00761

LA SEGURIDAD DE LAS TRANSACCIONES EN EL COMERCIO ELECTRONICO POR INTERNET

POR ERIC TARDIF

TESIS DE MAESTRIA

FACULTAD DE DERECHO

UNAM

NOVIEMBRE DE 2000

Indice

Introducción

Los adelantos que se han logrado recientemente en tres grandes ámbitos tecnológicos – las computadoras, las telecomunicaciones, y los programas de computación y otras tecnologías de la información – han cambiado nuestras vidas de una forma que difícilmente pudiéramos haber imaginado hace veinte años. Las nuevas formas de intercambiar datos y de efectuar transacciones comerciales han transformado, a varios niveles, la organización social y económica.

Estas tecnologías modernas son combinadas, especialmente gracias a Internet, para enlazar millones de personas en el mundo. La transmisión de información es facilitada y agilizada por Internet, que ofrece mas flexibilidad que el teléfono o el fax. Es un medio de comunicación global que ignora las fronteras políticas.

El comercio electrónico global, guiado por el desarrollo del Internet, será un motor de crecimiento imprescindible en la economía mundial del

siglo XXI. Ofrece varias nuevas oportunidades para los empresarios y los individuos de todas las regiones del mundo. En particular, las pequeñas empresas podrán obtener un acceso privilegiado a mercados internacionales con poca inversión, y los consumidores podrán elegir entre una variedad de bienes y servicios siempre más grande.

Estos desarrollos, y los intentos de regularlos[1] no pueden, sin embargo, ser ignorados por el mundo jurídico[2]. Las cuestiones que más han interesado los estudiosos del derecho tienen que ver con la aplicación del derecho internacional privado y de las teorías de conflictos de leyes, al ciberespacio. Los asuntos que tienen que ver con la propiedad intelectual y el derecho fiscal también han llamado la atención de los doctrinarios.

Pero la cuestión que más preocupa a los individuos que se enfrentan a esta nueva forma de hacer negocios, y que no deja de ser sumamente interesante para el estudioso del derecho, es la seguridad de las transacciones que se hacen por Internet.

El punto de partida de este trabajo será tratar de mostrar que, aunque existen mecanismos que permiten pensar que el comercio electrónico puede realizarse de manera segura, esta actividad, por estar en la fase embrionaria de su desarrollo, conlleva varios riesgos que se deben a las fallas del sistema.

---

[1] El año 2000 resulto ser muy fructífero a este nivel, ya que el gobierno de los Estados Unidos de Norteamérica legislo para adoptar una ley sobre la firma electrónica, la Unión Europea emitió dos directivas relacionadas con el comercio electrónico, y Mexico también legislo sobre el tema a través de un decreto.

[2] Podemos constatar, al nivel académico, un interés marcado para la disciplina del derecho del comercio electrónico, que se ha traducido por la organización de un numero importante de coloquios y seminarios en varias universidades mexicanas.

Después de haber definido los conceptos claves de "Internet" y de "comercio electrónico" (capitulo 1), veremos la composición de las fuentes de lo que conviene llamar la *lex electronica* (capitulo 2). Nos interesaremos luego en los sistemas de pago que se manejan en Internet, con sus riesgos inherentes (capitulo 3), y en el papel que desempeña el sistema probatorio, con las mejorías que es necesario aportarle (capitulo 4). En el capitulo 5, veremos como la firma electrónica ya se ha vuelto una herramienta básica del comercio electrónico y de su seguridad, y estudiaremos sus limitaciones.

El trabajo de investigación se basara en el estudio de textos de doctrina, por la mayor parte escritos por autores europeos y norteamericanos[3], visto el estado muy avanzado del derecho del comercio electrónico en estas zonas geográficas. Por lo mismo, haremos referencias frecuentes a la legislación más representativa de estos países, a guisa de un estudio comparativo, y conscientes que varios Estados mas se han inspirado de estas leyes.

Trataremos de referirnos a la terminología técnica informática en ingles como en castellano, sabiendo que la mayor parte de las palabras claves empleadas ya forman irremediablemente parte del vocabulario básico del jurista del siglo XXI.

Capitulo 1:
Conceptos preliminares

1.1 Internet

Si la computadora es la herramienta tecnológica más importante del último cuarto de siglo, conectar el globo con redes de computadores de alta capacidad (incluyendo el Internet), será el reto tecnológico más grande del primer cuarto del siglo XXI. Las redes públicas y privadas ya han empezado a transformar la manera en que trabajamos, tenemos acceso a y creamos la cultura, y construimos la comunidad. Además, el ritmo de este cambio es impresionante. Aunque el uso general, no académico y de amplia difusión del Internet empezó hace menos de una década, la tasa de difusión y el impacto en la sociedad de este medio han sido enormes.

[3] Con el afán de alivianar el texto, tradujimos libremente al castellano las varias citas que aparecen a lo largo de este trabajo.

No es entonces una sorpresa que el Internet ponga al Derecho (y a los abogados, jueces y legisladores) en contacto con una amplia gama de retos. El derecho, que es típicamente reactivo, esta teniendo dificultades en tratar de seguirle el paso al dinamismo del Internet. Parece ser que cada semana aparece un nuevo dilema impulsado por la tecnología en el radar jurídico. Es obvio que si el Derecho quiere jugar su papel tradicional y útil de ayudar a ordenar el comportamiento social y económico, es necesario desarrollar conocimientos jurídicos y marcos de análisis para enfrentarnos al Internet.

1.1.1 Evolución tecnológica y redes

No pretendemos dar aquí un repaso de los aspectos tecnológicos de las computadoras y de las redes de comunicación, bases del Internet. Francamente, hasta un análisis sofisticado de las tecnologías actuales sería poco útil, porque se volvería rápidamente obsoleto. Lo que es importante, y hasta crítico, es comprender que la tecnología se esta volviendo cada vez más pequeña, mejor (es decir con más fuerza y más facilidad de uso) y más barata, con una rapidez impresionante, gracias a los logros importantes en las tecnologías de los semiconductores y las técnicas de transmisión digital.

