explicita, en su artículo 1811, que las partes no tendrán que acordar la validez de estas técnicas.[28]

27 Véase Perales Viscasillas, M. P., "Formación del contrato electrónico", *Régimen jurídico de Internet, cit.,* nota 13, pp. 880 y ss.

28 La regulación de la técnica tampoco es tan absolutamente desconocida. Dos ejemplos sirvan para ilustrarnos. El primero, en el panorama nacional mexicano y el segundo en el estadounidense (si bien éste en el ámbito jurisprudencial, aunque dado su ordenamiento y tradición jurídica su valor bien puede ser cuasi equiparado en muchas ocasiones). Así, en México, un ejemplo particularmente resaltable es el que señala la Maestra Macarita Elizondo Gasperín, "En México, la informática vinculada a los procesos electorales se remonta al XXVII Congreso de los Estados Unidos Mexicanos, cuando aprobó la Ley para la Elección de Poderes Federales, la cual fue promulgada el día 1o. de julio de 1918, por Venustiano Carranza... Artículo 58. La votación podrá recogerse por medio de máquinas automáticas, siempre que llenen los requisitos siguientes: I. Que pueda colocarse en lugar visible el disco de color que sirva de distintivo al partido y los nombres de los candidatos propuestos. II. Que automáticamente marque el número total de votantes y los votos que cada candidato obtenga. III. Que tenga espacios libres donde los ciudadanos puedan escribir los nombres de los candidatos cuando voten por alguno no registrado. IV. Que pueda conservarse el secreto del voto. V. Que el registro total señalado automáticamente sea visible e igual a las sumas parciales de los votos obtenidos por cada candidato; VI. Que los electores de la sección respectiva conozcan su manejo". Véase Macarita Elizondo Gasperín, "Voto electrónico. Antecedentes y despliegue", *http://www.votobit.org/lallave/macarita.html* (consulta: 15 de agosto de 2007). El segundo de los ejemplos es el conocidísimo artículo de los Jueces del Tribunal Supremo, Samuel D. Warren y Louis D. Brandeis de finales del siglo XIX, donde se explica la evolución del derecho a la privacidad, apoyándose en un tratado muy renombrado sobre injurias de otro juez, llamado Cooley, donde defendía el derecho a "ser dejado en paz", y comienzan así a definir lo que en dichos ordenamientos se entiende la privacidad en la era moderna. No obstante, hay que tener en cuenta, en primer lugar, que se trata de un artículo de 1890, por lo que obviamente las preocupaciones hay que ponerlas en consonancia con las entonces existentes, pero, sobre todo, no deja de llamar la atención, en nuestra opinión, la idea de que se refirieran a "aparatos mecánicos", lo que podría, en una exégesis muy amplia, englobar el posterior desarrollo de la electrónica, y que ya se pudiera pergeñar el daño que la intrusión en la privacidad del individuo podía causar. Véase "The rigth to Privacy", *Harvard Law Review*, vol. IV, 15 de diciembre de 1890, núm. 5, con

Como breve apunte final, no podemos dejar de mencionar que en los países de larga tradición romanista, especialmente en los países de América Latina, la figura notarial[29] tiene una importancia clave, y así lo quiere resaltar el artículo 1834 bis en su segundo párrafo, dando paso a los fedatarios públicos,[30] para que éstos puedan realizar sus funciones mediante la utilización de medios electrónicos.

2. *Reformas al Código Federal de Procedimientos Civiles*

Adentrándonos en el ámbito procesal, también se reformó el Código Federal de Procedimientos Civiles, que en su artículo 210-A afirma varias cuestiones esenciales:

1. Se reconoce como *prueba* la información generada o comunicada que conste en "medios electrónicos, ópticos o en cualquier otra tecnología".
2. La *valoración de la fuerza probatoria* de dicha información se hará con base en los siguientes criterios:
   a. La fiabilidad del método en que haya sido generada, comunicada, recibida o archivada, remitiéndonos al apartado de firma electrónica para profundizar sobre este extremo.
   b. La posibilidad de atribución a las personas obligadas del contenido de la información relativa.
   c. Su accesibilidad para su ulterior consulta.

En este sentido, tenemos que decir que tampoco está exigiendo la norma grandes cosas, ni mucho menos diferentes al entorno físico, tradicional, donde también algunos medios de prueba son más fiables que otros. Sin embargo, el mero hecho de hacerse en el entorno electrónico parece que proviene de la supuesta y temida, aunque básicamente incierta, incertidumbre inherente al mismo.

modificaciones en *http://www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html*, consulta: 2 de julio de 2004.

29 Así también la directiva comunitaria europea de comercio electrónico, ya en su considerando 36, permite a los Estados miembros que establezcan excepciones para la intervención de los fedatarios públicos.

30 A este respecto, véase Oliver Lalana, A. D., "La eficacia jurídica de la firma electrónica, considerada en relación con los documentos electrónicos privados y públicos", en Davara Rodríguez, Miguel Ángel (coord.), *XIII Encuentros sobre informática y derecho*, Madrid, Universidad Pontificia Comillas, 2001, pp. 256 y ss.

3. Concepto de *originalidad del documento:*[31] si la ley requiere que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta. La originalidad del documento es una cuestión muy debatida en el entorno electrónico, donde las fronteras entre original y copia se vuelven cuando menos confusas.[32] Además, en relación con los mensajes de datos, el término "original", en cuanto al soporte en el que por primera vez, originariamente, se consignan los datos, carece de significado, pues es el destinatario de dicho mensaje siempre recibiría una copia. Es por eso que el término original trata de suprimir los obstáculos a la presentación de originales que en los ordenamientos jurídicos tradicionalmente se exigen y que en el comercio electrónico supone una dificultad que se trata de eliminar.[33] En este sentido, el concepto de originalidad tiene que entenderse como indisolublemente unido al de integridad[34] de la información y consecuentemente al concepto de autenticación, tal y como analizaremos más adelante detenidamente.

3. *Reformas al Código de Comercio*

En lo relativo al Código de Comercio, por un lado, se reforman toda una serie de artículos encaminados a reorganizar y modernizar el funcio-

31 En otras ocasiones, si bien se distingue el original de la copia, el precio de esta última es tan evidentemente beneficioso que el usuario se decanta por ella sin importarle la menor calidad, en su caso, en aspectos no determinantes.

32 M. A. Davara Rodríguez señala que el principal problema de la aceptación del documento electrónico son las dudas sobre su originalidad y la posible alteración o modificación de su contenido, pues hay que tener en cuenta que estos documentos necesitan una transformación a lenguaje natural para que puedan ser comprendidos, desde su originario lenguaje binario, mediante un procedimiento lógico, para que pueda ser entendido por el hombre. Véase Davara Rodríguez, M. A., *Manual de derecho informático*, 6a. ed., Pamplona, Aranzadi, 2004, pp. 412 y ss.

33 Es por tanto muy pertinente en relación con algunos títulos cuya originalidad es indispensable, como los títulos valores negociables. Véase párrafo 62 de la Guía para la incorporación de la Ley Modelo sobre Comercio Electrónico.

34 En cuanto a los requisitos para la integridad de la información, véase párrafo 65 de la guía para la incorporación de la Ley Modelo sobre Comercio Electrónico.

namiento del Registro Público de Comercio, en cuanto a la inscripción y posterior gestión de los actos mercantiles mediante la utilización de técnicas informáticas, electrónicas y telemáticas.

No podemos olvidar, reiteramos, que la legislación mexicana en esta materia se basa en gran parte en la Ley Modelo sobre Comercio Electrónico, que, como ella misma avanza, no tiene como objetivo imponer la utilización de los medios electrónicos, sino, lo que es muy distinto, fomentar la igualdad jurídica entre éstos y los tradicionales, por lo que se dice textualmente que "no debe invocarse el artículo 12 para imponer al destinatario las consecuencias jurídicas de un mensaje que le haya sido enviado, si el recurso a un soporte físico distinto del papel para su transmisión sorprende al destinatario".[35]

En el Código de Comercio mexicano se determinan una serie de reglas imprescindibles para la celebración de contratos electrónicos.

1. Perfeccionamiento de contratos desde la *recepción de la aceptación*:[36] los convenios y contratos mercantiles que se celebren por correspondencia, telégrafo, o mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología, quedarán perfeccionados desde que se reciba la aceptación de la propuesta o las condiciones con que ésta fuere modificada (artículo 80).

2. Concepto de *mensaje de datos*: en los actos de comercio podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología. El Código denomina mensaje de datos a "la información generada, enviada, recibida, archivada o comunicada a través de dichos medios" (artículo 89). El mensaje de datos es uno de los conceptos alrededor del cual podríamos decir gira toda la normativa. En primer lugar, hay que aclarar que dicho término no sólo se refiere a la comunicación, sino que comprende cualquier información consignada sobre un soporte informático que no esté destinada a ser comunicada, es decir, que "el concepto de *mensaje* incluye el de información meramente consignada". En este sentido, incluso hay que entender que la definición de

35 Véase párrafo 82 de la guía para la incorporación de la Ley Modelo sobre Comercio Electrónico.

36 Véase Rico Carrillo, M., "Comercio electrónico, Internet y derecho", Caracas, Legis, 2003, pp. 117 y ss. También, Mateu de Ros, R., "El consentimiento y el proceso de contratación electrónica", *Derecho de Internet. Contratación electrónica y firma digital*, Pamplona, Aranzadi, 2000, pp. 55 y ss.

mensaje de datos pretende abarcar también el supuesto de la revocación o modificación de un mensaje de datos, puesto que, aunque se supone que el contenido de un mensaje de datos es invariable, ese mensaje puede ser revocado o modificado por otro mensaje de datos.[37]

3. *Interpretación y aplicación de las normas:* como ya mencionamos en el ámbito de las normas de derecho de las tecnologías de la información y las comunicaciones resaltan varios principios en la interpretación y aplicación, como son el de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del mensaje de datos en relación con la información documentada en medios no electrónicos, y la firma electrónica en relación con la firma autógrafa, y, como dijimos, estos principios se especifican igualmente en el artículo 89 del Código de Comercio.

4. *Eficacia jurídica de la información electrónica*: el artículo 89 bis del Código de Comercio afirma que "no se negarán efectos jurídicos, validez o fuerza obligatoria a cualquier tipo de información por la sola razón de que esté contenida en un mensaje de datos". Esta cuestión se encuentra íntimamente relacionada con la equivalencia funcional que analizamos posteriormente y a la que nos remitimos para evitar reiteraciones ineficientes.

5. *Presunción de proveniencia del mensaje de datos:* se presumirá que el mensaje de datos proviene del emisor si ha sido enviado:

a) Usando medios de identificación, tales como claves o contraseñas del emisor o por alguna persona facultada para actuar en nombre del emisor respecto a ese mensaje de datos, o

b) Por un sistema de información[38] programado por el emisor o en su nombre para que opere automáticamente (artículo 90).

6. *Presunción de que el emisor ha enviado el mensaje de datos*. El destinatario o la parte que confía podrá actuar en consecuencia, cuando:

a) Haya aplicado en forma adecuada el procedimiento acordado previamente con el emisor, con el fin de establecer que el mensaje de datos provenía efectivamente de éste.

[37] Véase parágrafo 98 de la citada Guía de incorporación de la Ley Modelo sobre Comercio Electrónico.

