LAS PREGUNTAS MÁS COMUNES EN LA CONTRATACIÓN ELECTRÓNICA

El tema de contratación electrónica, incluso reducido al ámbito meramente notarial, es un tema de grandes y profundas implicaciones. Además, en los últimos años se ha producido una explosión de textos legislativos y de ensayos doctrinales referidos al tema. Los tratamientos son dispares, las novedades se suceden rápidamente y la necesidad de ordenar y prestar coherencia a la información es cada vez más acuciante.

Este ensayo tiene el propósito de aclarar el *status quaestionis* de la contratación electrónica y la intervención notarial. Para el caso, he dividido el tratamiento del tema en preguntas específicas que tratan de seguir un orden lógico y progresivo. Así, parto del tema de las firmas digitales para arribar al documento informático en general, plantear la controversia acerca de su valor

probatorio y relacionar, por último, todo el contexto legal actual del derecho informático.

Precisada así la primera parte del trabajo, examino un tema de gran complejidad doctrinal y legislativa, a saber, el del *momento* y el *lugar* de perfección del contrato electrónico -que ya ha sido objeto de un estudio mucho más pormenorizado en otro ensayo mío-.[1] A continuación, repaso el tema de la intervención notarial examinando puntos específicos como la posibilidad de su participación, las reformas legales necesarias, el procedimiento para la expedición de certificados, los ciclos vitales de este documento e incluso los costos de la intervención fedataria. Inmediatamente después derivo el estudio al campo -algo distinto- de la protección del consumidor. Finalmente, la última parte la dedico al estudio de las autoridades certificadoras y sus posibles funciones.

PARTE UNO: FIRMAS DIGITALES

1. ¿Cuál es la diferencia entre firmas electrónicas y firmas digitales?

R. La firma electrónica es el género; las firmas digitales son una especie dentro de ese género[2] (puede haber otras, como las basadas en dispositivos biométricos, la temperatura corporal, el iris de los ojos, la impresión dactilar, los registros genéticos de las células, la geometría de las manos o del rostro, el termograma facial, la forma de la oreja, el aroma corporal, la configuración de los vasos sanguíneos, la letra manuscrita, el modo de andar, la forma de mecanografiar, los impulsos cerebrales, los

[1] "Formación de los contratos. Buscando reglas uniformes" (incluye sinopsis en inglés, alemán, italiano y francés), en: *Notarius International*, número 1-2/2004, Würzburg, pp. 99-111.

[2] Este es, por ejemplo, el sentido que tiene en los arts. 2º del Decreto que regula el uso de la firma digital y los documentos electrónicos en la administración del Estado de Chile; 3º de la Ley de Firmas y Certificados Digitales del Perú; 18-19 del Decreto 65/98 reglamentando el uso del documento electrónico y la firma digital por la administración pública de Uruguay y en el Régimen Uniforme de la CNUDMI para las Firmas Electrónicas (2001).

rasgos de articulación de la rodilla, las marcas y tatuajes y hasta la modulación y el tono de nuestra voz).

En forma muy simple, la firma electrónica puede definirse diciendo que es la que se impone en un documento electrónico con la intención de asumirlo como propio, de modo que pueda identificarse al titular de la firma en relación con un mensaje de datos.

Por su parte, la firma digital es una especie de firma electrónica que utiliza un sistema criptográfico de claves públicas y privadas relacionadas matemáticamente entre sí.

En el estado actual de la tecnología informática, las leyes sobre contratación electrónica tratan de regular específicamente las firmas digitales.

2. ¿Cuál es la diferencia entre las firmas electrónicas *simples* y las *avanzadas*?

R. Esta es una distinción que se utilizó inicialmente en Europa. Según esto, la firma electrónica avanzada reúne los siguientes requisitos:

a. Es única para el signante;
b. Permite su identificación;
c. Mantiene bajo su control el código empleado, y
d. Es inalterable.

El Decreto-Ley de Firma Electrónica español dice en su art. 3º:

> La firma electrónica avanzada... tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta según los criterios de apreciación establecidos en las normas procesales.

Por su parte, en México, las reformas al Código de Comercio de veintinueve de agosto de 2003 consignan en el art. 97 fracciones I a IV los

siguientes requisitos para que la firma electrónica se considere “avanzada” o “fiable”:

> Artículo 97. […]
> La Firma Electrónica se considerará Avanzada o Fiable si cumple por lo menos los siguientes requisitos:
> I. Los Datos de Creación de la Firma, en el contexto en que son utilizados, corresponden exclusivamente al Firmante;
> II. Los Datos de Creación de la Firma estaban, en el momento de la firma, bajo el control exclusivo del Firmante;
> III. Es posible detectar cualquier alteración de la Firma Electrónica hecha después del momento de la firma, y
> IV. 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.

La nueva Ley Electrónica del Estado de Jalisco de 2006, se refiere a la “firma electrónica certificada” en los siguientes términos:

> Art. 3.
> [...]
> VIII. Firma electrónica certificada: Los datos que en forma electrónica son vinculados o asociados a un mensaje de datos y que corresponden inequívocamente al firmante con la finalidad de asegurar la integridad y autenticidad del mismo y que ha sido certificada por un prestador de servicios de certificación debidamente autorizado ante la Secretaría.
> [...]

Estos preceptos coinciden en los requisitos de atribución, exclusividad, inalterabilidad y confiabilidad de la firma. Así pues, hasta ahora coexisten dos tipos de firmas: las simples y las avanzadas, pero solamente la segunda es equiparable jurídicamente a la manuscrita.

3. ¿Puede una persona tener dos o más firmas digitales?

R. Sí, una persona puede tener varias firmas digitales y todas pueden ser objeto de reconocimiento formal.

4. ¿Es siempre idéntica la firma digital de una persona?

R. No, la firma digital cambia siempre con cada documento signado, de manera que ella es única e irrepetible. Sin embargo, esto no es ningún obstáculo para que el receptor del mensaje de datos aplique la clave pública al documento codificado y ambas encajen perfectamente.

5. ¿La firma digital es estrictamente personal?

R. No, no lo es. Por lo menos no en la forma en que sí lo es una firma tradicional, es decir, que tenga las características caligráficas y holográficas de rigor. La razón de ello estriba en que, aun con procedimientos técnicos sumamente complejos de seguridad, el autor de una firma electrónica siempre puede delegar su uso a otra persona, tan sólo comunicando la llave privada respectiva y el *password* de su computadora personal.

Una vez que el tercero posee ambas claves, nada impide que firme electrónicamente como lo haría su titular. Detectar la alteración o suplantación es absolutamente imposible desde el punto de vista técnico, a menos que alguna de las partes confiese la situación real.

¿Cómo se define pues, la atribución o imputabilidad de un mensaje de datos? Al respecto, el art. 90 del Código de Comercio establece lo siguiente:

> Salvo pacto en contrario, se presumirá que el mensaje de datos proviene del emisor si ha sido enviado:
>
> I. Usando medios de identificación, tales como claves o contraseñas de él, o
>
> II. Por un sistema de información programado por el emisor o en su nombre para que opere automáticamente.