Por ejemplo, el precio del procesador de computadoras ha ido bajando en un promedio de 30% al año en los últimos veinte años; entonces el costo de procesar información es un centésimo de 1% de lo que era al principio de los años 1970[4]. Para lo que se refiere a la transmisión de la

[4] Véase "A Survey of the World Economy: The Hitchhicker's Guide to Cybernomics", *The Economist* (28 de septiembre de 1996). Este articulo ilustra esta idea diciendo que si la industria automotriz fuera capaz de

información, la tendencia es también el desarrollo de medios de comunicación más pequeños, mejores, y más rápidos. Y aquí también, las últimas tecnologías en comunicación han producido importantes bajas en los precios.

La evolución de la computadora desde una máquina que solo procesa datos, hasta un aparato que procesa y también transmite datos ha hecho posible el Internet. Cabe subrayar, sin embargo, que el hecho de transmitir datos antecede a las computadoras de casi un siglo, visto que el telégrafo empezó a utilizarse de manera amplia en la década de los 1850. El telégrafo fue una tecnología seminal, porque desde el momento en que Gutenberg desarrolló la prensa para impresión en 1485, hasta el telégrafo casi 400 años después, la información que era contenida en un medio basado en el papel, se movía tan rápido como la gente y los bienes, visto que el correo era transportado por caballo o barco.

El telégrafo fue la primera tecnología en disociar la transmisión de la información del transporte en general, empezando así la caída de las distancias geográficas en las relaciones humanas. A partir de la década de los años 1880, la comunicación oral por teléfono empezó a desafiar la supremacía del telégrafo como el medio básico de comunicación. Por lo relacionado con la transmisión, al principio del siglo XX se empezó a utilizar el radio, y 25 años después apareció el primer modelo de televisión; al final de los años sesenta la televisión por cable empezó a implantarse, contemporáneamente a los primeros esfuerzos de comunicación de datos entre computadoras.

---

producir mejoras equivalentes en la relación rendimiento-precio,, un coche hoy en día costaría menos de cinco dólares, y podría hacer 250,000 millas con un galón de gasolina.

A partir de los años setenta, las computadoras empezaban a ser conectadas entre sí por redes locales. Al principio de los años 1990, la telefonía celular y los servicios de transmisión de datos por satélite fueron introducidos en el mercado. Hoy en día, el Internet, red de las redes conjunta varios de los elementos disparatados de las revoluciones informáticas y de telecomunicaciones.

1.1.2 El Internet hoy

El Internet es un fenómeno extremadamente importante, tanto para el derecho informático como para la sociedad en general. Empezó en los años 1970 con el objetivo de enlazar varios socios militares, industriales y académicos norteamericanos con computadoras conectadas a través de líneas telefónicas; el Internet se ha expandido de manera sorprendente en los últimos años, e incluye actualmente varios millones de usuarios particulares y empresariales.

Para muchas personas, una computadora personal conectada al Internet es primeramente un medio de comunicación, y solamente de manera accesoria un procesador de datos. Con el desarrollo de la telefonía y el Internet, las industrias informática y de las comunicaciones serán virtualmente fusionadas, por lo menos hacia los usuarios. El resultado es una plataforma para la nueva "inteligencia de redes" que nace de la potencialidad para millones de personas de ser capaces de comunicar como nunca antes, con contrapartes de misma afinidad.

Vale la pena describir brevemente algunos de los servicios y características del Internet, como varios de sus principales participantes. El

Internet es un fascinante ejercicio de anarquía simbiótica. Técnicamente, es una red de redes de computadora. Miles de computadoras anfitrionas sirven como depositarios electrónicos para volúmenes inmensos de datos, almacenados según un sistema de direcciones que da a cada sitio y a los buzones de correo en estos sitios, una residencia en el ciberespacio. Existe un número desconocido y creciente de computadoras que sirven como estaciones de enlace para la información que viaja entre computadoras anfitrionas.

El Internet es una red de computadoras e infraestructuras capaces de operar por medio de una serie de estándares (llamados protocolos de transferencia de datos) para el nombramiento de los sitios y para el envío de datos. Si es cierto que ninguna entidad en particular controla o posee el Internet, la *Internet Society* provee un liderazgo técnico en términos de la planeación de su arquitectura e ingeniería a largo plazo. Existen otros grupos responsables de otorgar los registros de las redes, para que una dirección de Internet siga designando sólo un lugar en el Internet.

Hay una gama amplia y variada de servicios en el Internet. Por un lado del espectro, encontramos el correo electrónico, o *e-mail*, por medio del cual se pueden enviar mensajes electrónicos a buzones electrónicos de correo registrados a nombre de particulares. El correo electrónico es un sistema de almacenajes y reenvío, y en unos minutos un mensaje puede pasar a través de varias computadoras antes de llegar a su destino. El e-mail puede ser mandado también a varios receptores. Otra característica muy distinta es el *usenet* o *usegroup*, que es un foro de discusión donde los participantes puede fijar recados y comentarios acerca de algunos temas.

La dimensión del Internet que crece más rápidamente es probablemente el *World Wide Web*, que permite a organizaciones crear sitios de información accesibles en una dirección específica, que pueden luego ser visitados por usuarios de cualquier punto del globo. Un aspecto increíblemente poderoso del "Web", como se llama coloquialmente, es la posibilidad de establecer reenvíos ("links") con distintas páginas de un sitio, o con otros sitios que quedan geográficamente a un mundo de distancia, simplemente haciendo "click" en las palabras subrayadas o enfatizadas. Esta característica del hipertexto ha permitido al Internet volverse una fuente inestimable de descubrimiento para toda una población de usuarios que no son muy familiares con las computadoras.

Hay unos cuantos participantes en el Internet que facilitan el acceso a esta herramienta. Los proveedores de servicios en línea son la alternativa de servicio completo, y ofrecen a través de sus propias computadoras, cierto número de servicios para sus clientes exclusivamente, además de ofrecer acceso a Internet. Estas empresas pueden por ejemplo agregar varios tipos de contenidos, servicios y características, para una variedad de sistemas de precios, según lo que el usuario encuentra más interesante.

Una variación de menor escala del proveedor de servicio en línea es el sistema de pizarras, que hasta podría ser manejado por una sola persona que utiliza un programa de mensajería de grupo. Por el otro lado del espectro está el proveedor de servicio de Internet que, en la mayoría de los casos, sólo ofrece acceso a Internet por una tarifa fija mensual, sin importar el número de horas de utilización. Entre estas dos opciones, se ubican los servicios de las compañías de teléfonos y cable que ofrecen más o menos servicios al cliente además del acceso a Internet.