[38] Entendiendo por sistema de información cualquier medio tecnológico utilizado para operar mensajes de datos (artículo 91 *in fine)*.

b) El mensaje de datos que reciba el destinatario o la parte que confía, resulte de los actos de un intermediario que le haya dado acceso a algún método utilizado por el emisor para identificar un mensaje de datos como propio.

c) Excepciones:

— A partir del momento en que el destinatario o la parte que confía, haya sido informado por el emisor de que el mensaje de datos no provenía de éste, y haya dispuesto de un plazo razonable para actuar en consecuencia, o
— A partir del momento en que el destinatario o la parte que confía, tenga conocimiento, o debiere tenerlo, de haber actuado con la debida diligencia o aplicado algún método convenido, que el mensaje de datos no provenía del emisor.[39]

7. Determinación del momento de recepción del mensaje:

a) Si el destinatario ha designado un sistema de información para la recepción de mensajes de datos, ésta tendrá lugar en el momento en que ingrese en dicho sistema de información, o

b) De enviarse el mensaje de datos a un sistema de información del destinatario que no sea el sistema de información designado, o de no haber un sistema de información designado, en el momento en que el destinatario recupere el mensaje de datos.

c) Si el destinatario no ha designado un sistema de información, la recepción tendrá lugar cuando el mensaje de datos ingrese a un sistema de información del destinatario.

Lo anterior, aun cuando el sistema de información esté ubicado en un lugar distinto de donde se tenga por recibido el mensaje de datos conforme al artículo 94.

8. Determinación del momento de expedición del mensaje: salvo pacto en contra entre las partes, el mensaje de datos se tendrá por expedido cuando ingrese en un sistema de información que no esté bajo el control del emisor o del intermediario.

9. Acuse de recibo:

[39] En este sentido, salvo prueba en contrario, se presumirá que se actuó con la debida diligencia si el método usado cumple con los requisitos del código para la verificación de la fiabilidad de las firmas electrónicas.

a) Si al enviar o antes de enviar un mensaje de datos, el emisor solicita o acuerda con el destinatario que se acuse recibo del mensaje de datos, pero no se ha acordado entre éstos una forma o método determinado para efectuarlo, se podrá acusar recibo mediante:

— Toda comunicación del destinatario, automatizada o no, o
— Todo acto del destinatario, que baste para indicar al emisor que se ha recibido el mensaje de datos.

b) Cuando el emisor haya indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, se considerará que el mensaje de datos no ha sido enviado en tanto que no se haya recibido el acuse de recibo en el plazo fijado por el emisor o dentro de un plazo razonable atendiendo a la naturaleza del negocio, a partir del momento del envío del mensaje de datos.

c) Cuando el emisor haya solicitado o acordado con el destinatario que se acuse recibo del mensaje de datos, independientemente de la forma o método determinado para efectuarlo, salvo que:

— El emisor no haya indicado expresamente que los efectos del mensaje de datos estén condicionados a la recepción del acuse de recibo, y
— No se haya recibido el acuse de recibo en el plazo solicitado o acordado o, en su defecto, dentro de un plazo razonable atendiendo a la naturaleza del negocio. El emisor podrá dar aviso al destinatario de que no ha recibido el acuse de recibo solicitado o acordado y fijar un nuevo plazo razonable para su recepción, contado a partir del momento de este aviso. Cuando el emisor reciba acuse de recibo del destinatario, se presumirá que éste ha recibido el mensaje de datos correspondiente.

d) Cuando en el acuse de recibo se indique que el mensaje de datos recibido cumple con los requisitos técnicos convenidos o establecidos en ley, se presumirá que ello es así.

10. *Forma escrita y firma*: si la ley exige estas condiciones, se tendrán por cumplidas en el caso de los mensajes de datos cuando éstos sean atribuibles a las personas obligadas y accesibles para su ulterior consulta[40]

[40] Como nota puntual, si la ley exige la formalidad de que el acto se realice ante instrumento ante fedatario público, éste y las partes obligadas podrán, a través de mensajes

(artículo 93). Se define así una norma básica: todo mensaje que se requiera que conste por escrito se entenderá cumplido dicho requisito cuando la información se presenta en forma electrónica y queda de manera accesible para su posterior consulta. Esta cuestión, por supuesto, está indisolublemente unida a la del documento electrónico, que al final es lo que contiene el escrito en soporte electrónico. Se proclama así el principio de equivalencia funcional[41] de los documentos electrónicos a los documentos en papel tradicionales. En definitiva, no se trata, por supuesto, de conceder validez jurídica a todo mensaje de datos electrónicos, sino equiparación en cuanto a las exigencias requeridas en el mismo caso a un mensaje, digamos tradicional. Asimismo, cuando la ley exija que un acto jurídico se otorgue en instrumento ante fedatario público, éste y los obligados podrán, por mensajes de datos, expresar las obligaciones, y el fedatario hará constar en el instrumento los elementos por los que dichos mensajes se atribuyen a las partes y conservar bajo su resguardo una versión íntegra para ulterior consulta, otorgándolo según la ley aplicable. No obstante, veremos en más detalle este tema al hablar de firma electrónica, por lo que nos permitimos remitir al lector a dicho punto para una mayor explicación.

11. *Concepto de original*: de nuevo observamos cómo la norma especifica (artículo 93 bis) la relevancia de la originalidad del documento, y se entenderá que la información está presentada y conservada en original si cumple respecto de un mensaje de datos lo siguiente:

> a) Si existe garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma.
>
> b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar.

de datos, expresar los términos exactos en que las partes han decidido obligarse, en cuyo caso el fedatario público, deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuyen dichos mensajes a las partes y conservar bajo su resguardo una versión íntegra de los mismos para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige (artículo 93 *in fine)*.

41 Véase Illescas Ortiz, R., "La equivalencia funcional como principio elemental del derecho del comercio electrónico", *Revista Derecho y Tecnología*, Venezuela, Centro de Investigaciones en Nuevas Tecnologías Universidad Católica de Táchira, 2002, p. 23.

12. *Integridad del contenido de un mensaje de datos*: se entiende que un mensaje de datos es íntegro si ha permanecido completo e inalterado independientemente de los cambios que hubiere podido sufrir el medio que lo contiene, resultado del proceso de comunicación, archivo o presentación. La confiabilidad exigida se determinará conforme a los fines para los que se generó la información y de todas las circunstancias relevantes del caso (artículo 93 bis *in fine*).

13. *Lugar de expedición del mensaje de datos*: salvo pacto en contrario, el mensaje de datos se tendrá por expedido en el lugar donde el emisor tenga su domicilio (artículo 94).

14. *Lugar de recepción del mensaje de datos*: salvo pacto en contrario, el mensaje de datos se tendrá por recibido en el lugar donde el destinatario tenga el suyo (artículo 94).

15. *Concordancia entre el mensaje recibido y el enviado*: siempre que se entienda que el mensaje de datos proviene del emisor, o que el destinatario tenga derecho a actuar con arreglo a este supuesto, dicho destinatario tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar el iniciador, y podrá proceder en consecuencia, salvo si el destinatario sabía o hubiera sabido, de haber actuado con la debida diligencia, o de haber aplicado algún método previamente acordado, que la transmisión había dado lugar a un error en el mensaje de datos recibido (artículo 95).

16. *Individualidad de los mensajes*: se presume que cada mensaje de datos recibido es un mensaje de datos diferente, salvo que el destinatario sepa, o debiera saber, de haber actuado con la debida diligencia, o de haber aplicado algún método previamente acordado, que el nuevo mensaje de datos era un duplicado (artículo 95).

17. *Prueba:* además de lo ya comentado en el Código Federal de Procedimientos Civiles, el Código de Comercio establece dos consideraciones relevantes:

a) Reconocimiento del mensaje de datos como prueba, valorando su fuerza probatoria estimando primordialmente, como decíamos, la fiabilidad del método en que haya sido generada, archivada, comunicada o conservada (artículo 1298-A).[42]

[42] De lo anterior podemos deducir que pueden existir igualmente diversos grados de fiabilidad en cuanto a la mencionada fuerza probatoria, con diversos criterios para eva-

b) Medios de prueba admitidos: son admisibles como medios de prueba todos aquellos elementos que puedan producir convicción en el ánimo del juzgador acerca de los hechos controvertidos o dudosos y en consecuencia serán tomadas como pruebas las declaraciones de las partes, terceros, peritos, documentos públicos o privados, inspección judicial, fotografías, facsímiles, cintas cinematográficas, de videos, de sonido, mensajes de datos, reconstrucciones de hechos y en general cualquier otra similar u objeto que sirva para averiguar la verdad (artículo 1205).

En la contratación electrónica, y en el comercio electrónico en general, parece que la cuestión de la prueba resulta crucial, y que las relaciones llevadas a cabo a través de medios electrónicos tienen que contar con medios de prueba más exhaustivos y definitivos que en el entorno tradicional, donde existen gran cantidad de medios probatorios que se dejan al libre albedrío, o, mejor dicho, a "la sana crítica del juzgador".

En el entorno electrónico, por el contrario, deben preverse multitud de instrumentos que garanticen todos los extremos de dicho proceso. Nuevamente, desde nuestro punto de vista, se acucia una falta de información y formación en los usuarios, y especialmente en los expertos encargados de asesorar sobre la licitud de la prueba y de valorar la misma, en este caso. Y, por supuesto, igualmente se torna de todo punto imprescindible la existencia de normativas técnicas que estandaricen las herramientas utilizadas y las consecuencias jurídicas de su utilización, en un tipo de "homologación" administrativa, en el sentido de otorgar automáticamente una valía determinada al uso de específicas herramientas tecnológicas, y, además, dentro de un contexto global, atendiendo al mismo tiempo al tan nombrado principio de neutralidad tecnológica.

Asimismo, resulta especialmente interesante la participación de peritos y expertos en la materia que atestigüen la fiabilidad de las técnicas utilizadas, pero, insistimos, el camino, a nuestro entender, es la estandarización técnica que permita una securización de las transacciones, no tanto desde el punto de vista tecnológico, sino, también, desde el enfoque jurídico, garantizando que el empleo de determinadas técnicas conllevará *de facto* un alto grado de seguridad jurídica.

luarla, por ejemplo, en función de si han sido consignados, archivados o comunicados de forma fiable.

Concluyendo de manera general este apartado, tan sólo nos permitimos dejar aquí apuntado que en la regulación del comercio electrónico una de las cuestiones más delicadas aparece cuando surgen los conflictos, con la consecuente necesidad de determinar la ley aplicable y la jurisdicción competente, y, lamentablemente, en nuestra opinión, los expertos en la aplicación de las leyes tradicionales no están preparados ni tienen las herramientas adecuadas para afrontar los problemas surgidos como consecuencia de la utilización de estas tecnologías en el perfeccionamiento de contratos y otras relaciones jurídicas. En este sentido, es necesario contar con sistemas jurídicos claros en el punto de resolución de controversias, y, además, de tipo internacional, teniendo en cuenta, asimismo, que este punto no se puede dejar a la entera libertad de las partes, ya que, de un lado, la autonomía de la voluntad no es absoluta, y, de otro, no se puede dar por sentada la igualdad de las partes en los procesos.

Así, propugnamos el establecimiento de reglas de solución de conflictos claras y pacíficas a nivel internacional, reglas especialmente adecuadas al entorno electrónico, poniendo especial énfasis en la determinación del punto de conexión con la controversia en concreto, de modo que no se produzcan equívocos ni soluciones contrapuestas entre varias jurisdicciones que clamen tener competencia sobre el mismo asunto, paralizando el comercio y la justicia en general.