Es interesante consignar como en ciertos casos algunos distribuidores de servicio exigen incluso que el usuario forme una secuencia de imágenes (números, letras) para cerciorarse de que en efecto el destinatario es una persona humana y no un programa automatizado. Son los denominados *captchas* (*Completely Automated Public Turing test to tell Computers and Humans Apart*), es decir, una palabra aleatoria, intencionalmente distorsionada, que evita que un robot acceda a la red.

6. ¿Cómo se representa gráficamente una firma digital?

R. No tiene representación gráfica. Ella solamente "existe" archivada en la memoria de la computadora. Ahora bien, si alguna vez llega a imprimirse, aparecerá en forma muy similar a esta:

> jt8LAbBxfVr9DHcBe1UABB+98G+22Gh7L9iAuNbHhVmqJ2UuhX2soUSpJMLVsfZA
> tJu9sly1Ku/XsEY4h9b+MLHPgArJMu9GNcELGpiNYGEowHtGGS7rlBjedR/ZbfOGs
> Ag5Tt11NmwryA80xlzEmMPiPSdrFnZCSa/99nEiRCTZRFbPfR/kt/Wl59w7t5937VS
> Tj3ndS9Cqe3Df1w45vqJ+dZ5Hpcahe5u108vRmy2/vqVK7We2jHyKd8d e9+85DDG

Como se ve, se trata de una combinación absolutamente aleatoria de números, letras y signos. Sin duda, no se trata de una firma en el sentido tradicional del término, ya que no contiene ningún rastro físico del sujeto. La palabra inglesa *signatura* viene del latín *signatus,* participio pasado de *signare,* que literalmente significa "sello" o "marca". El Servicio de Administración Tributaria mexicano (SAT) le llama, en efecto, "sello" o "cadena".

Este sello es la denominada "firma electrónica avanzada". La *cadena original* son los datos del usuario con los cuales se generó la FEA.

Al imprimirse (lo cual en efecto sucede en los comprobantes de pago de impuestos que expide el SAT), el mensaje aparece así:

> **Cadena Original:**

||10001=MAGA570327R1A|10017=28726|20001=40012|20002=627012008037|40002=20060927|40003=11:37|40008=0E3E761C94|10502=8|10527=2006|10522=1|10504=28405|10506=321|10508=28726|10516=0|10517=28726|10520=28726|30003=00000100000700015370 9||

Sello Digital:

kJVdJXhP/hfMNcG+ofLVgNeI3DsVN1xWJSEDaZfYUnMI9o1dfKlz4++8kIGVDS97H2vEAZTw3EuK8bvCLJSa1sp82q32MHhJZIJViABHArcX1q4ALUIWb9s1MFU6yL9sVJr6/xRwwI5kVDxsKJU1TC/77swmKG1UJYJdxXpoXLw=II

7. ¿Qué es la CIEC?

La denominada CIEC es la Clave de Identificación Electrónica Confidencial del SAT. Se forma a través del Registro Federal de Contribuyentes (RFC) y una contraseña que se debe generar personalmente, combinando números y letras. Es intransferible.

La FIEL, en cambio, es un conjunto de datos que se agregan a un mensaje electrónico. Consta de dos llaves, una pública que sirve para descifrar mensajes, conocida para todo usuario electrónico, y una privada, conocida solamente por el titular de la firma (*supra*, pregunta 6).

PARTE DOS: EL DOCUMENTO INFORMÁTICO

8. ¿Pueden considerarse los datos almacenados o la información que aparece en pantalla como “documentos”?

R. Las palabras “documento” e “instrumento” vienen de las palabras latinas *docere* e *instruire* que significan enseñar o mostrar. Un *documento electrónico* es aquel que ha sido elaborado en forma electrónica. Ahora bien, la palabra electrónico hace referencia a partículas de electricidad como uno de los elementos constitutivos del átomo y por tanto comprende a todo aparato que funcione a base de electrones. En este sentido se

comprenden invenciones como el teléfono, el celular, la radio, el telégrafo, la televisión, el fax, el télex, los modernos medios de información como la computadora y, en general, la transmisión lejana de datos (teleinformática).

El documento puede ser identificado, sin duda, con un gráfico o con un escrito, sea cual fuere el soporte que lo contenga. La cuestión que debe resolverse ahora es si puede conceptuarse además como documento un elemento de información que no posea materialidad o expresión física alguna. Según lo dispuesto en el art. 210-A CFPC, este requisito queda satisfecho en original si la información se ha mantenido íntegra, inalterada y accesible.[3]

A su vez, los arts. 1205 y 1298-A del Código de Comercio reconocen como prueba la información electrónica y los mensajes de datos. Su fuerza probatoria es discrecional, atendiendo primordialmente a la fiabilidad del método en que haya sido generada, archivada, comunicada o conservada dicha información (art. 1298-A CCo). Para valorar la fuerza probatoria debe atenderse a tres circunstancias: fiabilidad del método, atribución personal y accesibilidad para su consulta posterior.

El documento electrónico puede exigir algunas veces la ratificación en contenido y firma si no reúne estos requisitos legales de confiabilidad, atribución y accesibilidad.[4]

---

[3] El Código Procesal de Perú resuelve acertadamente la cuestión en sus artículos 233 y 234 que dicen: "Artículo 233.- Documento.- Es todo escrito u objeto que sirve para acreditar un hecho. Artículo 234.- Clases de documentos.- Son documentos los escritos públicos o privados, los impresos, fotocopias, facsímil o fax, planos, cuadros, dibujos, fotografía, radiografías, cintas cinematográficas, microformas tanto en la modalidad de microfilm como en la modalidad de soportes informáticos, y otras reproducciones de audio o video, la telemática en general y demás objetos que recojan, contengan o representen algún hecho, o una actividad humana o de resultado".

[4] El mismo proyecto brasileño 1589/99 distingue las certificaciones electrónicas *privadas* de las certificaciones electrónicas *públicas* en los arts. 24-25:

"TÍTULO IV. CERTIFICADOS ELETRÔNICOS.

Capítulo I. Dos certificados eletrônicos privados.

Art. 24. Os serviços prestados por entidades certificadoras privadas são de caráter comercial, essencialmente privados e não se confundem em seus efeitos com a atividade de certificação eletrônica por tabelião, prevista no Capítulo II deste Título.

Capítulo II. Dos certificados eletrônicos públicos.

Seção I. Das certificaçôes eletrônicas pelo tabelião.

Art. 25. O tabelião certificará a autenticidade de chaves públicas entregues pessoalmente pelo seu titular, devidamente identificado; o pedido de certificação será efetuado pelo requerente em ficha própria,

9. ¿Puede realmente distinguirse entre el original y las copias de documentos electrónicos?