Una variación en todos estos facilitadores es el *free-net*, una organización comunitaria que da acceso a Internet y a algunos de sus servicios. Y luego, obviamente, encontramos una multitud de proveedores de contenido, que van desde las entidades que ya mencionamos hasta las bibliotecas, universidades, corporaciones, gobiernos y particulares que pueden crear su propia presencia en el Internet a través de una página personalizada. Todas estas personas y entidades también son usuarios del Internet, dado que el Internet hace que se confundan los que hablan con los que escuchan que son los consumidores y los productores de la información.

1.1.3 El impacto en la sociedad

El Internet, aunque se encuentra prácticamente en una etapa embrionaria de su desarrollo, ya ha tenido un impacto importante en la sociedad. Aunque nos detendremos en los aspectos jurídicos, no hay que olvidar que estos cambios (y los más importantes que todavía tienen que llegar) también tendrán ramificaciones sociológicas, políticas y psicológicas impresionantes. Es obviamente difícil predecir con precisión como vaya a evolucionar el futuro del Internet.

La gente es propensa a sobrestimar el impacto a corto plazo de la tecnología, como subestima su impacto a largo plazo. Cuando el teléfono apareció, se pensaba ampliamente que aunque fuese útil para asuntos privados, nadie iba a utilizarlo para hablar de negocios. Los que piensan que el Internet es nada más una moda tienen parcialmente razón en el corto plazo, pero están totalmente equivocados a largo plazo, y no lograrán comprender el impacto crítico que tendrá en el desarrollo del derecho

informático. No queremos decir con esto que el Internet reemplazará pronto todas las formas de comunicación humana, particularmente porque es difícil para un nuevo medio de comunicación borrar completamente su predecesor – vemos por ejemplo que la radio y el cine han sobrevivido frente a la televisión y la videocasetera.

El Internet está, sin embargo más y más presente en el mundo social y económico. Sin embargo, hasta las predicciones hechas hace tres años se están revelando incorrectas, visto que algunos usos que se anticipaban para el Internet no se han materializado, y otros que no se previeron están creciendo exponencialmente. Como lo mencionamos anteriormente, las redes no son totalmente nuevas. El sistema de teléfono tradicional es una red, como también la televisión por cable. Hasta ahora, sin embargo, estos dos tipos de redes han sido muy diferentes de las redes de computo.

El teléfono ha sido esencialmente una comunicación interactiva de un punto a otro, mientras que la televisión por cable ha sido una comunicación no interactiva de un punto a varios. Las redes de cómputo facilitan las comunicaciones de un punto a varios, y de manera creciente, de varios puntos a varios más. Esta dinámica particular nunca se había visto antes, y su impacto será profundo, con importantes ramificaciones para nuestros sistemas educativos, de venta, financiero y político, para mencionar algunas áreas que cambiarán de manera significativa con el Internet.

Elizabeth Eisenstein ha narrado los cambios sociales profundos sucedidos en Europa alrededor de los años 1500 como resultado del cambio del proceso de los escribas (esencialmente los frailes y otros individuos copiando manuscritos) a la tecnología de la imprenta de Gutenberg, incluyendo el impacto fundamental e irreversible en la

educación, el lenguaje, la religión, la ciencia, y en las tendencias sociales como el crecimiento en la censura, la propiedad intelectual y las culturas nacionales[5]. Los cambios y las aceleraciones que resulten del desplazamiento del escrito por los medios electrónico centrados en el Internet serán así de básicos y con un alcance profundo.

Dos impactos sociales, resultados de la aparición del Internet, son dignos de notarse: la eliminación de la distancia y el acostumbramiento en masa. Podemos considerar la época en la que vivimos como la "Edad de la información", favorecida por la revolución informática, y oponiéndose a las edades agraria e industrial, cuando los puntos decisivos eran la tierra y los bienes físicos tangibles respectivamente, y no la información. Casi por definición, la geografía jugó un papel importante en la edad agraria, ya que la misma tierra era el aspecto decisivo del tiempo y los medios de comunicación eran lentos. En la edad industrial, el espacio geográfico todavía era importante porque era (y todavía es) caro mandar bienes tangibles a consumidores lejanos.

En contraste, una característica central de la Edad de la información es cómo las computadoras conectadas a redes electrónicas eliminaron en varias formas las distancias físicas. En la actualidad, la telefonía y los sistemas de cable ya han hecho que se encoja el mundo. Las redes totalmente electrónicas que pueden transmitir todas formas de información digital y de contenido eliminarán virtualmente la distancia geográfica como factor en varias empresas humanas, incluyendo la educación, la medicina, las finanzas y el entretenimiento.

---

[5] Eisenstein, E., *The Printing Revolution in Early Modern Europe*, Cambridge: Cambridge University Press, 1983

Por ejemplo, el impacto jurídico de la eliminación de la distancia será enorme. Las cuestiones jurídicas novedosas abundan cuando una persona u organización es capaz de mantener una presencia en otra jurisdicción de una manera meramente electrónica, o cuando alguien en una jurisdicción tiene acceso a un sitio web ubicado en una computadora que se encuentra en otra jurisdicción. ¿A partir de que momento se supone que una empresa esta legalmente realizando negocios en otra jurisdicción, de tal forma que esté sujeta a las leyes de la otra jurisdicción? O en el ejemplo de la telemedicina, un doctor que esta físicamente presente en Toronto, y operando remotamente a su paciente residente en un hospital en Colorado, ¿debe de tener una licencia del estado de Colorado para practicar?, y ¿está en ese momento practicando en Colorado?. Estos tipos de preguntas, se multiplicarán de manera exponencial con las nuevas e intrigantes aplicaciones que permitan eliminar el factor geográfico en las empresas humanas.

Con la importancia que esta tomando el intercambio de información en nuestra sociedad, y con la reducción en los costos de captura, almacenaje y manipulación de datos, las empresas y las agencias gubernamentales están empezando a conocer a los individuos como nunca antes. Las redes de cómputo, con sus grandes bases de datos, pueden ahora recrear el conocimiento detallado que el carnicero de la edad agraria tenía de los gustos de su clientela. La diferencia fundamental, obviamente, es que mientras el término de referencia del carnicero era su aldea, la base da datos moderna abarca literalmente el mundo entero.