Estas reglas, en nuestra opinión, no pueden ser las tradicionales del derecho internacional, que han demostrado su ineficiencia en la solución de las cuestiones de índole electrónico, llevando a varias jurisdicciones internacionales a reclamar su competencia en el asunto en cuestión, dirimiendo además resoluciones contrapuestas, de modo que en un mundo sin fronteras se puede estar actuando lícitamente conforme a la resolución de un órgano judicial pero de modo ilícito según otro. Deben, por tanto, ser reglas adecuadas a la solución de conflictos originados en otro entorno y que, consecuentemente, deben tener en consideración nuevos puntos de conexión y nuevas soluciones en un contexto de consenso internacional, para crear un ambiente jurídico lo más seguro posible y evitar la existencia de territorios fuera de control o favorecedores de conductas típicamente ilícitas.

Además, los conflictos surgidos en el entorno electrónico van a multiplicar exponencialmente la cantidad actual de conflictos necesaria-

mente, ya que las transacciones también se verán aumentadas proporcionalmente.

De otro lado, una gran parte de los conflictos serán repetitivos, igual que lo son en el entorno tradicional, o subsumibles en categorías generales, del mismo modo que las tradicionales. Asimismo, en muchas ocasiones serán conflictos de poca cuantía o de fácil solución.

Las estructuras tradicionales de resolución judicial de conflictos, ya abrumadas incluso en su propio entorno, son, en nuestra opinión, incapaces e ineficaces en este entorno. En este sentido, deviene imprescindible la creación de unos sistemas de resolución de conflictos alternativos, basados en soluciones extrajudiciales, eficaces y eficientes, rápidos y precisos, compuestos por expertos, con un coste asequible, y con un resarcimiento justo.

No estamos demandando la desaparición del sistema judicial tradicional, aunque sí debería reformarse en su agilidad y precisión, pero no es éste el lugar para esa disquisición, sino la creación de un sistema estandarizado, con un procedimiento serio, transparente y confiable, con profesionales dedicados a resolver conflictos dentro de su experiencia. Hablamos de la justicia distributiva en su más puro estadio, sin utopías, dando a cada quien lo que merece, de manera eficaz y eficiente.

El entorno electrónico no puede soportar la burocracia de los sistemas judiciales tradicionales, ni su falta de actualización o lentitud. En los conflictos que surjan por miles de transacciones electrónicas internacionales se deberá contar con expertos internacionales capaces de resolver de manera efectiva, ayudados por la regulación pertinente, que deberá ser flexible y práctica, así como, en la medida de lo posible, de la técnica.

En definitiva, en nuestra opinión, es necesario volver a los orígenes más remotos de la fundación de los sistemas jurídicos contemporáneos, en donde mecanismos como el arbitraje, la mediación o la conciliación, en cualquiera de sus modos, eran común y exitosamente utilizados, adaptándolo, asimismo, al entorno electrónico mediante el uso de las herramientas técnicas adecuadas.

4. *Reformas a la Ley Federal de Protección al Consumidor*

Adentrándonos ahora en las reformas a la Ley Federal de Protección al Consumidor, éstas se centraron en las transacciones entre proveedores

y consumidores realizadas a través del uso de medios electrónicos, ópticos, o de cualquier otra tecnología. Así, en su artículo primero establece como su objetivo: "la efectiva protección al consumidor en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología y la adecuada utilización de los datos aportados".

En este sentido, las reglas que podemos destacar, especificadas en el nuevo artículo 76 bis y sancionadas en caso de incumplimiento, según el artículo 128, con multa por el equivalente de una y hasta dos mil quinientas veces el salario mínimo general vigente para el Distrito Federal, son las siguientes:

1. *Utilización confidencial de la información proporcionada por el consumidor*: no se podrá transmitir o difundir a otros proveedores ajenos, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente.[43]

2. *Seguridad y confidencialidad:* el proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos.

3. *Información a proporcionar al consumidor:* el proveedor deberá proporcionar al consumidor, antes de celebrar la transacción, su domicilio físico, números telefónicos y demás medios a los que pueda acudir

[43] Como ya adelantábamos en nuestro planteamiento, no podemos abarcar en este trabajo todas las materias que cubre el denominado derecho de las TIC, y, en especial, no podemos entrar en detalle en la protección de datos de carácter personal. Sin embargo, en este punto, tenemos ineludiblemente que hacer una referencia a la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (publicada en el *Diario Oficial de la Federación* el 11 de junio de 2002, reformada el 11 de mayo de 2004) que, considerando que debemos recordar que no puede tenerse en cuenta como una norma en protección de datos, sino de acceso a la información, sólo define el principio del consentimiento en relación con la fase en la que los datos se transfieren a un tercero, es decir, cuando se produce la cesión o comunicación de datos a terceros, en la que el titular pierde, en su caso, aun más el control sobre su información personal. En consecuencia, no se contempla nada acerca de la necesidad del consentimiento para el tratamiento en origen o posterior de datos de carácter personal (igual que en esta ley de protección al consumidor) y, como decíamos, sólo se especifica que se requiere del consentimiento en la comunicación de datos en los términos que establece el artículo 21 de la mencionada LFTAIPG.

el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones. Asimismo, el consumidor tendrá derecho a conocer toda la información sobre los términos, condiciones, costos, cargos adicionales, en su caso, formas de pago de los bienes y servicios ofrecidos por el proveedor.

4. *Prácticas comerciales engañosas y otros medios de publicidad ilícita:* el proveedor evitará las prácticas comerciales engañosas respecto de las características de los productos, por lo que deberá cumplir con las disposiciones relativas a la información y publicidad de los bienes y servicios que ofrezca, según la ley y el ordenamiento jurídico en su conjunto. Del mismo modo, el proveedor deberá abstenerse de utilizar estrategias de venta o publicitarias que no proporcionen al consumidor información clara y suficiente sobre los servicios ofrecidos, y cuidará las prácticas de mercadotecnia dirigidas a población vulnerable, como niños, ancianos y enfermos, incorporando mecanismos que adviertan cuando la información no sea apta para esa población.

5. *Sistema de "opt-out"*:[44] el proveedor respetará la decisión del consumidor en cuanto a la cantidad y calidad de los productos que desea recibir, así como la de no recibir avisos comerciales.

Por último, a pesar de la breve referencia, la promoción de los códigos de ética o de conducta[45] resulta muy relevante. Así, el artículo 24 de la Ley queda reformado en su fracción IX bis destacando que se promoverán, en coordinación con la Secretaría, la formulación, difusión y uso de códigos de ética, por parte de proveedores, que incorporen los principios

44 Hemos señalado intencionalmente el anglicismo entre comillas, para resaltar nuestra oposición a la utilización de dicho término, puesto que se presta a confusión en nuestro ordenamiento jurídico, donde, por el contrario, las reglas del consentimiento, y sus distintas formalidades, desde el tácito (por no hablar del presunto), hasta el expreso por escrito (pasando por el verbal y similares) están perfectamente asentadas en nuestra tradición jurídica, y no coinciden con dichos términos actualmente utilizados, que, si bien no tendrían que suponer ningún problema, introducen en muchas ocasiones la mencionada confusión por su errónea utilización.

45 Los códigos de conducta constituyen un instrumento esencial para fomentar la confianza de los consumidores en el comercio electrónico, siendo además una opción que aporta un valor añadido para la entidad que lo implanta. Así lo entienden los diferentes textos normativos en derecho comparado. Por ejemplo, la directiva europea de comercio electrónico comienza ya en sus considerandos a decir que tanto la Comisión como los Estados miembros deberán fomentar la elaboración voluntaria de códigos de conducta de libre adhesión (considerando 49 y artículo 16, entre otros).

de la ley respecto de las transacciones que celebren con consumidores a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología.

En un entorno como el que estamos describiendo, donde la flexibilización de las normas y los ordenamientos jurídicos tradicionales deviene imprescindible, aparece, como instrumento regulatorio complementario absolutamente eficaz, en nuestra opinión, los denominados códigos de conducta, o incluso códigos éticos. En el entorno electrónico, en particular, resultan especialmente idóneos, gracias a su gran capacidad de adaptación y a su adecuación a los fines específicos. Su menor rigidez y su mayor especificidad puede ser aprovechada para regular aspectos concretos, respetando obviamente las estructuras generales proporcionadas por los principios fundamentales de derecho, ayudando al cumplimiento práctico de las leyes. No obstante, al carecer estas fuentes usualmente del poder coercitivo estatal es necesario que cuenten, especialmente, con un sistema eficaz y eficiente tanto de reclamación como de resarcimiento en caso de daño o perjuicio. En este sentido, abogamos por la posibilidad de introducir estos elementos regulatorios, de cualquier índole, en las aplicaciones informáticas que sustentan los procesos electrónicos, de manera que las transacciones puedan tener ya de inicio un cierto tinte de licitud y legalidad, estandarizando las operaciones, de modo que tan sólo los casos puntuales puedan ser fuente de conflicto o de necesaria interpretación jurídica.

III. La firma electrónica

1. *Generalidades*

Siempre que nos aproximamos al estudio de la normativa de firma electrónica, nos llama la atención en primer lugar su existencia, pues su paralelo en el entorno físico nunca ha necesitado de una norma específica, y menos aun de tanta longitud y complejidad, para explicar sus funciones y efectos. No obstante, esto es, de nuevo, comprensible atendiendo a la tecnicidad tanto de la herramienta como de la propia norma y a la

necesaria explicación de las consecuencias de la utilización de esta tecnología.[46]

Teniendo en cuenta lo anterior, no podemos plantear el estudio de la normativa sin antes hablar brevemente de la técnica que soporta su funcionamiento. Así, acercándonos de una manera muy sencilla, casi aterradoramente simplificadora, a la cuestión desde el punto de vista técnico, debemos comenzar por decir que la tecnología de firma electrónica está basada en la utilización de medios criptográficos,[47] creados por algoritmos matemáticos, de menor o mayor complejidad en relación con los

46 En este sentido, la firma electrónica es una materia, dentro del derecho de las tecnologías de la información y de las comunicaciones, que despierta y lleva ya despertando un gran interés entre la profesión. Interés justificado por la potencialidad de su uso e influencia en distintos ámbitos del derecho, pues la firma electrónica en definitiva tiene al menos la misma relevancia en el entorno electrónico que la firma tradicional tiene en el entorno físico, por lo que podemos fácilmente deducir las implicaciones en toda clase de negocios y relaciones jurídicas que se lleven a cabo habitualmente.