R. La respuesta es definitiva: no, a diferencia de lo que sucede con los documentos en soporte papel. Antes, en el papel se podía perfectamente distinguir entre el original y las copias, hasta que hicieron su aparición las excelentes fotocopiadoras "Xerox" donde, a menos que hubiese un detalle de color en el original, no podía diferenciarse el duplicado. Lo mismo sucede con las actuales fotocopiadoras con dispositivo láser.

10. ¿Cuál es el documento que debe considerarse como original?

R. En este punto, puede haber varias respuestas:

a. Considerar como original el documento conservado en la memoria de la persona que expide el mensaje de datos.
b. Considerar como original el documento que ha efectuado todo el viaje y que ha sido recibido efectivamente por el destinatario.
c. Considerar como original el documento que el destinatario almacena en la memoria de su computadora.
d. Considerar como original el primer impreso en soporte papel que se haga, considerando tanto una como otra parte.
e. Considerar como original el documento interceptado, conservado y certificado por la autoridad certificadora –sea ésta cual fuere–.

Una novedad importante es la que incorpora el art. 11 de la Ley 25506 de Argentina respecto a lo que se denomina como "originales de primera generación en cualquier soporte":

Un proyecto en Brasil ha intentado la distinción reputando *original* el documento electrónico sin materialidad física signado por el emisor, y *copia* el documento electrónico resultante de la digitalización del

---

em papel, por ele subscrita, onde constarão dados suficientes para identificação da chave pública, a ser arquivada em cartório."

documento físico, así como también la materialización física del documento electrónico original.[5]

En Ecuador, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (de 2002) propone considerar como *información original* aquella que conserve la integridad de información a partir del momento en que se generó por primera vez como mensajes de datos.[6] También se propone que se reconozca como documento original el creado primero en papel y luego en forma electrónica mediante escaneo, fax o sistema de *e-mail*.

Como se ve, el problema es sumamente complejo porque ya se vio que no hay forma de distinguir entre el original y los duplicados de los documentos electrónicos.

11. ¿Puede facturarse ya en forma electrónica?

R. Sí, de acuerdo con lo previsto en los arts. 89 al 114 y transitorios, primero al cuarto, del Código de Comercio; 28, 29 y 29-A del Código Fiscal de la Federación, y las resoluciones misceláneas fiscales de 2004 y 2006 (arts. 2.22.6 al 2.22.12 y Anexo 20).

Ejemplo de esta nueva facturación electrónica pueden encontrarse en empresas como IAVE, SAT, PEMEX, TELMEX y CFE, que permiten la consulta, descarga e impresión de facturas electrónicas con validez fiscal. Se espera que pronto se sumen a este esfuerzo otros organismos como el

---

[5] Esta es la versión en portugués:
"Título III. DOCUMENTOS ELETRÔNICOS.
Capítulo I. Da eficacia jurídica dos documentos eletrônicos.
Art. 14. Considera-se original o documento eletrônico assinado pelo seu autor mediante sistema criptográfico de chave pública.
§ 1º. Considera-se cópia o documento eletrônico resultante da digitalização de documento físico, bem como a materialização física de documento eletrônico original.
§ 2º. Presumem-se conformes ao original, as cópias mencionadas no parágrafo anterior, quando autenticadas pelo escrivão na forma dos arts. 33 e 34 desta lei.
§ 3º. A cópia não autenticada terá o mesmo valor probante do original, se a parte contra quem foi produzida não negar sua conformidade". (Art. 14 del Proyecto de ley 1589/99.)

[6] Ley de Comercio Electrónico, firmas y mensajes de datos. Ley no. 67 R. O. suplemento 557 de 17 de abril de 2002 (Art. 7).

Tribunal Electoral del Poder Judicial de la Federación, el IMSS y el Infonavit.

12. ¿En que consisten las certificaciones electrónicas *recíprocas* o *cruzadas* (*international cross certification*)?

R. Es el reconocimiento legal de los certificados electrónicos emitidos por entidades certificadoras extranjeras. Este reconocimiento (o interoperabilidad) depende del cumplimiento de los requisitos exigidos en el país de destino y de la homologación respectiva por una entidad certificadora nacional. Por tanto, es indispensable la existencia de una infraestructura de clave pública (ICP) a nivel internacional y la armonización de las políticas de certificación y de las declaraciones de las prácticas de certificación.

En algunos casos ya no se requiere más esta certificación (por ejemplo, en la Autoridad Reguladora de Telecomunicaciones y Correo de Bonn, la cual lleva su propio registro en la página *web* http: www.regtp.de. El gobierno local asume la responsabilidad).

13. ¿Qué pasará con las apostillas en el caso de documentos extranjeros?

R. La Convención de La Haya de 1961, como es de imaginar, no prevé nada al respecto. Antes bien, los arts. 1 y 4 se refieren a documentos públicos y prevén la colocación de dicha apostilla “sobre el propio documento o sobre una prolongación del mismo”.

Algunos autores imaginan un procedimiento de legalización mediante la denominada “apostilla electrónica”. Al respecto, las leyes 15.16 y 118.12 en el estado de Florida ya prevén tal hipótesis referida a la apostilla que certifica la autoridad del *civil-law notary.*

Recientemente se puso en marcha el Programa piloto de Apostillas Electrónicas (e-APP), en virtud del cual se da seguimiento a resoluciones puntuales de la Conferencia de La Haya de Derecho Internacional Privado.

Bélgica y Colombia han adoptado ya un registro electrónico de características compatibles.

PARTE TRES: VALOR PROBATORIO DEL DOCUMENTO INFORMÁTICO

14. ¿Cuál es, a la fecha, la actitud de la jurisprudencia ante la contratación electrónica en general?

R. Los tribunales han dictado muchas sentencias, pero la mayoría se refieren en general a las transmisiones por facsímil y al valor de copias fotostáticas. Otras muchas tienen que ver con la obligación de las instituciones de crédito para almacenar y conservar datos, la acreditación del pago, el cumplimiento de deberes fiscales, los acuses de recibo, la transferencia de fondos, etc., todo en forma electrónica.

15. ¿Cuál es el valor probatorio de los documentos informáticos?

R. Para valorar su fuerza probatoria, deben atenderse tres circunstancias: la fiabilidad del método empleado, su atribución personal y su accesibilidad para consulta (*cfr*. art. 210-A CFPC en relación con los arts. 1205 y 1298-A del CCo, que reconocen como prueba la información electrónica y los mensajes de datos).

Así, se ha considerado que su fuerza probatoria es sólo discrecional, atendiendo primordialmente a la fiabilidad del método en que haya sido generada, archivada, comunicada o conservada dicha información (art. 1298-A CCo) y se ha agrupado a los documentos informáticos bajo el rubro de "elementos aportados por la ciencia" (art. 188 del Código Federal de Procedimientos Civiles), con un valor meramente indiciario -y que, por tanto, debe adminicularse y robustecerse con otros elementos probatorios-.

La Corte, en efecto, ha dicho que la información en la red constituye un "hecho notorio" (art. 88 del Código Federal de Procedimientos Civiles) y

los tribunales colegiados han decidido que la eventual referencia a ella es válida “aun cuando no se tenga a la vista de manera física el testimonio autorizado”.