El fenómeno de la producción de masa hecha a la medida descansa en la habilidad de las computadoras y las redes de dividir un producto o un servicio en sus componentes de información y entrega física. Actualmente,

una paciente va al hospital para la información y la entrega del servicio requerido. De manera similar, un consumidor va a una tienda par informarse (obtener un precio, determinar la disponibilidad y la calidad, el color, etc.) y para que se le entregue físicamente el producto.

De forma creciente, la información es dada con antelación a los usuarios potenciales del servicio o el producto. Esto ya esta pasando en algunos ámbitos incluso en el ambiente de la venta por catálogos, o de los pedidos de pizza por teléfono. Cuando los catálogos de productos, la información médica, o cualquier otra fuente de interés para el consumidor se encuentre en línea, el proceso de bifurcación se habrá acabado. Y conforme vaya el consumidor conociendo nuevos productos o servicios a través del Internet, el proveedor de esta información estará aprendiendo más acerca de este consumidor, agregando así más información personal a la base de datos.

La compilación y especialmente la diseminación a terceros de estos datos plantea unas cuantas cuestiones legales relacionadas con la privacidad, la protección de datos, y varias cuestiones comerciales. No es de sorprendernos que un cambio tan fundamental en la forma en que se harán muchos de los negocios, resulte en una revaluación importante de muchos de los principios jurídicos vigentes hoy en día, con al afán de traer a la Edad de la información las leyes que se encuentran actualmente completamente obsoletas o que necesitan una mejoría parcial.

1.2 Una aplicación practica: el comercio electrónico

La expresión "comercio electrónico" se encuentra muy de moda hoy en día. Sin embargo, algunas consideraciones básicas acerca de esta nueva manera de hacer negocios siguen siendo nebulosas porque radican en interpretaciones múltiples y a veces contradictorias. Esta constatación es significativa porque estas diferencias de interpretación raramente se mencionan. Pero no dejan de afectar la comprensión general de la noción de comercio electrónico. Es entonces deseable aclarar este concepto. En esta óptica, la siguiente parte tiene como objetivo presentar la noción de comercio electrónico y sus principales manifestaciones.

1.2.1 Definiciones

El concepto de "comercio electrónico", utilizado desde hace años, no es definido de manera formal y universalmente aceptada. Aunque muy comentada por varios integrantes del mundo jurídico, informático y contable, la expresión "comercio electrónico" sigue siendo ambigua. Se trata, prácticamente, de una expresión acerca de la cual encontramos casi tantas definiciones como individuos u organismos para definirla.

Para algunos, el comercio electrónico se define simplemente con el ejercicio de actividades comerciales por medio de las infraestructuras de información actuales. Según el *National Information Infrastructure*, el comercio electrónico es la evolución del intercambio de datos informáticos (mas conocido bajo la sigla inglesa "EDI") hacia otros tipos de datos y

transacciones[6]. Otros expertos prefieren definiciones más elaboradas donde el comercio electrónico integra las comunicaciones, la gestión de los datos y los servicios de seguridad con el fin de permitir las aplicaciones de negocio dentro de distintas organizaciones para intercambiar automáticamente información. La definición del comercio electrónico se encuentra entonces entre estos dos polos, desde la simple utilización de las capacidades de las infraestructuras de comunicación, hasta la integración de sistemas de comunicación, de gestión de datos y de seguridad.

La mayoría de las definiciones del comercio electrónico presentan algunos puntos en común. El primer elemento de consenso es el cumplimiento de actividades de manera automática por medio del uso de tecnologías informáticas y de comunicación. Como lo subrayan los investigadores del *San Antonio Electronic Commerce Ressource Centre*, "la clave para comprender el comercio electrónico consiste en considerar las actividades que, durante los últimos años, debían de ser cumplidas manualmente, personalmente, o por correo, y que ahora pueden cumplirse automáticamente y electrónicamente"[7].

Como estamos hablando de comercio electrónico habría que agregar a esta definición el hecho que las actividades que hay que considerar son las de naturaleza comercial. Esta calificación permite distinguir ese tipo de actividades de las de contenido cultural o social que también encontramos en el ámbito de ambientes informáticos. Ese es, de forma general, el segundo elemento de consenso que, aunque evidente, cabe recordar: la noción de comercio es el fundamento del comercio electrónico.

---

[6] www.ttfcat.nist.gov:94/doc/ElectronicCommerce.html
[7] www.saecic.org/test/about.htm

Por otro lado, se considera generalmente que la expresión "comercio electrónico" se refiere a una gama entera de actividades que implican los recursos informáticos actualmente disponibles. El comercio electrónico se define también por sus manifestaciones. El correo electrónico, la transferencia electrónica de fondos, y más particularmente el intercambio de datos informáticos, son ejemplos frecuentemente citados. Sin embargo, resulta difícil identificar con precisión las demás manifestaciones del comercio electrónico. Es que existe una falta de homogeneidad que refleja las dificultades planteadas por el carácter eminentemente cambiante y evolutivo de las nuevas tecnología de la información y comunicación.

1.2.2 El Internet comercial

La aparición de las motivaciones comerciales en Internet no se ha hecho sin algunas convulsiones que parecen hoy en día haber desaparecido. Desde su creación en 1969, el Internet se ha desarrollado sin ninguna preocupación económica, hasta recientemente. La abertura de esta red a un público más variado que los investigadores y militares, se ha hecho en dos etapas.

La primera etapa coincide con la invención del web por Tom Berners-Lee. Esta pantalla gráfica más agradable que las solas líneas de texto, atrae a los estudiantes de las universidades norteamericanas, quienes ven en ella una manera de intercambiar informaciones con otras casas de estudios. Esta primera abertura no provoca reacciones adversas con los científicos quienes entienden los deseos de sus alumnos, y atraen la atención de los empresarios y de los medios de comunicación. Para

reglamentar los comportamientos en la red, los investigadores y estudiantes desarrollan un código de buena conducta la "Netiqueta".