47 La criptografía (término que procede del griego *kryptos:* oculto y *graphe*: escritura), es, según el *Diccionario de la Real Academia Española*, "el arte de escribir con clave secreta o de un modo enigmático". La criptografía es una ciencia usada desde la más remota antigüedad, lo único novedoso es la utilización de medios tecnológicos en su construcción (véase, por ejemplo, Ribagorda Garnacho, A. "Sistemas de certificación: la firma y el certificado digital", *Régimen jurídico de Internet*, *cit.*, nota 13, pp. 1315-1320). Por ejemplo, el antiquísimo método criptográfico judío *Atbash,* que consiste en sustituir la letra última del alfabeto por la primera y la penúltima por la segunda. Se dice que hasta textos del Antiguo Testamento estaban así cifrados; la cifra de César es otra de las sustituciones monoalfabéticas más simples que se pueden utilizar, y consecuentemente también más fácil de romper. Se dice que Julio César escribía a sus amigos usando una cifra simple de sustitución, donde la letra del texto sin cifrar era sustituida por la que ocupara tres lugares más tarde en el alfabeto, por ejemplo, la letra D sería sustituida por la G y así sucesivamente; Polybius era un Griego que inventó un sistema de convertir caracteres alfabéticos en caracteres numéricos, y que permitía utilizar antorchas para cifrar mensajes; la cifra de la rueda de Jefferson, que no fue utilizada sino hasta mucho después de su muerte (ya avanzado el siglo XX), se obtenía a partir de un cilindro de madera de unos 15 cm de largo y 4 de ancho que se agujereaba para permitir que se insertara un huso, cortando después el cilindro en esferas de unos 5 mm, que se dividen a su vez en 26 secciones a cada una de las cuales se le asigna una letra aleatoriamente. Estas esferas se ponen sobre el huso y empieza la codificación, que por supuesto requiere que el remitente tenga un cilindro igual para descifrar, porque las ruedas al girar dejan ver un fragmento del mensaje y cuando se vuelve a girar sigue saliendo más mensaje; u otros métodos mecánicos han sido ya más modernamente utilizados como la máquina enigma, utilizada por los alemanes en la Segunda Guerra Mundial para cifrar los mensajes militares, que es simétrico también, porque el método de codificación y el que descifra es igual, aunque las máquinas se deben instalar idénticamente para que funcione.

métodos de cifrado más usuales (simétrico o asimétrico) empleados. Mediante el cifrado, unos datos legibles se convierten en ilegibles, de forma que los terceros que desconozcan la clave necesaria para descifrarlos no puedan tener acceso a los mismos.

El cifrado de clave simétrica o secreta es aquél en el que para cifrar y descifrar unos datos se utiliza la misma clave, que deberá ser conocida tanto por el emisor como por el receptor de la comunicación, y que requiere de la confianza entre las partes para poner en conocimiento de la otra parte la clave utilizada y, en su caso, de un canal seguro para comunicar la clave. Por lo tanto, este método tiene varios inconvenientes a simple vista.

El segundo tipo de cifrado es el de clave asimétrica o pública, en el que se utilizan dos claves, lo que una cifra la otra lo descifra, y viceversa. Por ejemplo, si utilizamos la clave privada para cifrar los datos y la clave pública para descifrarlos, el receptor de una determinada información conocerá la clave pública del emisor con la que descifrará unos datos que sólo podrán haber sido cifrados con la clave privada del emisor. El algoritmo de cifrado utilizado se apoya en la conocida infraestructura de clave pública (o PKI por sus siglas en inglés, *public key infraestructure*). Este método de cifrado tiene las ventajas de las que carece el simétrico ya comentado y es el usualmente utilizado en las transacciones de comercio electrónico que requieren mayor seguridad.

Habiendo visto, como avisábamos, de manera absolutamente escueta el funcionamiento técnico que soporta la firma electrónica, y reiterando y entendiendo que el ámbito de esta publicación requería, en nuestra opinión, dicha aproximación, vamos a pasar a analizar otras cuestiones que nos conducen a la problemática jurídica que conlleva la utilización de las mismas.

Así, si comenzamos pensando en el entorno tradicional, acerca de las funciones que desarrollan las firmas, esto es, en términos generales,[48] las manuscritas, parece que éstas se encuentran muy asentadas: identifican y autentican. Es decir, garantizan quién es el que firma y por tanto le identifi-

[48] Las firmas, no obstante, no sólo son manuscritas (en contraposición a la firma electrónica que estamos analizando), pues podemos hablar de distintos procedimientos, que también se denominan firmas, aunque evidentemente aporten mayor o menor certeza, que se utilizan para asignar la voluntad de su autor al documento al que se incorpora, como por ejemplo, los métodos de estampillado o sellado, firmas mecanografiadas o perforadas.

can, y asocian la voluntad, la intención del autor al firmar el documento, es decir, le autentican, asocian el contenido del documento[49] al autor.

En cuanto al grado de certeza,[50] como decíamos, es una característica también predicable de los distintos tipos de firma, incluida la electrónica, y así en las diferentes normativas se prevé la posibilidad de establecer distintos niveles de firmas electrónicas, con vistas a obtener una equivalencia funcional perfecta. Podemos distinguir las siguientes funciones[51] en el mecanismo de firma electrónica:[52]

- *Identificación de las partes:* el uso de la firma electrónica garantiza que los intervinientes son quienes dicen ser.

49 Ya hemos hecho siquiera una concisa referencia al reconocimiento de eficacia jurídica del documento electrónico y a su admisión como prueba documental. No obstante, cabe mencionar aquí que, como documentos electrónicos, como veremos en su momento, podemos diferenciar tres clases, en primer lugar el documento en soporte papel que haya sido generado por medios informáticos; esto es el listado impreso de la información que se encuentra en un soporte informático (lo que se conoce como un *"printout"*), en segundo lugar el documento informático que se encuentra en soporte de información electrónico, creado por datos almacenados en la memoria de un ordenador (lo que se conoce como *"input"*), y en tercer lugar encontramos un soporte de información electrónico formado mediante el intercambio de mensajes con una estructura determinada utilizando unas normas de intercambio informáticas (el conocido como EDI o *Electronic Data Interchange*).

50 Igualmente se podría profundizar en el estudio de los diferentes medios utilizados para conseguir el objetivo final de la autenticación, que básicamente podríamos agrupar bajo los que se definen por "lo que el usuario sabe" (una contraseña, por ejemplo), "lo que el usuario tiene" (un *token*, una tarjeta de plástico, etcétera) y "lo que el usuario es" (por ejemplo, un dato biométrico como la huella dactilar o la retina). Estos métodos, por supuesto, tienen distintos grados de fiabilidad. No obstante, en general resulta más fiable en cuanto se combinan varios de ellos (por ejemplo, una contraseña con la inspección ocular de retina). Pero eso no se puede afirmar con carácter general, ya que la fortaleza de toda cadena depende de la debilidad del más débil de sus eslabones, es decir, si uno de esos medios de autenticación es más débil que cualquier otro, aunque los otros dos fueran idénticos en su forma de autenticar (por ejemplo, si dos contraseñas como idéntica forma de autenticar fueran más fuertes que una tarjeta y una contraseña a causa, por ejemplo, de la débil seguridad de la tarjeta), en realidad esta mezcla de formas de autenticar no estaría añadiendo sino restando seguridad. Pero, en todo caso, como venimos argumentando reiteradamente, ningún método o tecnología puede ser descartado si cumple con los requisitos de seguridad y garantiza los objetivos perseguidos en la legislación.

51 Véase párrafo 29 de la guía de incorporación de la Ley Modelo sobre firmas electrónicas.

52 Véase Davara Rodríguez, M. A., "Una aproximación al concepto jurídico de firma electrónica", *Revista del Colegio Oficial de Ingenieros Industriales de Madrid,* Madrid, Colegio Oficial de Ingenieros Industriales de Madrid, febrero de 2002.

- *Autenticación del contenido:* el contenido del mensaje que se transmite a través de medios electrónicos tiene que ser el que las partes pusieron.
- *Integridad del contenido:* el mensaje no puede haber sido modificado durante su transmisión.
- *Confidencialidad:* el contenido debe ser secreto entre las partes, evitando que un tercero no autorizado pueda tener acceso al mismo.
- *No repudio entre las partes (en origen y en destino):* se tiene que poder garantizar que ninguna de las partes puede negar haber enviado o recibido el mensaje.

Estas funciones no son explicadas de forma unánime por la doctrina, y que la normativa, mexicana e internacional, como sabemos, no las distingue tan claramente.[53] En muchas ocasiones se unen, por ejemplo, los conceptos de autenticación e integridad, pues se dice que si un mensaje es auténtico tiene que estar íntegro y viceversa. No obstante, si pensamos en relación con el funcionamiento práctico de la firma electrónica, entonces podemos razonar del siguiente modo: cuando se firma el documento en concreto, entonces se tiene que garantizar la identificación de las partes y la autenticación del mensaje; ahora bien, cuando el mensaje se envía a su destinatario, es decir, sale del poder de disposición del emisor, entonces se tiene que garantizar la integridad y, en su caso, la confidencialidad.[54]

53 Estas funciones no son así explicadas por todos los autores, incluso la normativa, como sabemos, no las distingue tan claramente, y, también, hemos de reconocer que así no lo hicimos en un primer artículo publicado en la revista *Otrosí* del Ilustre Colegio de Abogados de Madrid de diciembre de 2002, rectificando sin embargo en otro artículo en la misma publicación al poco tiempo (véase, respectivamente, Davara F. de Marcos, I., "La firma electrónica", *Otrosí*, Ilustre Colegio de Abogados de Madrid, diciembre de 2002; y *id*., "La nueva Ley de Firma Electrónica", *Otrosí*, Ilustre Colegio de Abogados de Madrid, febrero de 2004).

54 Nos resulta curioso, de nuevo, cómo a la versión electrónica de la firma se le exigen o, mejor dicho, se pretende hacer que cumpla muchos más requisitos que la firma tradicional manuscrita, y, aun cumpliéndolos, todavía se desconfía más de su uso. Es el caso de la confidencialidad. En ningún momento en el entorno físico el hecho de firmar un documento implica que dicha firma pueda garantizar la confidencialidad del mismo, y, sin embargo, en el ámbito electrónico, si bien no es una función que la ley deba imponer, en muchos casos se aconseja. No nos quejamos de que esto sea así, pues si la técnica puede aportar estas ventajas, debe aprovecharse, pero sí nos perturba que exista esa desconfianza sobre la misma.

La autenticación supone que el contenido del mensaje es legítimo, es decir, que se asocia a sus autores tal y como ellos dispusieron.[55]

En cuanto a la integridad, tiene que poder asegurarse que el contenido del mensaje no ha sido manipulado durante su transmisión. A nivel técnico, y sin ánimo de profundizar en ello, la función *hash* (o resumen), es la que garantizaría que el mensaje no ha sido manipulado al tener que coincidir el resumen cifrado con el mensaje.[56]

[55] A lo largo de la Ley Modelo sobre firmas electrónicas, podríamos entrar en lo que la doctrina entiende como autenticación, es decir, si el contenido representa la voluntad del firmante. Pero la Ley Modelo sobre firmas electrónicas aun va más allá y se cuestiona si se produce algún efecto jurídico al utilizarse técnicas de firma electrónica cuando el firmante no tiene la clara intención de quedar jurídicamente vinculado por la aprobación de la información firmada por medios electrónico. Y todo lo anterior sin ni siquiera entrar en el contenido de la información, porque la Ley Modelo sobre firmas electrónicas no entra en esas cuestiones, puesto que no pretende interferir en el derecho contractual o de obligaciones, es decir, el hecho de que la vinculación del firmante produjera efectos jurídicos (contractuales o de otra índole) dependería de la naturaleza de la información consignada y de otras circunstancias que habría que evaluar conforme al derecho aplicable al margen de la Ley Modelo sobre firmas electrónicas. Por su parte, la OCDE entiende que, mientras que el término autenticación electrónica se refiere a un método tecnológico de confirmación sobre algo acerca de una pieza de información, el término "firma electrónica" generalmente se refiere a un identificador adjunto a, o lógicamente asociado con, un mensaje electrónico, documento o datos, y cuyo propósito implica el concepto legal de una "firma" aplicado en el mundo electrónico. En este sentido, el término firma electrónica refleja una implicación legal cuando una tecnología concreta se utiliza para firmar un mensaje. Una firma electrónica puede indicar la intención de una persona de respaldar, aprobar, estar vinculado por, o en otro caso estar asociado a los contenidos de un mensaje electrónico, documento u otros tipos de datos. Sin embargo, en esta aproximación legal, la tecnología de firma electrónica no necesita necesariamente, en o por si misma, verificar ninguna pieza de información, sólo necesita indicar la intención del firmante: por ejemplo, un nombre mecanografiado al final de un mensaje de *email* es un tipo de firma electrónica —aunque uno con unas limitaciones de seguridad obvias— si indica la voluntad del firmante con respecto al texto del mensaje. Cuando una firma electrónica utiliza un método particular de autenticación electrónica para conseguir sus objetivos legales, hay un solapamiento entre los dos conceptos. Véase OCDE, *Background paper on electronic authentication technologies and issues, Joint OECD-Private Sector Workshop on Electronic Authentication, Organisation for Economic Cooperation and Development*. Information, Computer and Communications Policy Committee, Working Party on Information Security and Privacy. Stanford and Menlo Park, California, 2-4 June 1999.