16. ¿Vale un documento impreso por la computadora como si fuera un original duplicado?

R. De acuerdo con lo dispuesto en el art. 210-A y B, CFPC, ya se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.

Vale como original solamente si la información:

a. Se ha mantenido íntegra e inalterada, y
b. Si puede ser accesible para su consulta ulterior.

17. ¿Debe el oferente exigir ratificación en contenido y firma?

R. Por regla general no, si es que reúne precisamente los requisitos de atribución, accesibilidad y confiabilidad. Por tanto, en sentido contrario, habrá casos especiales en que sí resulte necesario pedir la ratificación.

18. ¿Qué sucede si se desconoce su validez?

R. La carga de la prueba corresponde a quien desea hacer valer el documento electrónico, según lo dispone, por ejemplo, el artículo 6º de la Ley 25506 argentina.

19. Este documento generado en forma electrónica, ¿trae aparejada ejecución?

R. No, la ley no reconoce hasta ahora efectos ejecutivos a este tipo de documentos (como sí lo hace, en cambio, para las sentencias ejecutoriadas, para los documentos públicos que hacen prueba plena conforme al Código Federal de Procedimientos Civiles, para los documentos privados reconocidos ante notario o ante la autoridad judicial, para los contratos o las pólizas y los estados de cuenta, para los negocios

sobre derechos patrimoniales inscritos en el Registro de Derecho de Autor y para todos los demás documentos que traigan aparejada ejecución conforme a la ley).

PARTE CUATRO: CONTEXTO LEGAL DEL DERECHO INFORMÁTICO

20. ¿Cuáles son, hasta ahora, los *principios doctrinales* más importantes en el derecho informático?

R. A pesar de la proliferación que se ha producido en los últimos años en la legislación sobre el empleo de medios de comunicación telemáticos, de comercio electrónico, firmas digitales y entidades de certificación, es posible advertir, sin embargo, que casi todas las leyes se ajustan en mayor o menor medida a un reducido número de principios doctrinales que matizan y uniforman su aplicación.

Estos principios son los siguientes:

- Autenticidad, conservación, confidencialidad e integridad del mensaje de datos;
- Autonomía de la voluntad;
- Libertad de prestación de servicios;
- Libre competencia;
- Neutralidad tecnológica;
- Reciprocidad o compatibilidad internacional;
- Principio de equivalencia funcional, y
- Buena fe -inherente a todo el derecho internacional-.

Como es de esperar, el ajuste de la legislación a estos pocos principios de derecho informático constituye un valioso auxiliar en la interpretación de sus preceptos, de modo que la heterogénea normativa pueda guardar cierta armonía con los principios señalados.

21. ¿Qué significa el principio de neutralidad tecnológica?

R. Este principio supone que las políticas gubernamentales deben adoptar decisiones técnicas sin compromiso alguno con tecnologías determinadas. En la práctica, aunque la legislación proclame dicho principio, las decisiones gubernamentales han coincidido mayoritariamente en la utilización de una infraestructura de clave pública (ICP), de modo que las decisiones políticas han terminado por especificar una cierta tecnología y, por tanto, han transitado de un criterio de "neutralidad" a un cierto criterio "prescriptivo".

22. ¿Cuáles son las leyes federales mexicanas que a la fecha han incorporado preceptos sobre aspectos electrónicos específicos?

R.
- Código de Comercio (arts. 20 *bis*, 25, 26, 30 *bis*, 89-94, 100 y 1298-A).
- Código Federal de Procedimientos Civiles (art. 210-A).
- Código Civil Federal (arts. 1803, 1834 bis).
- Norma Oficial Mexicana NOM-035-SCFI-1994.
- Lineamientos para la operación del Registro Público de Comercio, 2000.
- Reglamento del Registro Público de Comercio, 2003.
- Convenio de Coordinación para la operación del Registro Público de Comercio, 2007.
- Ley Federal de Protección al Consumidor (arts. 1º fr. VIII, 24 fr. IX *bis* y 76 *bis*).
- Ley Aduanera (art. 36 y 38).
- Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (arts. 26, 27, 56, 65 y 67).
- Ley de Instituciones de Crédito (art. 52).
- Ley de Obras Públicas y Servicios relacionados con las mismas (arts. 27, 28, 31, 33, 47, 48, 83 y 85).
- Ley del Mercado de Valores (art. 91, V).

- Ley Federal de Derechos de Autor (arts. 101-114, 123).
- Programa Nacional de Normalización.
- Reglamento Interior del Registro Agrario Nacional (art. 106).
- Reglas Generales a que deberán sujetarse los Prestadores de Servicios de Certificación.
- Reglas y Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación.

En todos estos casos se conceden algunos efectos legales a las firmas electrónicas, aunque limitados exclusivamente a ciertos funcionarios, instituciones o actos (notarios, corredores, registradores de comercio, instituciones de crédito y sus usuarios, contratos de intermediación bursátil, funcionarios aduanales, importadores y exportadores, registradores agrarios).

Como se ve, el marco legal en México es muy complejo y se encuentra disperso en una gran pluralidad de leyes. Así, en pocos años se ha transitado de la total ausencia de regulación legal a una gran multiplicidad de disposiciones.

23. ¿Cuáles son los códigos civiles en la República Mexicana que ya disponen de normas sobre contratación electrónica?

R. Código Civil de Puebla, 1995 (art. 1460)
Código Civil de Jalisco, 1995 (arts. 1261, 1273, 1279 y 1308).
Código Civil de Tabasco, 1997 (art. 1928)
Código Civil de Coahuila, 1999 (arts. 1920 y 1926)
Código Civil del Estado de México, 2004 (art. 7.51)

En general, estas normas previenen la posibilidad de la contratación electrónica, suprimen el precontrato anteriormente necesario y no exigen más la imposición de signos convencionales o marcas secretas en los originales, excepto en el caso del Estado de México.

A la fecha, cinco entidades en la República Mexicana disponen ya de leyes electrónicas. Son las siguientes:

1. Ley sobre el uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato, 9 de julio de 2004.
2. Ley sobre el uso de Firma Electrónica Avanzada para el Estado de Sonora, 6 de julio de 2006.
3. Normatividad en materia de Firma Electrónica Avanzada para el Estado de Chiapas, 13 de septiembre de 2006.
4. Ley de Firma Electrónica Certificada para el Estado de Jalisco y sus municipios, 14 de septiembre de 2006.
5. Ley sobre el uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo, 30 de marzo de 2008.

Así, puede advertirse que a nivel nacional hemos elegido el denominado “plan B”, es decir, la adición de leyes ya existentes; sin embargo, a nivel local puede verse que por lo menos estas cinco entidades han elegido el denominado “plan A”, es decir, la expedición de leyes específicas sobre el tema.

24. ¿Cuáles son las limitaciones legales de la tecnología electrónica?