La falta de autoridad central, capaz de definir reglas y sancionarlas, hace que se tema cierta forma de anarquía. La red se organiza entonces alrededor de estas reglas a la vez jurídicas (una forma de jusnaturalismo) y morales. Las reglas prohiben las injurias en los foros, denuncian el racismo, disuaden la transferencia de archivos demasiado grandes que saturan la red, etc. Algunas de ellas se imponen de manera evidente, pero como en cualquier derecho natural, otras son más discutibles.

Por ejemplo el uso obligatorio del Inglés, excluyendo los demás idiomas que juegan el papel de dialectos locales, y la prohibición de toda acción de carácter comercial. Parece que, como en las artes, la ciencia no tiene buenas relaciones con los negocios. Esta prohibición ha hecho del Internet un espacio donde la información es gratuita, como también los programas de aplicación que se llaman *freeware*.

La segunda etapa coincide con la abertura de la red al público en general. Esta abertura fragiliza la Netiqueta. Los usuarios ignoran el código de buena conducta y comunican en su propio idioma; algunos hasta venden bienes físicos o información. En 1995, los profesionales que viven gracias a Internet encuentran sus principales recursos en la venta de acceso a las empresas y los particulares y la elaboración de servidores web. Se prohiben entre sí lanzar servidores mercantiles, porque una iniciativa de este tipo constituiría una violación flagrante de la Netiqueta.

Ya no nos enfocamos tanto en ello, pero las prohibiciones de la Netiqueta han tenido un impacto importante sobre el desarrollo del Internet

comercial. No existe ya ningún tabú, y la red esta empezando una segunda carrera que no elude totalmente la noción de gratuidad, pero rehabilita la posibilidad de vender información y bienes físicos. Esta evolución es necesaria, y la red no puede seguir recibiendo un número siempre creciente de usuarios, sin aceptar y promover un modelo económico viable. El costo de las infraestructuras de telecomunicación no puede ser financiado únicamente por los abonos pagados a los proveedores.

Hoy en día, el web cuenta con más de un millón de servidores, operados por empresas, administraciones, universidades o simplemente particulares. En este conjunto heterogéneo, los servidores comerciales se multiplican de manera impresionante, y no hay que dudar que la evolución de sus efectivos en los últimos años prefigura una verdadera explosión del comercio electrónico. Un estudio del despacho Júpiter Communication prevé que se haga el equivalente de 7,3 mil millones de dólares en negocios en la red durante el año 2000[8].

Los pioneros del comercio electrónico son los norteamericanos, que ofrecen servicios, información y bienes físicos. Algunos sitios son ya célebres, como la empresa Amazon Books, que vende más de 1 millón de libros exclusivamente en Internet, y dispone de la clientela más importante de la red. Amazon propone la más grande variedad de libros a precios rebajados. Como cada autor y cada título elegido por el cliente son automáticamente registrados en una base de datos, Amazon corresponde vía correo electrónico con sus clientes para señalarles otros libros que podrían interesarles.

1.2.3 Problemas jurídicos

Existen varias razones por las cuales el volumen de actividades es todavía bastante bajo en el ciberespacio comercial. A continuación, mencionaremos los principales problemas suscitados por el desarrollo del comercio electrónico, a guisa de ilustración.

1.2.3.1 Mecanismos de pago[9]

El Internet facilita las transacciones entre partes que se encuentran en lugares opuestos en el globo, a cualquier hora de la noche o del día, y por grandes o pequeños montos. Esto crea problemas únicos en términos de pago. Actualmente, la forma más popular de pagar para una transacción en Internet es por tarjeta de crédito. Debido a la naturaleza misma del Internet, existen riesgos asociados cuando se mandan datos a través de un servidor sin utilizar métodos criptográficos. Además, la tarjeta de crédito no es aceptable para todas las formas de transacciones. A veces, el monto es demasiado pequeño, o el consumidor puede desear que la transacción quede anónima, o no tiene acceso a una tarjeta de crédito. Otro problema que puede ocurrir es el riesgo de que haya una confusión por parte del consumidor acerca del monto de la compra cuando el precio aparece en una divisa extranjera.

Se ha puesto mucha atención en el desarrollo del dinero digital, que promete permitir a los consumidores hacer pequeñas compras anónimas en el Internet. El dinero digital es una lista de dígitos que emite un banco

[9] www.jupitercommunications.com/stats.html

atribuyéndole un valor definido (por ejemplo una ficha de diez dólares). Cada ficha tiene una "estampilla" digital que el banco utiliza para verificar su validez cuando el comerciante a quien se hizo el pago, lo presenta para su canje. Aunque las listas de dígitos pueden ser multiplicadas, la inclusión de esta "estampilla" asegura la autenticidad de la ficha.

Otra opción es el cheque digital, que opera esencialmente de la misma forma que un cheque de papel, en el sentido que actúa como una autoridad para transferir fondos desde el banco del consumidor al del comerciante. Las tarjetas prepagadas, similares a las utilizadas para las fotocopias o las llamadas telefónicas, son también disponibles para el comercio en Internet. Estas tarjetas tienen un valor, que puede ser o no recargable. Cada vez que se hace una transacción, el monto es transferido de la tarjeta al comerciante.

1.2.3.2 Derechos de autor

El Internet es concebido como un canal natural de distribución de bajo costo para la información y los productos de diversión como películas, música y libros. Estos productos son actualmente distribuidos en formatos físicos como los videos, los discos compactos, y varios impresos, pero podrían ser fácilmente bajados del Internet por el consumidor. Las preocupaciones acerca de la inadecuación de la protección actual de los derechos de autor han limitado los desarrollos en este ámbito. En el mes de julio del 2000, este problema ha llegado a un nuevo nivel, con las demandas de varias compañías disqueras entabladas en Estados Unidos de

[9] Para un estudio mas profundizado, véase el análisis que proponemos ulteriormente en el capitulo 3 de este trabajo.

Norteamérica, en contra de empresas como Napster, que permiten al publico usuario bajar de Internet grabaciones protegidas por derechos de autor.

Varios gobiernos han anunciado que harían reformas a sus legislaciones nacionales y locales para incluir un derecho de comunicación al público que se aplique a las obras disponibles a través del Internet y de otros servicios en línea. Estas reformas deberían ayudar a eliminar las preocupaciones de las empresas que quieren manejar materiales que involucran derechos de autor en el Internet, pero que hasta ahora se habían negado a hacerlo a causa de preocupaciones basadas en los derechos de autor.