[56] La Ley Modelo sobre firmas electrónicas trata en su artículo 6o., clave dentro del texto, la cuestión de la integridad del mensaje firmado electrónicamente. En los aparta-

Por último, la posibilidad de contar con el no repudio de las partes resulta de una importancia esencial a efectos de la conclusión y el perfeccionamiento de las relaciones jurídicas así formalizadas.[57]

Logísticamente, el mercado comercial de la firma electrónica se ha estructurado básicamente, y de nuevo reiterando la simplicidad en la exposición de este estudio debido a su peculiar enfoque, conforme a la denominada infraestructura de clave pública, sistema basado en la existencia de terceros de confianza que típicamente emiten certificados que incorporan la clave pública que corresponde a la clave privada generada por el titular de dicho certificado y que además pueden incluir otra gran cantidad de información sobre sus titulares.

Estos prestadores de servicios de certificación (PSC), sobre los que también encontramos referencias a ellos en la doctrina y en derecho comparado como "autoridades de certificación" o comercialmente como "terceros de confianza", son, por lo tanto, los encargados de, entre muchas otras cosas, gestionar los certificados que, en última instancia, unen a los titulares o signatarios, usuarios de la firma electrónica, con los datos que verifican que ostentan dicha titularidad.

La estructura piramidal de la infraestructura de clave pública en el mercado[58] mexicano se puede esquematizar del siguiente modo:[59]

- En el nivel superior la autoridad raíz,[60] que es la base de confianza de toda la infraestructura de clave pública (PKI) y es la que da valor a los certificados electrónicos a través de su certificado raíz.

dos *c* y *d* se regulan la integridad de la firma electrónica y la integridad de la información consignada en el mensaje firmado electrónicamente.

57 Davara & Davara, *Factbook sobre comercio electrónico, cit.,* nota 7, pp. 50 y ss.

58 Para una mayor explicación de la estructura de funcionamiento de los PSC, en concreto en un entorno de Infraestructura de Clave Pública, véase varios autores, "Autoridades de certificación y confianza digital", *XIII Encuentros sobre informática y derecho, cit.*, nota 30, pp. 179 y ss.

59 Véase párrafo 51 de la guía para la incorporación de la Ley Modelo sobre firmas electrónicas.

60 La autoridad raíz (*Root CA*) es la entidad que se encuentra en el nivel más alto de la jerarquía de la infraestructura de clave pública y está encargada de autorizar y emitir los certificados de las autoridades de certificación o PSC. Se trata por tanto de la base de confianza de toda la infraestructura de clave pública, puesto que emite el certificado raíz sobre el que se generan el resto de certificados electrónicos que se utilizan para generar la firma electrónica.

- En un nivel inferior se encuentran las autoridades de certificación o prestadores de servicios de certificación,[61] ya sean personas físicas o jurídicas, que proporcionan los servicios de firma electrónica entre los que se encuentran la emisión de certificados.
- Dependientes de estas últimas, se encuentran las autoridades de registro,[62] que son personas o entidades que desarrollan determinadas funciones de verificación de la identidad de los solicitantes de los certificados, llevando a cabo en su caso la gestión de las solicitudes ante los PSC.
- Finalmente, tenemos a los solicitantes de los certificados, que pueden coincidir o no, con los firmantes, ya que puede tratarse de la persona física o jurídica que va a firmar o de un representante de la misma. En este sentido, la firma electrónica de las personas jurídicas es una cuestión muy complicada[63] en la que lamentable-

61 La autoridad de certificación (CA, *Certification Authority* o TTP, *Thrusted Third Partie*) o PSC, es definida por la directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre, por la que se establece un marco comunitario para la firma electrónica (en adelante, Directiva europea sobre firma electrónica) como:"la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica", aunque la denomina proveedor de servicios de certificación. Son las terceras partes, los PSC, en quienes confían los usuarios y quienes, entre otras cosas, emiten los certificados que contienen los datos de verificación de firma de dichos usuarios.

62 La autoridad de registro (en inglés RA, *Registry Authority*) es la entidad encargada de identificar de forma inequívoca al solicitante y de gestionar su solicitud ante la autoridad de certificación o PSC. Ésta no es una figura legal, sino comercial.

63 Véase al respecto el parágrafo 121 de la guía para la incorporación de la Ley Modelo sobre firmas electrónicas que analiza la problemática de la firma en las personas jurídicas cuando unos mismos datos de creación de firma pueden haber sido utilizados por varios firmantes. Y asimismo, en su parágrafo 122, vuelve a plantear la posibilidad de que el firmante pudiera autorizar a otra persona a utilizar en su nombre los datos de la firma, poniendo varios ejemplos. De igual forma, quizá éste haya sido el tema más controvertido de todas las novedades introducidas en la Ley de Firma Electrónica Española (Ley 59/2003, del 19 de diciembre, de firma electrónica publicada en el *Boletín Oficial del Estado* núm. 304, del 20 de diciembre) respecto de su predecesora (el Real Decreto-ley 14/1999, del 17 de septiembre, sobre firma electrónica, publicado en el *Boletín Oficial del Estado* del 19 de septiembre). Véase Davara F. de Marcos, I., "La nueva Ley de Firma Electrónica", *cit*., nota 53.

mente, de nuevo, no podemos profundizar lo que sería necesario.[64]

Para finalizar esta breve introducción nos gustaría señalar que la utilización de la firma electrónica sólo está en sus estadios iniciales. La firma electrónica será un elemento tan usual en nuestra vida como nuestra tarjeta de pago, o más incluso, por todas sus aplicaciones. Existen aplicaciones que podrían parecer grandilocuentes que ya se vislumbran, como el voto electrónico, pero el uso de la firma electrónica va a ir mucho más allá, por su cotidianeidad, porque será nuestro identificador más personal. Asimismo, la firma electrónica será, en concreto, de gran utilidad en el entorno empresarial, donde resulta especialmente interesante la evolución de la tradicional y obligadamente formal figura de la representación.

Es necesario, por ende, que el titular tome conciencia del significado de la firma electrónica, resaltando la relevancia del concepto de identidad virtual como algo inseparable, no técnica sino idealmente, de nuestra identidad física, pero, con, al menos, las mismas consecuencias.

2. *Marco normativo*

En definitiva, con la regulación sobre firma electrónica, lo que se persigue, al igual que en normas de ámbito similar, es generar en el entorno virtual condiciones de seguridad y confianza similares a las existentes en el mundo físico y estimular así el desarrollo del comercio y de la administración electrónicas.

De nuevo, como adelantábamos, la normativa mexicana se basa en la mencionada Ley Modelo sobre Firmas Electrónicas, donde se trató en principio de abarcar todas las situaciones de hecho en que se utilizan firmas electrónicas, independientemente del tipo de firma electrónica o de técnica de autenticación que se aplique.[65]

64 Para mayor información, véase Linares Gil, M. I. "La administración tributaria electrónica", *Derecho de Internet. Contratación electrónica y firma digital*, *cit.,* nota 36, pp. 615 y 616.

65 Tal y como se explica en la guía de incorporación de la Ley Modelo sobre firmas electrónicas: "Durante la preparación de la Ley Modelo se estimó que si se excluía alguna forma o algún medio mediante una limitación del ámbito de aplicación de la Ley Modelo podían surgir dificultades prácticas que irían en contra de la finalidad de ofrecer unas disposiciones auténticamente neutrales con respecto a los medios técnicos y a las tecnologías".

Ningún método de firma electrónica puede ser discriminado, es decir, debe darse a todas las tecnologías la misma oportunidad, sin diferencias de tratamiento entre los mensajes firmados electrónicamente y los documentos de papel con firmas manuscritas, ni entre diversos tipos de mensajes firmados electrónicamente, siempre y cuando cumplan los requisitos básicos.[66]

En este sentido, la Ley Modelo sobre Firmas Electrónicas trata de reflejar en particular: el principio de la neutralidad[67] respecto de los medios técnicos utilizados;[68] además de la no discriminación de todo equivalente funcional de los conceptos y prácticas que tradicionalmente funcionan sobre soporte de papel, así como una amplia confianza en la autonomía de la voluntad contractual de las partes.[69]

66 Realmente, muchos de los requisitos van unidos a la comprobación y aseguramiento de la fiabilidad de la firma, lo que, tal y como señala Davara Rodríguez, se puede garantizar mucho más fácilmente en las firmas electrónicas que en las tradicionales manuscritas. Véase Davara Rodríguez, M. A. "Firma electrónica y autoridades de certificación: El notario electrónico", *XIV Jornadas de Archivos Municipales. El acceso a los documentos municipales*, Parla 23-24 de mayo de 2002, pp. 247-250.

67 La guía para la incorporación de la Ley Modelo sobre firmas electrónicas señala asimismo en su parágrafo 5: "Las palabras *entorno jurídico neutro*, utilizadas en la Ley Modelo de la CNUDMI sobre Comercio Electrónico, reflejan el principio de la no discriminación entre la información consignada sobre papel y la información comunicada o archivada electrónicamente. La nueva Ley Modelo refleja asimismo el principio de que *no debe discriminarse ninguna de las diversas técnicas* que pueden utilizarse para comunicar o archivar electrónicamente información, un principio a veces denominado «de neutralidad tecnológica» (A/CN.9/484, párrafo 23)".

68 A pesar de lo anterior, la Ley Modelo sobre firmas electrónicas sí distingue, en su beneficio, ciertas técnicas consideradas particularmente fiables independientemente de las circunstancias en que se utilicen, y así lo dispone en su artículo 6.3. El objetivo de esta disposición es añadir mayor certeza a que la que proporcionaba la Ley Modelo sobre Comercio Electrónico en cuanto al efecto jurídico que cabe esperar de la utilización de tipos de firmas electrónicas particularmente fiables. En definitiva, lo que el artículo 6.3 dice es que se tiene que crear la certeza, en el momento de utilizarse la técnica de firma electrónica o con anterioridad a ese momento (*a priori*), de que la utilización de una técnica reconocida producirá efectos jurídicos equivalentes a los que surtiría una firma manuscrita.