R. El ámbito de aplicación se acota cada vez más, pasada la euforia de los años iniciales. La gran mayoría de las leyes electrónicas consignan artículos que expresamente excluyen cierto tipo de actos o negocios. Los más importantes son los siguientes: los que requieren la intervención de autoridades judiciales, administrativas o notariales, actos familiares o sucesorios, derechos de propiedad intelectual, protección del consumidor, actos personalísimos, contratos inmobiliarios, etc.

PARTE CINCO: PERFECCIÓN DEL CONTRATO ELECTRÓNICO

25. ¿La contratación electrónica se considera celebrada entre presentes o entre no presentes?

R. Según lo dispuesto en el art. 1805 CCF, este tipo de contratación se equipara a la realizada entre personas presentes (al igual que la telefónica, ya que se considera que la expresión de la oferta y su aceptación se realizan en forma inmediata o sucesiva).

Por ejemplo, el Código Civil de Jalisco establece en su art. 1273 lo siguiente:

> Si la oferta se hace 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 cualquier medio de telecomunicación simultánea, electrónico, óptico o de cualquier otra tecnología que permita la expresión de la oferta y la aceptación en forma inmediata.

Ahora bien, es necesario aclarar que en la práctica hay dos tipos de comunicación electrónica. Se llama *síncrona* a la comunicación efectiva en tiempo real: es el caso de las pláticas por *chat* y de las conferencias en audio, video o ambos canales (ya se ve que no se requiere que ambas partes estén en un mismo lugar). Se llama *asíncrona*, en cambio, al tipo de comunicación donde no coinciden ni el lugar ni el tiempo: es el caso de los foros de debate, el correo electrónico y la red.

Así, en la práctica sucede que los eventuales contratantes, de frente a su computadora, pueden, desde luego, no encontrarse mutuamente en "tiempo real" -por diversas razones de orden práctico-. Algunas de las modalidades que impiden esta comunicación en tiempo real son las siguientes:

a. *Problemas técnicos*: incompatibilidad de programas, peso en *bits* del archivo, defectos en la red, recepción tardía de archivos adjuntos, servidor saturado, irrecuperabilidad técnica del mensaje.

b. *Modalidades sofisticadas*: buzones electrónicos, sistemas de acuse de recibo automatizados, arriendo de servidores, redes cerradas, sistemas múltiples de acceso, ventas *face to face* con máquinas (por ejemplo, expedidoras de billetes aéreos o ferroviarios), compras *self-service*, etc.

c. *Problemas administrativos internos*: horas habituales de servicio, negligencia en la revisión del correo, espera de decisiones colegiadas, ausencia del empleado que guarda en su poder los códigos de acceso.

d. *Incompatibilidades de orden internacional*: diversos husos horarios, días festivos nacionales, diferencias lingüísticas.

e. *Causas de fuerza mayor*: defectos en el suministro de energía eléctrica, paro de labores, huelgas, etc.

26. ¿Qué tipo de doctrina se reconoce en el caso de la contratación electrónica para el perfeccionamiento del contrato?

R. Como se sabe, hay cuatro doctrinas: doctrina de la declaración, doctrina de la expedición, doctrina de la recepción y doctrina de la información. En este caso nuestra ley reconoce la teoría de la recepción, o sea la tercera cronológicamente hablando, en términos de lo dispuesto en los arts. 80 y 91-92 del CCo.

27. ¿Qué sucede si alguno de los sujetos tiene redes de cómputo o distintos establecimientos comerciales?

R. En este caso, algunas leyes electrónicas previenen que el domicilio oficial será el que tenga “una relación más estrecha con la operación subyacente”. De no existir ésta, con el establecimiento que se juzgue como “principal”. Si no tiene ningún establecimiento se tomará en cuenta su residencia habitual. Si tiene su equipo de cómputo en redes, se considerará que la recepción tiene lugar en el momento en que entre el

mensaje de datos en cualquier sistema informático del destinatario, aun cuando se encuentre en otra ciudad.

Por último, ¿cuándo se tiene por lograda la recepción si el mensaje no arriba al sistema de información designado? Pues bien, la recepción tendrá lugar hasta el momento en que el destinatario original logre recuperar el mensaje de datos.

28. ¿Cuál es la forma en general de los contratos electrónicos?

R. Cuando sea ante notario, la forma se rige por la ley del notariado local. En general, las leyes modelo de la CNUDMI (por ejemplo, LMCE, art. 6) solamente exigen que la contratación electrónica conste por escrito.

29. Dicho consentimiento, ¿se puede otorgar en instrumento público ante notario?

R. Sí, según los arts. 1834 *bis* del CCF y 93 del CCo. Es importante hacer constar en el documento los elementos a través de los cuales la información se atribuya a las personas obligadas y el fedatario debe conservar bajo su resguardo una versión íntegra para su consulta posterior.

30. ¿Se requiere de contrato previo para entablar contratación electrónica?

R. No, el art. 1811 CCF ya no lo exige más.

31. ¿Qué tipo de interpretación debe aceptarse en la contratación electrónica?

R. El Código Civil Federal dice en su art. 1857 que

> Cuando absolutamente fuere imposible resolver las dudas por las reglas establecidas en los artículos precedentes, si aquéllas recaen sobre circunstancias accidentales del contrato, y éste fuere gratuito, se resolverán en favor de la menor transmisión de derechos e intereses; si fuere oneroso se resolverá la duda en favor de la mayor reciprocidad de intereses [...].

Por su parte, los *Principios sobre los Contratos Comerciales Internacionales* (art. 4.6) han establecido la regla doctrinal de la *interpretatio contra proferentem.*

A su vez, los Principios sobre los Contratos Comerciales Internacionales (PCCI) de UNIDROIT (1994) establecen en sus artículos 1.6 y 1.7 que deben tomarse en cuenta el carácter internacional de la normativa, la necesidad de promover la uniformidad en su aplicación, los principios de buena fe y lealtad negocial (*the golden rule*) inherentes al comercio internacional y su conformidad con los principios generales del derecho.

En cuanto a su interpretación técnica, los artículos 4.1 y 4.2 aclaran que el contrato debe interpretarse "conforme a la intención común de las partes", o bien "conforme al sentido que le habrían dado personas sensatas de la misma condición que las partes colocadas en las mismas circunstancias".[7]

PARTE SEIS: EL DERECHO INFORMÁTICO Y LA INTERVENCION NOTARIAL

32. ¿Pueden firmar electrónicamente los notarios o corredores públicos?

R. Sí, según el art. 30 *bis*, 1 del CCo, siempre que se les autorice previamente el acceso a la base de datos del Registro Público de Comercio (RPC). Cada fedatario debe otorgar una fianza por un total de $548,000 pesos, equivalentes a diez mil veces el salario mínimo vigente en el Distrito Federal (unos $41,000 dólares norteamericanos, aproximadamente) y requieren estar previamente certificados por la Secretaría de Economía. La Secretaría ejerce control para salvaguardar la confidencialidad de la información remitida por vía electrónica.

[7] El *Uniform Comercial Code* (UCC) de los Estados Unidos previene la regla *parol evidence rule* (parágrafo 2.202).