1.2.3.3 Asuntos relacionados con los consumidores

Conforme vaya creciendo el uso del Internet para las transacciones comerciales, también se multiplicarán los problemas relacionados con los consumidores. Las preocupaciones particulares acerca de la explotación de los consumidores incautos, podrían nacer de algunos factores, como:

- el hecho de que el comerciante en Internet puede no tener ninguna dirección física, o encontrarse en otro país, creando problemas potenciales para la devolución eventual de la mercancía;

- que el acceso a talleres de reparación o servicio sea difícil o imposible;

- que el producto no sea conveniente para condiciones locales, o que sea incompatible con requisitos locales;

- que se dé la situación, particularmente en las ventas destinadas a los niños, en que un menor revele ingenuamente su dirección o entregue información delicada, por ejemplo acerca de una tarjeta de crédito.

Como existen dificultades a nivel de jurisdicciones, costos, plazos, y la aplicación de las leyes, es difícil pensar que la resolución de estos problemas transnacionales pueda basarse solamente en los recursos jurídicos. Es necesario un acercamiento internacional a través de iniciativas como la armonización de las leyes y la cooperación entre las agencias de ejecución, los programas de educación del consumidor, el compartir la información de las bases de datos acerca de los fraudes, el desarrollo de estándares de certificación en la industria y de códigos de comportamiento, y la armonización de estándares internacionales.

1.2.3.4 Asuntos fiscales

Como es el caso de cualquiera nueva empresa comercial, la viabilidad del comercio electrónico será determinada por lo menos parcialmente por el régimen fiscal aplicable. Los Estados Unidos de Norteamérica han adoptado la posición que no debería existir ningún régimen fiscal discriminatorio en contra del comercio electrónico por Internet. De hecho, aboga por una zona sin impuestos en el ciberespacio.

Esta política de zona sin impuestos no se extendería a los productos tangibles que se ordenen y que se paguen en línea, pero que se entreguen de la forma convencional. Los principios claves del derecho fiscal internacional, como la fuente de ingresos, la residencia y el lugar de establecimiento permanente, se encuentran quebrantados por la aparición del comercio electrónico. El impacto del sistema de impuestos para el comercio electrónico varía según las industrias; algunos métodos de pago electrónicos, como el dinero digital, tienen un alto potencial para la evasión fiscal, porque facilitan las transacciones globales rápidas y anónimas.

Además algunas tecnologías como la encriptación pueden ser utilizadas para reducir la disponibilidad y la confiabilidad de la información necesaria para la administración fiscal (como las cuentas de transacción y los archivos de negocios). Las leyes nacionales acerca del poder de fiscalización de las transacciones por el Estado, y las reglas acerca de la contabilidad tendrán que modificarse para adecuarse al medio electrónico; y la efectividad de los mecanismos existentes de recaudación se ve reducida por el comercio electrónico, porque facilita numerosas pequeñas transacciones directas, y elimina la necesidad de un intermediario (como un agente aduanal de importación), que muy a menudo ha tenido hasta ahora la responsabilidad de recaudar los impuestos. El funcionamiento eficaz del comercio electrónico requiere que se resuelvan todas estas preocupaciones, de una forma tecnológicamente neutral y que tenga un apoyo y reconocimiento internacionales.

1.2.3.5 Asuntos jurisdiccionales

A medida que el comercio electrónico abre nuevas oportunidades para el comercio internacional aparecen nuevos cuestionamientos acerca de la aplicación de las leyes a las transacciones que se conducen enteramente o parcialmente en línea. Los gobiernos de los países donde se utiliza más el comercio electrónico ya han empezado a recibir quejas de consumidores acerca de productos y servicios comprados de otros países.

Estas quejas son difíciles de resolver de manera individual a causa de los problemas jurisdiccionales, de la aplicación del derecho, y de los costos y plazos correspondientes. Las reglas jurisdiccionales como el lugar de la transacción y el derecho aplicable al contrato se vuelven obsoletas por la ausencia de fronteras que caracteriza Internet. Los comerciantes inescrupulosos encontrarán que es fácil evitar la reglamentación en el mercado electrónico, sin un acercamiento cooperativo y global a estos asuntos.

Capitulo 2:
Las fuentes de la *lex electronica*

Frente al carácter voluntariamente general de la noción de *lex electronica*, es natural que nuestro intento de identificación de sus componentes se articule alrededor de las fuentes tradicionales que asociamos al modelo de donde surge su inspiración, es decir la *lex mercatoria*. Es común integrar en esta última cinco categorías de normas: los tratados y convenciones internacionales; los contratos–modelo aplicados a un ámbito en particular; la jurisprudencia arbitral; los usos que emanan de la práctica, y finalmente, los principios generales del derecho[10].

Las tres primeras categorías corresponden a lo que podríamos llamar las fuentes institucionales es decir las vinculadas a una organización

habilitada, *de facto* o *de iure*, mientras que el carácter jurídico de las dos últimas tiene que ver con las particularidades inherentes a estas normas. Llamaremos las tres primeras "fuentes institucionales", mientras que nos referimos a las dos últimas como "fuentes substanciales". Cada uno de estos dos acercamientos pertenece a corrientes no clásicas: la primera corriente se fija en el derecho mas allá de la sola producción del Estado, según una visión pluralista y la segunda trata de atenuar los criterios de generalidad y de "imperatividad" que asociamos a las normas jurídicas.

2.1 Las fuentes institucionales

Hablar de fuentes institucionales merece una explicación previa. Basándonos en fundamentos teóricos, podemos decir que el derecho puede verse ante todo como el producto de organismos que gozan de un reconocimiento en una comunidad en particular. Según los teóricos del derecho, lo que hace que un conjunto de normas pertenezcan al derecho, es que se integren a un orden jurídico[11]. El orden jurídico internacional, en particular el que se refiere al comercio electrónico, dispone de instituciones cuya estructura y reputación son tales que pueden producir este tipo de normatividad.

Tocaremos entonces por encima este tema, interesándonos por empezar en la legislación internacional y local vigente en el ámbito del comercio electrónico. Luego, examinaremos los distintos instrumentos

[10] Para que sea creíble, pensamos que la autoreglamentacion debe de incluir el establecimiento de reglas significativas, que impongan verdaderas obligaciones a los actores, derechos y obligaciones que atribuidos a los participantes en una transacción.