69 En el entorno europeo, la Directiva 1999/93/CE sobre firma electrónica, señala en su Considerando 8 "Los rápidos avances tecnológicos y la dimensión mundial de Internet hacen necesario un *planteamiento abierto a diferentes tecnologías y servicios de autenticación electrónica de datos*", y en el considerando 27: "Considerando 27: transcurridos dos años desde su aplicación, la Comisión procederá a una revisión de la presente Directiva a fin de cerciorarse de que los avances tecnológicos y los cambios del entorno jurídi-

Por otro lado, como mencionábamos, el principio de la equivalencia funcional es quizás la característica más nombrada cuando hablamos de legislación de firma electrónica, siguiendo, asimismo, la pauta de la Ley Modelo sobre Comercio Electrónico.[70]

En concreto, el uso de la firma electrónica en lo que hace a México está regulado en varios ordenamientos distintos.[71] En el Código de Comer-

co no han creado obstáculos al logro de los objetivos formulados en la presente Directiva. La Comisión debe estudiar la incidencia de ámbitos técnicos afines y presentar un informe al respecto al Parlamento Europeo y al Consejo". Y, en un ámbito más concreto resulta en este sentido interesante lo expuesto en el Dictamen del Comité de las Regiones sobre la Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se establece un marco común para la firma electrónica (1999/C 93/06) aprobada los días 13 y 14 de enero de 1999: "2.2. Las telecomunicaciones y el comercio electrónico mundiales dependen, según la propuesta, de la *adaptación progresiva de la normativa nacional e internacional a la rápida evolución de la infraestructura tecnológica.* Aunque, a menudo, proceder por analogía con las normas existentes brinda una solución satisfactoria, en ocasiones es necesario introducir modificaciones en función de las nuevas tecnologías para evitar efectos indeseados. Aunque las firmas digitales creadas con técnicas criptográficas *son hoy un tipo importante de firma electrónica,* en opinión de la Comisión, el marco reglamentario europeo debe poseer flexibilidad suficiente para regular otras tecnologías que puedan utilizarse con fines de autenticación".

70 Hay que tener en cuenta que la Comisión se planteó en algún momento redactar la Ley Modelo sobre firmas electrónicas como una continuación de la Ley Modelo sobre comercio electrónico, en desarrollo de su artículo 7o. (véase párrafo 65 de la guía de incorporación de la Ley Modelo sobre firmas electronicas).

71 En el ámbito comercial: decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor; Norma Oficial Mexicana NOM-151-SCFI-2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos; Decreto por el que se reforman y adicional diversas disposiciones del Código de Comercio en Materia de Firma Electrónica; Reglamento del Código de Comercio en materia de Prestadores de servicios de Certificación; Reglas generales a las que deberán sujetarse los prestadores de servicios de certificación. En el ámbito tributario: decreto por el que se reforman, adicionan y derogan diversas disposiciones del Código Fiscal de la Federación; Primera Resolución de Modificaciones a la Resolución Miscelánea Fiscal para 2004; Anexo 20 de la Resolución Miscelánea Fiscal para 2004. En el sector bancario: Transitorio Cuarto, Reformas Código Comercio 2003 faculta a Banco de México para regular y coordinar a la autoridad registradora central, registradora y certificadora de las instituciones financieras y de las empresas que les prestan servicios auxiliares o complementarios relacionados con TEF o valores que presten servicios de certificación; Circulares Telefax 19/2002 y 19/2002 bis, del 5 de julio de 2002 y del 11 de julio de 2003-Infraestructura Extendida de Seguridad. En el sector pú-

cio[72] se entiende recomendable que, en cualquier caso, se utilice una firma electrónica que permita ser equiparada funcionalmente con la firma manuscrita y sea admisible como prueba en juicio, de manera que debe tenderse al uso de la firma electrónica avanzada.[73]

3. *Ámbito comercial*

No obstante, a pesar de la ya mencionada dispersión de ordenamientos jurídicos, lo cierto es que las normas cruciales, cuantitativamente en función de su ámbito competencial y cualitativamente por su aplicación supletoria y subsidiaria en muchos casos, y en la materia son las emitidas por la Secretaría de Economía.[74]

Comenzando por el decreto del 29 de agosto de 2003, y analizando lo referido a firma electrónica, remitiéndonos a la parte de contratación en lo que se haya modificado al respecto, en concreto el esencial artículo 89, ya analizado anteriormente, comienza, como ya dijimos, por asentar los principios esenciales en la interpretación y aplicación de las normas

blico: Ley Federal de Procedimiento Administrativo (LFPA), habilitando el empleo de medios electrónicos para algunos procedimientos administrativos de gestión; Código Fiscal de la Federación, en su artículo 17-D párrafo 10 dice que el SAT aceptará los certificados de FEA que emita la SFP para los servidores públicos según las leyes; Acuerdos Tramitanet, Declaranet y Compranet.

72 Decreto por el que se reforman y adicionan diversas disposiciones del Código de Comercio en Materia de Firma Electrónica, publicado en el *Diario Oficial de la Federación* del 29 de agosto de 2003.

73 Así, en definitiva, en México hay cuatro (o tres en puridad) autoridades registradoras centrales (ARC) de firma electrónica avanzada según la Ley de la Administración Pública Federal, el Código de Comercio, el código Fiscal y la Ley de Instituciones Financieras, cuya administración ostentan la Secretaría de la Función Pública (gobierno), Secretaría de Economía (comercio), la Secretaría de Hacienda y Crédito Público (fiscal, junto con Banco de México) y el Banco de México (sistema financiero).

74 En concreto nos referiremos a las siguientes por su relevancia, sin perjuicio de otras de menor rango o más específicas:

1. Decreto por el que se reforman y adicionan diversas disposiciones del Código de Comercio en materia de firma electrónica, publicado en el *Diario Oficial de la Federación* el viernes 29 de agosto de 2003.

2. Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación, publicado en el Diario Oficial de la Federación el 19 de julio de 2004.

3. Reglas generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, publicadas en el Diario Oficial de la Federación el 4 de agosto de 2004.

de tecnologías de información y comunicaciones, insistimos, la neutralidad tecnológica, la autonomía de la voluntad, la compatibilidad internacional y la equivalencia funcional del documento, y la firma electrónicos.

Las definiciones, como en todas las normas técnicas, son indispensables.[75] En este sentido, por razones principalmente de exposición, pasamos a resaltar y comentar algunas de ellas:

1. *Firma electrónica*: ya no sólo por la relevancia *per se* de la definición, sino porque la norma entiende que cualquier firma electrónica, sin distinción de ninguna tecnología aplicada, produce los mismos efectos jurídicos que la firma autógrafa y es admisible en juicio. Así, señala la definición:

> Los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología,[76] que son utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información contenida en el mensaje de datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.

Como ya adelantábamos, la definición implica identificación del autor y autenticación del contenido, además de exponer el concepto de equivalencia funcional, núcleo de esta legislación. Por otro lado, sin embargo, y

75 Aun a riesgo de caer en lo que previene la conocida máxima latina: "*Omnis definitio in iure civili periculosa est: parum est enim, ut non subverti posset",* es decir, toda definición en derecho es peligrosa porque hay poco que no pueda ser impugnado (Javoleno, Digesto, 50, 17, 202).

76 Ante la evolución de las innovaciones tecnológicas, la normativa establece criterios para el reconocimiento jurídico de las firmas electrónicas independientemente de la tecnología utilizada (a saber, firmas electrónicas basadas en la criptografía asimétrica; los dispositivos biométricos que permiten la identificación de personas por sus características físicas, como su geometría manual o facial, las huellas dactilares, el reconocimiento de la voz o el escáner de la retina, etcétera; la criptografía simétrica; la utilización de números de identificación personal; la utilización de contraseñas para autenticar mensajes de datos mediante una tarjeta inteligente u otro dispositivo en poder del firmante; versiones digitalizadas de firmas manuscritas; la dinámica de firmas; y otros métodos, como la selección de un signo afirmativo en la pantalla electrónica mediante el ratón). Es decir, la normativa es, como decíamos, tecnológicamente neutral, aunque, por otro lado, es justo decir que se decanta por el uso de una tecnología, la de cifrado, y más concretamente la de clave pública, que es la que se entiende tiene mayor reconocimiento.

uniendo este concepto al siguiente de firma electrónica avanzada, toda la materia probatoria encuentra aquí gran relevancia.[77]

2. *Firma electrónica avanzada o fiable*: a continuación la norma describe lo que se entiende por firma electrónica avanzada o fiable,[78] remitiéndose al artículo 97 para especificar sus requisitos, que son los siguientes:[79]

a) Los datos de creación de firma en el contexto que son utilizados corresponden exclusivamente al firmante.

77 La diferencia jurídica entre estos dos tipos de firma es sustancial, principalmente desde el enfoque de la validez probatoria y de la eficacia jurídica. No obstante lo anterior, insistimos, a ningún tipo de firma electrónica se le podrá negar efectos jurídicos ni será excluida como prueba en juicio por el mero hecho de presentarse en forma electrónica.

78 Por un lado, tenemos que mostrar nuestra disconformidad ante el adjetivo de fiable que parece que prejuzga que el otro tipo de firma electrónica carece de dicha fiabilidad. Por su parte, el artículo 6o. de la Ley Modelo sobre firmas electrónicas puede parecer a simple vista que no establece una distinción diáfana entre la utilización de un determinado tipo de firma y otro. No obstante, sí lo hace, en cuanto a sus efectos jurídicos (al igual que, por ejemplo, lo hacen la normativa comunitaria europea y la norma española). Sin embargo, durante la tramitación de la Ley Modelo sobre firmas electrónicas se convino en hacer una distinción más sutil (véase, entre otros, parágrafo 118 de la Guía para la incorporación de la Ley Modelo sobre firmas electrónicas) entre las diversas técnicas posibles de firma electrónica, ya que debería evitarse que la Ley Modelo sobre firmas electrónicas discriminara algún tipo de firma electrónica, y dejar claro en todo caso que cualquier técnica (principio de neutralidad tecnológica) de firma electrónica aplicada con el propósito de firmar un mensaje de datos en el sentido del artículo 7.1.a. de la Ley Modelo sobre Comercio Electrónico podía producir efectos jurídicos, siempre y cuando fuera suficientemente fiable habida cuenta de todas las circunstancias, incluidos los eventuales acuerdos entre las partes (esto es, respeto al principio de la autonomía de la voluntad). A pesar de lo anterior, la Ley Modelo sí distingue, en su beneficio, ciertas técnicas consideradas particularmente fiables independientemente de las circunstancias en que se utilicen, y así lo dispone en el párrafo 3o. del artículo 6o. de la Ley Modelo. El objetivo de esta disposición es añadir mayor certeza a la que proporcionaba la Ley Modelo sobre Comercio Electrónico en cuanto al efecto jurídico que cabe esperar de la utilización de tipos de firmas electrónicas particularmente fiables (como dice el parágrafo 4 de la Guía de incorporación de la Ley Modelo sobre firmas electrónicas). En definitiva, lo que el artículo 6.3 dice es que se tiene que crear la certeza, en el momento de utilizarse la técnica de firma electrónica o con anterioridad a ese momento (*a priori*), de que la utilización de una técnica reconocida producirá efectos jurídicos equivalentes a los que surtiría una firma manuscrita. En realidad, los apartados *a)* a *d)* del párrafo 3o. expresan criterios objetivos de fiabilidad técnica de las firmas electrónicas.

79 La firma electrónica avanzada es aquella firma electrónica creada por medios que el signatario mantiene bajo su exclusivo control y está vinculada a él y a los datos a los que se refiere, permitiendo detectar cualquier modificación ulterior de los mismos.

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.

d) Respecto a la integridad de la información de un mensaje de datos, es posible detectar cualquier alteración de ésta hecha después del momento de la firma.

Señalaremos finalmente, como mero apunte, que la definición termina diciendo: "En aquellas disposiciones que se refieran a firma digital, se considerará a ésta como una especie de la firma electrónica".[80]

3. *Mensaje de datos*: la definición resalta que será cualquier información generada, enviada, recibida o archivada por "medios electrónicos, ópticos o cualquier otra tecnología", como ya hemos analizado en relación con la legislación general del Código de Comercio adonde nos remitimos.