33. ¿Qué es el FEDANET y cuál es su marco legal?

R. La Secretaría de Economía ha implementado el Sistema Integral de Gestión Registral (SIGER) a través del programa FEDANET. Este sistema permite al corredor o notario utilizar medios electrónicos para inscribir actos de comercio en el RPC, utilizando una firma electrónica avanzada con ayuda de un dispositivo biométrico, una tarjeta inteligente y la huella dactilar.

El marco legal está conformado por los artículos 10, 20 *bis*, fracción V, 21 y 21 *bis* del Código de Comercio, según reformas del 19 de mayo de 2000, 4-11 del Reglamento del Registro Público de Comercio, de 2003, así como los Lineamientos de Operación del Registro Público de Comercio, de 2000 y el Convenio de Coordinación para la Operación del Registro Público de Comercio de 2001, publicado en el *Diario Oficial de la Federación* el 7 de febrero de 2002. Su uso es obligatorio.

34. ¿Se tiene que reformar la ley del notariado para incluir la contratación electrónica?

R. La respuesta depende de la modificación que se pretenda. En el estado actual de los avances de la tecnología electrónica, es posible localizar cinco áreas en las que esta interacción puede producirse:

a. Reconocer la posibilidad legal de la contratación negocial por medios electrónicos precisando sus alcances y limitaciones (lugar y tiempo del perfeccionamiento, determinación de las consecuencias legales, precisar si se trata de comunicación entre presentes o entre ausentes, clasificación del lugar y modo de expedición y recepción, clasificación del consentimiento como tácito o expreso, etc.).

b. Reconocimiento de la firma digital como equivalente a una firma autógrafa y, por tanto, con plenos efectos legales.

c. Reconocimiento del concepto “mensaje de datos” y su valoración como medio de prueba.

d. Reconocimiento de ciertos entes públicos o privados como agentes certificadores electrónicos (notarios y corredores, en el caso de México).
e. Reconocimiento de lo que se ha denominado “protocolo notarial electrónico” (libros, certificaciones, testimonios, índices, sello y respaldo técnico).

Como se ve, lo relativo al comercio electrónico, a las firmas digitales y al concepto “mensaje de datos” ha sido ya objeto de reconocimiento en algunos códigos civiles, de comercio y leyes federales en el caso de México. La posibilidad de que algunos fedatarios se constituyan en agentes certificadores proviene de un convenio realizado con organismos gremiales, empresas privadas y la administración pública a través de la autoridad correspondiente (Secretaría de Economía). El reconocimiento del protocolo notarial electrónico depende de la legislación local en cada una de las entidades.

Desde un punto de vista estricto, una vez establecida la equivalencia respecto de la forma escrita en soporte papel y en soporte electrónico, así como el valor legal de la firma digital, no hay necesidad de modificar la ley del notariado, por lo menos respecto de estas dos cuestiones.

En general, puede concluirse que la *función* notarial permanece invariable; lo que sí cambia es, desde luego, la *técnica* del notario. Es algo muy similar al proceso experimentado cuando se pasó de la pluma fuente a la máquina de escribir y luego a la impresión en gelatina, *offset* y computadora. No hay ningún precepto en la ley del notariado que impida esta transición técnica.

35. ¿En qué tipo de actos puede intervenir ya el notario?

R. Desde 1998 la Asociación Nacional del Notariado Mexicano, A. C., celebró con “Informática Selectiva” (INFOSEL) la denominada “Alianza para el desarrollo de la red de certificación y registro de firmas digitales de los

notarios públicos mexicanos". En términos de ese acuerdo, los notarios afiliados al servicio estarían en posibilidad de efectuar la certificación y el registro de firmas digitales según un mecanismo estándar a nivel nacional e internacional, a través de tres sujetos: agentes certificadores (los notarios), una agencia certificadora aplicativa (ANNM) y una agencia registradora aplicativa (la empresa privada).

Pocos años después, la compañía ACERTIA sustituyó a INFOSEL, pero en la práctica, los avances no fueron muy grandes. Actualmente la compañía "Seguridata, S. A. de C. V." es la que presta el servicio en el marco de la "Red de Certificación Digital" (RCD), donde intervienen la Secretaría de Comercio y Fomento Industrial (actualmente Secretaría de Economía), la Asociación Nacional del Notariado Mexicano, A. C., la propia Seguridata y los usuarios del servicio.

Los denominados "quioscos" municipales proporcionan ya en forma muy eficiente los siguientes servicios: pago de predial, licencias comerciales, multas, impresión de constancias, informes catastrales, formatos diversos, actas del registro civil, constancias de avalúos, certificados de adeudos, etc.

En estos casos pueden distinguirse cuatro fases graduales en el servicio. Primero, la información sólo *estática* (aparece la descripción del trámite o servicio, con dirección, teléfono y horario); segundo, la información *dinámica* (se puede recibir información mucho más específica y bajar formatos para impresión); tercero, la *interactiva* (se consulta y proporciona la información dentro de una base de datos) y por último, cuarto, la *transaccional* (hay cuentas donde se hacen cargos y abonos e incluso se expide la documentación solicitada).

Hasta ahora, los actos más comunes en los cuales interviene el notario son:

a. La certificación de sitios *web*,
b. Fe de hechos frente a la pantalla de computadora, y
c. Certificaciones de firmas digitales.

36. ¿Cuál es el procedimiento para la expedición de certificados?

R. El manual describe así el procedimiento:

El fedatario hace constar “el reconocimiento de firma y la fe de hechos” que se realiza a solicitud del compareciente, quien exhibe un documento denominado “solicitud-requerimiento de certificación de firma digital”. Dicho documento contiene la clave pública que se asume como propia del compareciente, la cual se encuentra vinculada a una clave privada y se relaciona con los datos del titular. Además se entrega el *diskette* con el archivo electrónico que contiene dicha información para su proceso, validación y registro.

El compareciente reconoce la firma autógrafa contenida en el documento y, desde luego, ratifica su contenido. Lo mismo hace con el documento conocido como “Declaración de Prácticas de Certificación”, donde se definen las políticas y procedimientos del servicio y los estándares respectivos.

Por su parte, el fedatario receptor levanta declaración unilateral de voluntad donde constata la capacidad legal del compareciente, así como su identidad, dice que tuvo a la vista los documentos del caso, que leyó y explicó el instrumento y que además se firmó en su presencia. A continuación, expide un certificado digital usando el *kit* de operación respectivo.

El procedimiento es muy similar en el caso de personas morales, si bien en este caso el notario debe constatar los pormenores que se refieren a la legal existencia y capacidad de la empresa, la satisfacción de los requisitos estatutarios, las atribuciones del representante y la cadena de las decisiones societarias para el acto específico.

El convenio prevé también la certificación de sitios *web* con el perfil legal y comercial de una empresa determinada. En este caso el fedatario da asimismo fe de la declaración de voluntad del usuario, expide el certificado digital y finalmente emite el “sello de sitio certificado”.