[11] Véase Rocher, G., "Pour une sociologie des ordres juridiques", (1988) 29 *Cahiers de droit*, Montreal, p.105

contractuales que estas instituciones ofrecen. Finalmente, daremos un breve bosquejo de las instancias arbitrales que se dedican a las cuestiones de comercio electrónico.

2.1.1 Legislación

Las convenciones y tratados internacionales son los instrumentos en los cuales pensamos inmediatamente cuando una cuestión implica nacionales de varias jurisdicciones. Estos instrumentos, que ocupan un lugar primordial en la jerarquía normativa, constituyen a menudo la solución predilecta para acabar con las incompatibilidades que pueden existir entre distintas leyes nacionales. Sin embargo, su carácter formal y el largo periodo necesario a su elaboración, representan limitaciones importantes a su eficacia.

Esta constatación es mas cierta aun en el ámbito del comercio electrónico, que evoluciona muy rápidamente. Obviamente, no disponemos actualmente de tal documento. Sin embargo, existe una ley modelo elaborada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), sobre comercio electrónico. También nos parece importante mencionar algunas convenciones internacionales elaboradas en ámbitos más generales, para apreciar las exigencias que se mencionan acerca de la forma que las transacciones deben respetar. Estudiaremos su adecuación con el comercio electrónico.

2.1.1.1 La Ley modelo de la CNUDMI sobre comercio electrónico

Antes de hablar del documento en sí, es importante decir algunas palabras acerca de la CNUDMI. Este organismo, parte de las Naciones Unidas, tiene como misión facilitar los intercambios comerciales internacionales[12]. La CNUDMI se interesa desde hace mucho al caso preciso de la integración de la informática y de la electrónica en el comercio internacional[13]. Sin embargo, es a partir de 1991 que ha empezado una investigación profundizada de los intercambios de datos informáticos. Los trabajos de la CNUDMI se concluyeron con la adopción, por la Asamblea General en junio de 1996, del documento llamado "Ley modelo sobre el comercio electrónico"[14].

Sin fuerza obligatoria, esta ley constituye sin embargo una etapa importante en el proceso de adaptación del derecho a las nuevas técnicas de comunicación. La utilidad de este documento se manifiesta desde dos puntos de vista. Por empezar un modelo de ley es propuesto a los Estados para que lo adapten en su jurisdicción. Además, gracias a la reputación de la institución, este documento participa a la elaboración de principios que formarán los primeros elementos del derecho del comercio electrónico recién nacido.

Sin embargo, la primera utilidad parece lograda de mejor forma que la segunda. En efecto, la Ley propone sobre todo a los Estados una manera de librarse de las legislaciones nacionales que impondrían algunas

[12] Varias convenciones muy conocidas fueron elaboradas por este organismo, como por ejemplo la Convención de Viena de 1980, la Ley-modelo sobre arbitraje comercial, la Ley-modelo sobre transferencia de créditos, etc.
[13] Véase por ejemplo, UNCITRAL, "Report by the Secretariat, Legal Value of Computer Records", A/CN.9/269 (1985).
[14] UN.Doc./A/51/1 (1996).

exigencias de forma, mientras que con este nuevo texto, la CNUDMI no define siempre bien los conceptos. Esto es de hecho bastante sorprendente cuando sabemos que los trabajos preparatorios fueron bastante exhaustivos al respeto.

2.1.1.2 Otras convenciones

Si consideramos las exigencias de fondo que hay que satisfacer, es necesario examinar las convenciones internacionales vigentes que abarcan ámbitos más generales que el comercio electrónico. A menudo, se enumeran criterios en estas para determinar las modalidades exigidas para que una operación se juzgue válida. Este trabajo de repertoriar las cláusulas que tratan del tema ha sido realizado por una comisión especializada de las Naciones Unidas comúnmente llamada WP4[15]. Este tipo de investigaciones tienen como objetivo verificar como las exigencias formales, como las nociones de escrito, de firma, de documento, de original, etc., se manejan en los tratados.

El resultado, desafortunadamente, es que las convenciones no son muy bien adaptadas a las nuevas tecnologías de la información. En un informe del WP4, se menciona entre otras cosas que:

> Las reglas actuales acerca de las transacciones de comercio internacional tal vez no respetan de manera satisfactoria la realidad del intercambio de datos informáticos. En varias situaciones, bajo estas reglas,

[15] Doc.UN/Trade/WP.4/R.1096, "Review of Definitions of Writing, Signature and Document Employed in Multilateral Conventions and Agreements Relating to International Trade" (1994).

los mensajes informáticos siguen siendo potencialmente inaceptables como medios jurídicos de comunicación.[16]

De manera más optimista, podemos decir que las convenciones antiguas no podían hablar de otros soportes que el papel, visto que no existían medios de comunicación tan confiables como este medio. Se puede mostrar una evolución en la relación de las convenciones, y las más recientes integran mas y más los nuevos métodos de transacción por medio de soportes tecnológicos. Sin embargo, a pesar de esta observación, las convenciones que establecen criterios precisos acerca de las exigencias formales necesarias para la validez de una transacción, son raras.

2.1.1.3 El marco europeo

La Unión Europea ha adoptado una Directiva sobre el comercio electrónico en mayo del año 2000[17] , que cubre todos los servicios de la sociedad de la información, entre empresas y consumidores, y los servicios prestados gratuitamente al usuario, como los servicios que permiten las transacciones electrónicas en línea como la venta interactiva de bienes y servicios y los centros comerciales en línea.

Las actividades cubiertas incluyen los periódicos en línea, las bases de datos en línea, los servicios financieros en línea, los servicios profesionales en línea (abogados, médicos, contadores, agentes inmobiliarios), los servicios de diversión en línea, la mercadotecnia y la publicidad directas, y los servicios de acceso a Internet.

[16] Doc.UN/Trade/WP.4/R.1096, p.2.
[17] "Directive 2000/31/CE", www.europa.eu.int/comm/internal_market/fr/media/eleccomm/2k-442.htm.