4. *Prestador de servicios de certificación*: la persona o institución pública que preste servicios relacionados con firmas electrónicas y que expide, en su caso, los certificados. El reformado capítulo III del título II se dedica a dichos PSC y lo comentaremos más adelante brevemente .

Pasando al articulado, el capítulo II del título II se dedica por entero a las firmas, comenzando su artículo 96 por exponer que todas las disposiciones del Código de Comercio deberán aplicarse para que no excluyan, restrinjan o priven de efecto jurídico cualquier método de firma electrónica, lo que de nuevo vuelve a reforzar los conceptos y principios generales ya comentados.

El artículo 97, como ya hemos visto, está destinado a los requisitos que debe reunir la firma electrónica avanzada o fiable, estableciendo, además, que se puede demostrar la fiabilidad o no fiabilidad de una firma electrónicas por cualquier persona, y, ya en el artículo 98, que los prestadores de servicios de certificación deberán determinar y dar a conocer si las firmas electrónicas avanzadas que utilicen cumplen los requisitos

[80] Párrafo muy acertado en su concreción, aunque no sabemos si en su necesidad dentro del articulado. La firma electrónica, alejándonos ahora de requisitos a efectos de su distinta eficacia jurídica, es una firma creada por medios electrónicos, que está asociada a unos datos en forma electrónica. El concepto de firma digital, por su parte, sin ninguna trascendencia jurídica, puede referirse a cualquier forma digitalizada de firma, desde un firma manuscrita escaneada, hasta una firma utilizando un lápiz óptico, por ejemplo, pero no es un término jurídico y por lo tanto no debemos utilizarlo dentro de este ámbito.

mencionados en el artículo 97. Para cerrar el capítulo, el artículo 99 se dedica a las obligaciones del firmante.[81]

El capítulo III, por su parte, como adelantábamos, se destina a desarrollar la figura de los prestadores de servicios de certificación. Tal y como establece el artículo 105, será la Secretaría de Economía la que coordinará y actuará como autoridad certificadora y registradora respecto de los PSC establecidos que, según su artículo 100 pueden ser, previa acreditación por la Secretaría de Economía, los notarios y corredores públicos,[82] las personas morales privadas[83] y las instituciones públicas según su normativa. En el artículo 102 se establece el proceso de acreditación de los PSC ante la Secretaría de Economía, para la cual deben cumplirse unos requisitos, entendiéndose concedida dicha acreditación si la Secretaría no ha resuelto sobre la misma en los 45 días siguientes a la solicitud.

En el artículo 104 se enumeran las obligaciones de los PSC, entre las que cabe destacar, la identificativa[84] del firmante, la informativa, u otras

81 A saber: 1. Cumplir las obligaciones derivadas del uso de la firma electrónica.

2. Actuar con diligencia y establecer los medios razonables para evitar la utilización no autorizada de los datos de creación de la firma.

3. Cuando se emplee un certificado en relación con una firma electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el certificado, con su vigencia, o que hayan sido consignadas en el mismo, son exactas, siendo responsable de las consecuencias jurídicas de no cumplir oportunamente sus obligaciones.

4. Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el destinatario conociere de la inseguridad de la firma electrónica o no hubiere actuado con la debida diligencia.

82 Es importante señalar en este sentido que el artículo precisa que la expedición de certificados no conlleva por sí misma la fe pública.

83 El artículo 101 establece las actividades que dichos PSC deberán recoger en su objeto social.

84 Nótese que esta obligación de identificación del firmante es, en la práctica, una de las más relevantes en la prestación de servicios de certificación, incluso aun cuando se pueda delegar. Así señala Martínez Nadal: "Se señala así la función básica de los certificados, que es, efectivamente, vincular un elemento de verificación de firma (una clave pública, en el caso de la criptografía asimétrica) a una persona determinada. Por ello, es esencial la confirmación y verificación de la identidad del titular de tal elemento, a la que se refiere, como hemos visto, el borrador de directiva. Y es esencial que el proveedor de servicios de certificación asuma responsabilidad por ello. En la práctica se utilizan distintos sistemas de verificación (presencia física, envío de documentos acreditativos, sumi-

como la de puesta a disposición de los dispositivos de generación de los datos de creación y verificación de firmas, mantener el registro de certificados, establecer una declaración de prácticas de certificación, y diversas medidas de seguridad.

Hay que resaltar el artículo 106 puesto que, en conjunción con el transitorio cuarto, representa la habilitación al Banco de México para ser la autoridad registradora central en la prestación de servicios de certificación en el ámbito financiero. Es decir, se determina así que en el ámbito financiero las entidades sujetas a la competencia del Banco de México tendrán que seguir las normas específicas en prestación de servicios de certificación. En este sentido, nos remitimos al apartado de sucinto análisis de la firma electrónica en dicho ámbito que se hará posteriormente.

La responsabilidad del destinatario y de la parte que confía, además, de lo que se pueda establecer *a sensu contrario* en el contrato previsto en el artículo 103, está recogida en el artículo 107 del Decreto.

Los certificados tienen que contener una serie de aspectos para su validez, detallados en el artículo 108, como el código de identificación único, periodo de vigencia, fecha y hora de emisión, suspensión y renovación, responsabilidades asumidas por el PSC, etcétera, dejando de surtir efectos, según el artículo 109, en caso de expiración de su vigencia, revocación por el PSC, pérdida o inutilización por daño del dispositivo, o resolución judicial o de autoridad competente, entre otros. En caso de que un PSC sea suspendido, inhabilitado o cancelado, el registro y los certificados expedidos pasarán para su administración a otro PSC señalado por la Secretaría (artículo 113).

Las sanciones se impondrán conforme a la Ley Federal de Procedimiento Administrativo, sin perjuicio de las responsabilidades civiles o penales, en su caso, y las autoridades competentes podrán hacer uso de todas las medidas legales necesarias, incluyendo la solicitud de adopción de medidas cautelares (artículos 111 y 112).

nistro de información *on-line*), de entre los que el único que ofrece seguridad (y no absoluta, pues aun así podrán darse supuestos de suplantación de personalidad no detectados y ni siquiera detectables por un proveedor diligente) es el de la presencia física". Véase Martínez Nadal, A., "Aproximación al borrador de propuesta de directiva para un marco común en materia de firma electrónica y proveedores de servicios relacionados", *Actualidad Informática Aranzadi,* Navarra, núm. 29, 1998, pp. 1 y ss.

Finalmente, el artículo 114, único que compone el capítulo IV, se destina al reconocimiento internacional de certificados y firmas electrónicas extranjeros, estableciendo, como regla general, que la producción de efectos jurídicos de los mismos no tendrá en cuenta el lugar de expedición ni el lugar de establecimiento del PSC que lo emita o del firmante, sino que tendrá los mismos efectos jurídicos que uno expedido en la república mexicana si presenta un grado de fiabilidad equivalente a los contemplados en la normativa, y, de idéntica forma, toda firma electrónica creada o utilizada fuera de la república mexicana tendrá los mismos efectos jurídicos que una nacional si presenta un grado de fiabilidad equivalente. Para hallar esta equivalencia se considerarán las normas internacionales reconocidas por México y cualquier otro medio de convicción pertinente.

Por último, como referencia clara a la autonomía de la voluntad, si las partes acuerdan la utilización de unas firmas y certificados electrónicos, se reconoce este acuerdo como suficiente a efectos del reconocimiento transfronterizo, a no ser que no sea válido o eficaz conforme a derecho.

Como ya habíamos mencionado, al Decreto del 29 de agosto de 2003 le siguió un reglamento, publicado en el *Diario Oficial de la Federación* el 19 de julio de 2004, que entró en vigor el 20 de julio del citado año. Este reglamento se destina a detallar los requisitos en cuanto a los elementos humanos, materiales, económicos y tecnológicos que los prestadores de servicios de certificación que se sujeten al ámbito de la Secretaría de Economía, como autoridad certificadora y registradora, deben cumplir para conseguir la acreditación.

El reglamento, en primer lugar, se remite con carácter general a las reglas expuestas en el Código de Comercio, puntualizando algunos aspectos concretos, como que la Secretaría tendrá que emitir una relación de los PSC acreditados o suspendidos, así como un padrón de los profesionistas en materia jurídica e informática.

El trámite de acreditación comienza con la solicitud de la misma, teniendo ésta que contener, en el caso de los notarios, copia de su habilitación para ejercer, en el caso de las personas morales, copia de su acta constitutiva, y, en el caso de las instituciones públicas, copia del instrumento jurídico de su creación. En cuanto al fondo, deberá comprobarse que se cuenta con los elementos humanos (un profesionista jurídico, otro informático y cinco auxiliares de apoyo informático), materiales (espacio

físico, controles de seguridad, medidas de protección y políticas), económicos (capital suficiente en función de la inversión y seguro de responsabilidad), y tecnológicos (infraestructura informática, equipos y software, plan de seguridad, estructura de certificados y listas de revocación, procedimientos informativos, etcétera). Además, deberá contarse con una fianza y someterse a la auditoría de la Secretaría en cualquier momento, entre otras cosas.

Además, el panorama normativo en este ámbito se completa con las Reglas Generales de la Secretaría, emitidas el 4 de agosto de 2004, pero publicadas el 10 de agosto en el *Diario Oficial de la Federación*, con más de cinco meses de retraso frente a lo previsto en el transitorio segundo del decreto del 29 de agosto de 2003 al respecto. Estas reglas detallan aún más los elementos requeridos por el reglamento, desglosando a lo largo de su articulado los requisitos exigidos en cuanto a elementos humanos, materiales, económicos y tecnológicos. Sin adentrarnos en su detalle, podemos resaltar el sistema de sello temporal previsto, bien por el prestador de servicios o por un tercero (apartado 2.4.3.4 y 7 de las reglas, en conjunción con el artículo 18 del reglamento), la fianza exigida para la acreditación, o la emisión de certificados en territorio nacional y la posibilidad de resguardar la copia en el extranjero.

A continuación, y en relación con otros ordenamientos jurídicos que regulan la firma electrónica, pasamos a analizar muy brevemente el régimen establecido para las instituciones financieras y en el Código Fiscal.

4. *Ámbito financiero*

Como ya habíamos señalado, en virtud del artículo 106 y del cuarto transitorio del reformado Código de Comercio, el Banco de México se convierte, en el ámbito de su competencia, en la autoridad que regule y coordine a la autoridad registradora central, registradora y certificadora, para las instituciones financieras y las empresas que les prestan servicios auxiliares o complementarios relacionados con transferencias de fondos o valores, que presten servicios de certificación.

En este aspecto, hay que atender a lo desarrollado por la circular 6/2005, del 15 de marzo, sobre la denominada infraestructura extendida de seguridad (conocida como IES, siendo una infraestructura de clave pública en la que la autoridad registradora central es Banco de México),

que sustituye a la anterior circular 19/2002 y sus modificaciones (entre ellas, la circular 19/2002 bis). El Banco de México, con fundamento en los artículos 3o. y 24 de su Ley, implementa los requisitos mínimos técnicos e informáticos que deben cumplir las instituciones financieras y demás empresas mencionadas que deseen actuar como autoridad registradora o certificadora dentro de esta infraestructura.