También se podría certificar una transacción electrónica elaborando el documento en el protocolo electrónico del fedatario y enviándolo a través de la red. Los contratantes lo firmarían digitalmente y entonces el notario lo autorizaría incorporándolo definitivamente a su protocolo. Una vez registrados los certificados, el notario puede proceder a la expedición del testimonio respectivo.

37. ¿Qué sucede cuando el notario certifica una determinada situación jurídica que luego cambia con el tiempo?

R. La respuesta se encuentra en el servicio de publicidad registral en la red a cargo de una *autoridad certificante superior* que registra todos los movimientos de actualización, modificación, vigencia y extinción de los derechos originalmente acreditados por la autoridad certificante. Es lo que se llama "ciclo vital del certificado" (*operational period*), que abarca el periodo que va desde la solicitud o expedición del certificado hasta su terminación –por la causa que fuere–.

38. ¿Cuánto cuesta una certificación electrónica?

R. En México se tenía previsto un costo de $195 dólares para personas físicas y $390 dólares para personas morales, según los convenios firmados por la Asociación Nacional del Notariado Mexicano, A. C. y la empresa "Seguridata".

La certificación de sitio costaba $780 dólares (dominio principal). Los dominios relacionados, $585 dólares por cada año.

En Estados Unidos depende del tipo de *software* que se decida adquirir. En promedio, tiene un costo aproximado de $400 dólares. Normalmente son válidos por un año a partir de la fecha de expedición. La empresa VeriSign dispone del *Secure Site Seal* (sello de sitio seguro) con costos de $695 y $1,790 dólares, con dos rangos de certificación en 128 y 256 *bits* y servicios accesorios provistos por NetSure, una empresa respaldada por Lloyd's de Londres. A la fecha VeriSign ha expedido unos 450,000

certificados digitales de sitios *web* y casi cuatro millones de certificados digitales para particulares.

Por último, en algunos otros países el costo depende del grado de seguridad que el usuario exija, de modo que la empresa certificante dispone de distintos niveles y costos en la certificación del acto. Incluso en algún país es posible encontrar que la certificación se haga sin el respaldo documental o electrónico necesario en el archivo de la emisora. En todo caso esta circunstancia debe ser puntualmente advertida al usuario.

PARTE SIETE: DERECHO INFORMÁTICO Y PROTECCION DEL CONSUMIDOR

39. Desde otro punto de vista, ¿las transacciones vía electrónica son consideradas como ventas mediatas o como ventas entre presentes (*face to face*)?

R. Los arts. 51-56 de la LFPC tratan de las ventas a domicilio mediatas (o indirectas). El art. 53 de la LFPC previene especialmente las ventas por teléfono, televisión, servicios de correo o mensajería "u otros donde no exista trato directo con el comprador", por lo cual una transacción electrónica debe ser considerada como venta a domicilio mediata o indirecta y no como venta entre presentes, con lo cual en esta área del derecho de consumo se rompe el principio general del 1805 CCF que equipara la venta a contratación entre presentes.

40. ¿El consentimiento por vía electrónica en ventas masivas es expreso o tácito?

R. Según el art. 1803, frac. I del CCF el consentimiento es expreso cuando se manifiesta por medios electrónicos. Ahora bien, no debe olvidarse que en todo caso la gran mayoría de los contratos electrónicos son contratos de adhesión -aunque desde luego siempre hay un modo interactivo con el

usuario-. También existe la aceptación escrita, cuando por ejemplo uno llena un formulario existente en la red, que luego puede enviarse por correo electrónico, vía postal ordinaria o fax.

Al final, de todas formas queda claro que el consentimiento con estos medios novedosos se resuelve finalmente en la presión de un botón haciendo clic (o incluso doble clic, o poniendo el nombre, o el correo electrónico, de modo que la aceptación resulte más deliberada). Así pues, nos encontramos sin duda frente a un gesto o movimiento físico, pero no necesariamente frente a una aceptación expresa según la doctrina volitiva tradicional (*cfr.* preg. 5, sobre *captchas*).

41. ¿Cuál debe ser el contenido del documento donde se consigne la transacción electrónica?

R. El documento en cuestión debe contener la siguiente información:

a. Datos personales del proveedor (76 *bis*, III LFPC);
b. Duración de la oferta (76 *bis*, IV);
c. Lugar y fecha de perfección del contrato;
d. Descripción de los artículos (76 *bis*, III, IV, V);
e. Calidad de las mercancías (76 *bis* VI);
f. Precio total incluyendo manejo, embarques o impuestos (76 *bis*, V);
g. Especificación de garantías;
h. Tipo de cambio monetario;
i. Disposiciones específicas aplicables sobre tarjetas de crédito;
j. Periodo de revocación (*cooling off period*);
k. Tiempo de entrega de los bienes o de ejecución del servicio (76 *bis* V);
l. Devolución del pago en su caso o cambio de mercancías;
m. Información para quejas (76 bis III) y persona física responsable, y
n. Por último, información sobre mecanismos informales de resolución de disputas (76 *bis* III).

42. ¿Cuántos años deben conservarse los registros electrónicos por comerciantes?

R. Diez años. La Norma Oficial Mexicana (NOM) de fecha 20 de marzo de 2002 (publicada en el *Diario Oficial de la Federación* con fecha cuatro de junio de 2002) estableció las condiciones técnicas.

43. ¿Qué sucede con los pagos anticipados si la mercancía no llega o está defectuosa?

R. El art. 54 LFPC trata de responder a esta interrogante limitándose exclusivamente a la obligada advertencia que el proveedor debe realizar al consumidor. Sin embargo, el problema no tiene fácil solución, porque el cargo puede hacerse en forma automática al recibo telefónico, a la tarjeta de crédito o a una cuenta específica. Lo mismo sucede cuando el consumidor debe pagar obligatoriamente una llamada de larga distancia o sufragar los gastos de entrega.

44. ¿Qué pasa en caso de controversia formal? ¿Cuál es la jurisdicción aplicable?

R. Esta pregunta se relaciona directamente con el *dónde* y *cuándo* se perfecciona el contrato. Ya he dicho que el momento de perfección del contrato se establece precisamente en la tercera etapa, es decir, al momento de la recepción. Si esto es así, el contrato se tiene realizado cuando el oferente o vendedor recibe en su computadora la solicitud o el pedido del cliente que, por tanto, ya aceptó la oferta y es en ese preciso momento y en la ciudad de recepción cuando se tiene por concluido el contrato.

Para un consumidor nacional, esto significa que frecuentemente el contrato se habrá concluido en el extranjero, ya sea en Los Ángeles, Miami, Singapur o Taiwán, porque el art. 94 del CCo dice: "Salvo pacto en contrario, el mensaje de datos se tendrá por expedido en el lugar donde el

emisor tenga su domicilio y por recibido en el lugar donde el destinatario tenga el suyo".

45. ¿En general, está protegido el consumidor en la contratación electrónica?

R. Sí, con fundamento en el art. 1º fr. VIII de la LFPC que dice:

> Art.1º
> [...]
> El objeto de esta ley es promover y proteger los derechos del consumidor y procurar la equidad y seguridad jurídica en las relaciones entre proveedores y consumidores.
> Son principios básicos en las relaciones de consumo:
> [...]
> VIII. 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.

Por su parte, el art. 24 fracción IX *bis* prevé la redacción de códigos de ética, pero sólo en forma voluntaria:

> Art. 24. La Procuraduría tiene las siguientes atribuciones.
> […]
> IX *bis*. Promover en coordinación con la Secretaría la formulación, difusión y uso de códigos de ética, por parte de proveedores, que incorporen los principios previstos por esta ley respecto de las transacciones que celebren con consumidores a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología.

También se aplican los arts. 76 *bis* y 128 de la misma LFPC en los siguientes términos:

a. La información que el consumidor proporcione al proveedor será confidencial;
b. El proveedor debe informar al consumidor de los elementos técnicos disponibles para la seguridad y confidencialidad de este último;

c. El proveedor debe informar antes de la transacción su domicilio físico, números telefónicos y demás medios para quejas o aclaraciones;
d. El proveedor debe evitar prácticas comerciales engañosas.
e. El proveedor debe dar información al consumidor sobre las condiciones, costos y forma del pago;
f. El proveedor debe asegurar la calidad de los materiales.
g. No debe enviar avisos comerciales, y
h. Por último, sus estrategias de venta o publicidad deben ser claras, especialmente para los niños, ancianos y enfermos.

46. ¿Existen periodos de espera forzosa para la revocación del contrato (*cooling off period*) considerando que la contratación es mediata o indirecta?

R. El art. 56 de la LFPC dice que el contrato se perfecciona a los cinco días hábiles a partir de la entrega del bien o de la firma del contrato, lo último que suceda. Sin embargo, esto plantea problemas en el derecho internacional: Canadá tiene un plazo de diez días; Estados Unidos lo reduce a tres y un decreto español sobre contratación telefónica o electrónica lo fija en siete. Los "Lineamientos para la protección al consumidor en el contexto del comercio electrónico", expedidos por la Organización para la Cooperación y el Desarrollo Económico (OCDE) en diciembre de 1999 disponen también de un "procedimiento de confirmación" (Segunda Parte, IV), pero sólo para cancelar la transacción precisamente *antes* de concluirse la compra.

PARTE OCHO: AUTORIDADES CERTIFICADORAS (A.C.)

47. ¿Cuáles son las funciones más importantes de una autoridad certificadora?

R. Las funciones más importantes son las siguientes, sin tomar en cuenta los distintos niveles en que pueden actuar:

a. La función tradicional de certificar un documento en contenido y firma o cotejarlo con su original;

b. La función de certificar la identidad de las personas físicas y acreditar la representación de las personas morales y, en ambos casos, su capacidad legal o la vigencia de sus derechos;

c. Archivar y conservar el documento, así como copias de las llaves para el caso eventual de extravío o demostración de existencia cierta.

d. Acreditar el momento y el lugar exacto de presentación del documento, a la manera de un reloj checador o *time stamping*.

e. Servir como ventanilla electrónica, aprovechando una previa infraestructura comercial de conveniente ubicuidad.

f. Acreditar lo que se denomina el *ciclo vital del certificado* expedido, consignando la exactitud de las declaraciones, así como los servicios oportunos de revocación, cancelación y extinción del certificado.

g. La novedosa función de certificar a quien certifica, a cargo de un organismo gremial o de una autoridad privada o gubernamental (certificación superior o *superior certification authority)*.

h. La función de homologar las certificaciones en el ámbito del derecho internacional.

i. Por último, intervención en las redes internas (*intranet*) del sistema informático de entidades gubernamentales o privadas.

48. ¿Cuál es la diferencia entre las autoridades de certificación *abiertas* y *cerradas*?

R. Las entidades de certificación *cerradas* emiten certificados que sólo pueden ser utilizados entre la propia entidad emisora y el eventual suscriptor. Es muy útil en los casos de empresas transnacionales, entidades universitarias y organismos gubernamentales.

Por su parte, las entidades de certificación *abiertas* emiten certificados que pueden ser utilizados en forma genérica. Los requisitos de estas últimas entidades son mucho más rigurosos e incluyen cuestiones tales como el acreditamiento de su personalidad, capacidad de administradores o representantes legales, declaración de prácticas de certificación satisfactorias, capital social mínimo, constitución de garantías, infraestructura óptima, auditorías legales y técnicas, etc.

49. ¿Quiénes pueden ser autoridades certificadoras?

R. Hasta el momento hay una amplia variedad de personas y organizaciones, tanto públicas como privadas. He aquí una breve relación de ellas:

Alemania: notarios públicos electrónicos, Autoridad Reguladora de Telecomunicaciones y Correo de Bonn.

Argentina: Comisión Nacional de Valores, Consejo Federal del Notariado Argentino, Ministerio de Justicia y Derechos Humanos, gerentes de sitios internet (*website's postmasters*), compañías de seguros, registradores, conservadores de la propiedad, funcionarios oficiales, bancos, correos paralelos (DHL, UPS, FedEx, Redpack), Secretaría de la Función Pública y
Certisur (VeriSign).

Brasil: Central Brasileira de Sinal Público (Colegio de Notarios de Brasil).

Chile: ministros de fe, notarios, conservadores.

Colombia: cámaras de comercio.

España: Fundación para el Estudio de la Seguridad de las Telecomunicaciones (FESTE).

Japón: *malls* especializados, proveedores de equipos electrónicos, asociaciones de comercio electrónico, empresas productoras de *software*.

Perú: fedatarios particulares juramentados.

Estados Unidos: *cybernotaries*, *International notarial practitioners*, despachos de abogados (Arthur Andersen), secretarías de estado, oficinas postales, *International Civil-Law Notaries*, empresas privadas (Microsoft, BelSign, VeriSign, GemPlus).

Alabama: *civil-law notaries* (Florida).

Texas: *escrow agents*.

Uruguay: casas de bolsa, oficinas de correo, cámaras de comercio.

Así las cosas, es probable que en el futuro cercano suceda un fenómeno similar al de los *money orders*, donde los bancos, oficinas postales, compañías de carga y tiendas especializadas funcionan como agentes autorizados o mediadores prestadores de infraestructura comercial.

50. ¿Quiénes son en México las autoridades certificadoras y los agentes registradores (A.R.)?

R. Hasta ahora están legalmente autorizados como autoridades certificadoras centrales para las firmas electrónicas avanzadas los siguientes organismos: Secretaría de la Función Pública, Secretaría de Economía, Secretaría de Hacienda y Crédito Público y el Banco de México. Como agencias certificadoras están normativamente previstos los notarios, los corredores, los bancos y las instituciones gubernamentales.

A la fecha se han habilitado tres PSC autorizados por la Secretaría de Economía: Advantage Security, PSC World y recientemente CECOBAN (agosto de 2008).