En la IES, por consiguiente, se establecen las obligaciones que deben cumplir las partes intervinientes, tanto quienes presten servicios de certificación como los titulares de los certificados emitidos en este entorno. De este modo, se enumeran las obligaciones de la agencia certificadora (como corroborar la identidad de los solicitantes, proporcionar el *software* que genera los datos de creación y verificación de firma electrónica, poner en conocimiento del solicitante sus derechos y obligaciones, solicitar a una agencia registradora el registro de los certificados digitales emitidos, conservación de documentos, etcétera); de la agencia registradora (mantener y administrar en línea un registro público de certificados digitales, permitir la realización de consultas en líneas, impedir la realización de búsquedas sistemáticas, respaldar información); y de los titulares (entre sus derechos: información, recibir el *software*, poder revocar en línea o verificar el estado de su certificado, y entre sus obligaciones, hacer declaraciones veraces, avisar de cualquier modificación custodiar adecuadamente sus datos de creación de firma y la frase de seguridad vinculada, etcétera).

Desde el punto de vista procedimental, quien desee prestar servicios de certificación debe preparar un documento que contenga las políticas de la entidad al respecto, que se denomina Declaración de Prácticas de Certificación, donde se detalle todos los requisitos, aspectos, y elementos con que se cuente para cumplimentar las exigencias. Además, una vez presentado este documento ante el Banco de México, se someterá a la entidad en cuestión a un procedimiento de pruebas que verifique el cumplimiento en la práctica de lo declarado.

5. *Ámbito fiscal*

El artículo 17 del Código Fiscal de la Federación y la fracción XXII del artículo segundo de las Disposiciones Transitorias de dicho Código, publicadas en el *Diario Oficial de la Federación* mediante decreto del 5 de enero de 2004, establecen que corresponde a el Servicio de Adminis-

tración Tributaria emitir los certificados digitales a las personas físicas y morales y lo relativo a los sellos digitales, para la presentación digital con firma electrónica avanzada de los documentos a las autoridades fiscales.

Así, el artículo 17D del Código Fiscal de la Federación afirma: "Cuando las disposiciones fiscales obliguen a presentar documentos, estos deberán ser digitales y contener una firma electrónica avanzada del autor, salvo los casos que establezcan una regla diferente".

Y el artículo continúa disponiendo que para personas morales y sellos digitales se tendrá que contar con un certificado emitido por el SAT, mientras que las personas físicas tendrán que acudir a un PSC autorizado por el Banco de México, es decir, se remite así a los prestadores de servicios de certificación que puedan operar conforme a la IES. De este modo, las entidades financieras y demás empresas que les presten servicios, como hemos mencionado, tienen participación en el mercado tributario de prestación de servicios de certificación. Y así el SAT ha establecido un convenio para ser autoridad de certificación y autoridad de registro para expedir certificados digitales, aprovechando la infraestructura de clave pública proporcionada por el Banco de México.

6. *La conservación de los documentos*[85]

En otro orden de cosas, a pesar de su indiscutible relación y dependencia, haremos una última referencia a la cuestión de la conservación de los documentos electrónicos, que resulta absolutamente crucial. [86]

[85] Para un análisis en profundidad del problema de la conservación de los documentos digitales, véase varios autores, *La prueba por medios audiovisuales e instrumentales de archivo en la LEC 1/2000*, Valencia, Tirant lo Blanch, 2002, pp. 56 y ss.

[86] El tema de la conservación del documento digital es esencial, y así lo hace notar Izquierdo Loyola, citando a su vez a Rothenberg: "Año de 2045. Mis nietos (que no han nacido aún) están explorando el desván de mi casa (que no he comprado todavía). Descubren una carta fechada en 1995 y un disco CD-ROM. La carta dice que el disco contiene un documento en el que se da la clave para heredar mi fortuna (que no he ganado aún). Mis nietos sienten viva curiosidad, pero jamás han visto un disco compacto, salvo en viejas películas. Aun cuando localizaran un lector de discos adecuado ¿cómo lograrían hacer funcionar los programas necesarios para la interpretación del contenido? ¿Cómo podrían leer mi anticuado documento digital". La historieta anterior extraída del sugestivo artículo de Jeff Rothenberg "¿Son perdurables los documentos digitales?", *apud* Izquierdo Loyola, V. M., "Directrices de seguridad, normalización y conservación de documentos

No sólo se trata de la conservación del documento en términos de su accesibilidad para su ulterior consulta, sino, en sentido amplio, de que se entienda que esta conservación se puede cumplir satisfactoriamente si se realiza electrónicamente, eliminando los obstáculos que impidan el asentamiento del comercio electrónico. En este sentido, por ejemplo, es de particular interés la idea de conservar toda la información, no sólo el mensaje, sino relativa a la determinación del origen y el destino del mensaje, así como la fecha y hora de su recepción o envío. Así, al exigir que la información de la transmisión relacionada con el mensaje se conserve, puede parece que se crea una norma más exigente que sus correlativas respecto a las comunicaciones en papel, pero no debe en ningún caso interpretarse como si se impusiera una obligación de conservar la información relativa a la transmisión adicional a la contenida en el mensaje de datos cuando se generó, almacenó o transmitió, o la información en un mensaje de datos separado, como un acuse de recibo. Además, hay que tener en cuenta que aunque alguna información sobre la transmisión es importante y debe conservarse, otra puede no guardarse sin que ello altere la integridad del mensaje de datos.

Respecto a lo anterior, la Norma Oficial Mexicana NOM-151-SCFI-2002, relativa a los requisitos que deben observarse para la conservación de mensajes de datos, tiene como objeto establecer los requisitos que deben observarse para la conservación del contenido de mensajes de datos que consignen contratos, convenios o compromisos, obligatoria para los comerciantes que deban conservar los mensajes en que se consignen los citados documentos, así como para todas aquellas personas con quienes los comerciantes otorguen o pacten dichos contratos, convenios o compromisos. Sin embargo, la resolución de inicio de vigencia de la NOM 151 no se publicó en el *DOF* hasta el 19 de diciembre de 2005, contándose 60 días naturales para su observancia.

En definitiva, la NOM es de observancia general para los comerciantes que deban conservar los mensajes en que se consignen los citados documentos, así como para todas aquellas personas con quienes los comerciantes otorguen o pacten dichos contratos, convenios o compromisos.

electrónicos en la administración", *Encuentros sobre informática y derecho*, Davara Rodríguez, Miguel Ángel (coord.), *cit.*, nota 30, pp. 191 y ss. Para el artículo de Rothenberg, véase "*Ensuring the Longevity of Digital Information"*, disponible en *http://www.clir. org/pubs/archives/ensuring.pdf*, consulta: 20 de septiembre de 2004.

En la conservación de los mensajes de datos, se requiere de la utilización de tecnología PKI y de la existencia y participación de un PSC. Además, la migración deberá ser cotejada por un tercero legalmente autorizado, quien constatará que dicha migración se realice íntegra e inalterablemente tal y como se generó por primera vez en su forma definitiva.

En nuestra opinión, además de la necesaria observancia de esta ley, sancionada de manera indirecta en la misma y con otras consecuencias en el ámbito procesal y fiscal, representa una oportunidad de adecuación y adaptación de los documentos de obligatoria conservación, ya que permite que éstos sean considerados originales si se cumplen una serie de requisitos en la migración a soporte electrónico.

IV. Sucintas conclusiones

Desde nuestro modesto punto de vista, las consecuencias jurídicas derivadas de la utilización de las nuevas tecnologías pueden ser, en su mayoría, interpretadas conforme a las estructuras jurídicas y exegéticas disponibles y asentadas ya tradicionalmente.

Ahora bien, tampoco sería del todo correcto entonces argumentar, en nuestra opinión, que nada ha cambiado, o que poca influencia tienen las mencionadas herramientas. La realidad y los grandes cambios sociales y culturales originados parecen apuntar a justamente lo contrario.

Sin embargo, a nuestro juicio, lo que ocurre es que la potencialidad de la herramienta utilizada para la concreción o perfeccionamiento de las relaciones es tan fuerte que impregna todas las esferas y ámbitos de la sociedad, haciendo necesario que este elemento, que ya no es tan accidental, no por su necesidad, sino por la consecuencia de su utilización, califique la relación en su conjunto, entrando inmediatamente a formar parte de una serie de transacciones que se tienen que regir por unas reglas determinadas debido a su concreción electrónica. Así, desde nuestro punto de vista, el medio se convierte en esencial a la hora de la aplicación de las normas, creando un grupo de relaciones en las que la forma constituye un elemento determinante. Los conceptos de distancia, de tiempo, de frontera, de presencia física de las partes, deben ser reinterpretados y ajustados a los nuevos medios de contratación, para que se ajusten a las nuevas características impuestas por estos medios de contratación, cuando menos en lo referente a las consecuencias jurídicas

derivadas de la categorización como uno u otro tipo de contratación mencionados.

Es, por lo tanto, necesario adaptar no sólo nuestros ordenamientos jurídicos, sino nuestra mentalidad, en esta especie de vidas paralelas que tenemos, en el entorno físico y el electrónico, donde cada vez más de las actividades cotidianas se realizan sin dificultad, desplazando a sus equiparables físicas.

No obstante, en nuestro parecer, no se debería en ningún caso permitir paralizar la utilización de técnica alguna con la sola excusa de una inseguridad, omnipresente en todos los ámbitos por otro lado, si la citada inseguridad está razonablemente cubierta dentro del estado actual del arte en cada momento. Por ello, en conclusión, debería promoverse el fomento del uso de estas técnicas eliminando reticencias jurídicas hacia una herramienta que garantiza en el entorno electrónico, cuando menos, la misma seguridad jurídica que su homónima física. En este sentido, creemos que es obligación de los profesionales jurídicos impulsar el desarrollo y confianza de la sociedad en general, eliminando obstáculos y facilitando su implantación.

Estos cambios van a requerir de una rapidez y capacidad de adaptación muy superior a la que estábamos acostumbrados, pero, al mismo tiempo, surge la oportunidad para el derecho, y en consecuencia para los profesionales de los mismos, de recuperar la cercanía que en sus orígenes tuvo con los regulados, gracias precisamente a este mayor dinamismo y concreción.

El derecho tiene la ocasión de dejar de ser un ente extraño y sólo conocido y entendido, en el mejor de los casos, por los expertos, y, en ocasiones, muy alejado de la realidad y sin soluciones adecuadas por razones de obsolescencia, para convertirse en verdadero motor de la sociedad, para recoger las inquietudes y las necesidades precisas en el momento necesario, para que sea formado a través de la participación de los que van a ser regulados a su vez, y para que su adaptación y su flexibilidad sean lo que en origen pretendían ser.

Si una vez el derecho romano sirvió para regular gran parte del mundo conocido, podemos ahora llegar a un acuerdo sobre las normas que debe regir a nivel internacional de manera común, creando, además, una comunidad intelectual internacional, de expertos que apliquen e interpreten las normas necesarias para resolver los conflictos surgidos en este nuevo

entorno, procurando una especie de derecho mínimo común, uniforme, aplicable a todos los ordenamientos jurídicos, salvaguardando las peculiaridades regionales.

Las herramientas tecnológicas aplicadas al derecho, y, viceversa, el derecho que surge como consecuencia de la utilización de las mismas, son una posibilidad real para acercar el derecho a los ciudadanos y, también, para que los ciudadanos puedan intervenir más directamente en la sociedad.

En una época en la que la globalización podría parecer que conduce a la deshumanización e irrelevancia del individuo, en la práctica, los cauces de participación y decisión, directa y efectiva, son un medio para construir una sociedad más igualitaria, más ponderada y más equilibrada.