La Directiva se aplica exclusivamente a los proveedores de servicios establecidos en la Unión Europea. Sin embargo, para no causar trabas al comercio electrónico mundial, el texto trata de evitar incompatibilidades o incoherencias con los desarrollos jurídicos de otras partes del mundo. Además, en algunos sectores, la Directiva prevé soluciones que pueden servir como modelo a nivel internacional.

La Directiva define el lugar de establecimiento como el lugar donde un operador ejerce de manera efectiva una actividad económica a través de una instalación estable, sin importar donde se ubiquen los sitios web o los servidores o donde el operador tenga un buzón. Esta definición es conforme a los principios establecidos por el Tratado de las comunidades europeas y la jurisprudencia de la Corte europea de justicia. Esta definición levantara la incertidumbre jurídica y garantizara que los operadores no puedan sustraerse a la vigilancia, ya que esta será ejercida en el Estado miembro en el cual este establecido.

El texto prohibe a los Estados miembros imponer a los servicios de la sociedad de la información, regímenes de autorización especiales que no se apliquen a servicios parecidos que se prestan por otros medios. La Directiva prevé también que los Estados miembros obligan los proveedores de servicios de la sociedad de la información a facilitar, para sus clientes y las autoridades competentes, el acceso directo y permanente a las informaciones de base relativas a sus actividades (nombre, dirección, dirección electrónica, numero de matricula del registro del comercio, titulo profesional y afiliación a organismos profesionales, numero de registro de IVA, etc.)

La Directiva obliga los Estados miembros a suprimir todas las prohibiciones o restricciones acerca del uso de contratos electrónicos. Además, garantiza una seguridad jurídica, imponiendo algunas obligaciones de información para la conclusión de contratos electrónicos, especialmente para ayudar a los consumidores a evitar errores técnicos. Estas disposiciones completaran la Directiva que se adopto en los meses anteriores, en lo que atañe a las firmas electrónicas[18].

Con el afán de eliminar las incertidumbres jurídicas y evitar los acercamientos divergentes entre Estados miembros, la Directiva exonera los intermediarios de toda responsabilidad que desempeñan un papel pasivo, y que solamente aseguran el transporte de informaciones procedentes de terceros, limitando también la responsabilidad de los proveedores de servicios para otras actividades "intermediarias" como el almacenaje de información.

La Directiva establece un equilibrio riguroso entre los varios intereses involucrados, con el objetivo de fomentar la cooperación entre las varias partes y así reducir el riesgo de actividades en línea ilícitas.

El texto define las comunicaciones comerciales (como la publicidad y la mercadotecnia directa) y las somete a algunas condiciones de transparencia para reforzar la confianza del consumidor y garantizar practicas comerciales leales. Para que los consumidores puedan reaccionar con mas facilidad a la intrusión, la Directiva exige que las comunicaciones comerciales por correo electrónico puedan ser claramente identificadas.

[18] Véase el capitulo 5, en el cual tratamos de manera mas extensa de las firmas electrónicas.

Además, para las profesiones reglamentadas (como los abogados o los contadores), la Directiva establece el principio general según el cual la prestación de servicios en línea es autorizada, y que las reglas nacionales sobre la publicidad no impiden que estos profesionales utilicen sitios web. Estas actividades deberán sin embargo respetar algunas reglas de ética profesional, enunciadas en los códigos de conducta que sean elaborados por las asociaciones profesionales.

La Directiva quiere reforzar los mecanismos que permiten la aplicación de la legislación comunitaria y de las legislaciones nacionales existentes. Por estos efectos, sugiere la elaboración de códigos de conducta en la Unión Europea, estimula la cooperación administrativa entre los Estados miembros y facilita la utilización de sistemas en línea transfronterizos de solución de diferendos que sean eficaces. La Directiva exige también que los Estados miembros prevean recursos jurisdiccionales rápidos y eficaces, que sean apropiados al medio en línea, y velar que las sanciones aplicables a las violaciones de las disposiciones tomadas en aplicación de la Directiva sean efectivas, proporcionadas y disuasivas.

La Directiva precisa que el principio de reconocimiento mutuo de las legislaciones nacionales (uno sobre los cuales descansa el mercado común europeo) y el principio del Estado miembro de origen, deben aplicarse a los servicios de la sociedad de la información. No podrán entonces existir restricciones sobre la prestación de tales servicios a partir de otro Estado miembro. El texto no trata de la aplicación de la Convención de Bruselas sobre la competencia judicial y la ejecución de las decisiones en materia civil y mercantil, y no interfiere con la Convención de Roma sobre el derecho aplicable a las obligaciones contractuales en los contratos concluidos por

los consumidores, y tampoco afecta la libertad de las partes de elegir el derecho que rija su contrato.

El texto autoriza los Estados miembros a imponer restricciones a la prestación de los servicios de la sociedad de la información a partir de otro Estado miembro, si fuesen necesarias en relación con el orden publico, en particular para la protección de los menores, la lucha contra la incitación al odio por razones de raza, sexo, religión o nacionalidad, especialmente para los atentados contra la dignidad humana de los individuos, la salud publica o la seguridad y la protección de los consumidores, incluso los inversionistas.

Sin embargo, estas restricciones deberán ser proporcionadas con su objetivo declarado; además solo podrán ser impuestas (excepto en casos de emergencia o de acciones judiciales) después de que el Estado miembro involucrado haya pedido al Estado miembro en el cual esta establecido el proveedor de servicios, de tomar las medidas apropiadas, y que este no las haya tomado, y haya notificado a la Comisión europea y a este Estado miembro su intención de imponer restricciones. Cuando la Comisión considere que las restricciones propuestas o aplicadas no son justificadas, se invitara los Estados miembros a no imponerlas o a ponerle termino.

2.1.1.4 El caso de México

En México, la legislación se limitaba a prever como únicos medios para contratar entre no presentes al correo y al telégrafo. A la luz de tal disposición, las partes de un contrato podían acordar como mecanismo para dar el consentimiento el uso de medios electrónicos, previa celebración de un contrato marco por escrito, a fin de evitar la repudiación o la violación de

las obligaciones contraidas por las partes; sin embargo, el uso de los medios electrónicos estaba limitado a lo exclusivamente contenido en el contrato marco; era necesario adicionarlo o celebrar uno nuevo para cualquier modificación de las obligaciones originalmente contraidas.

En términos generales, la legislación no reconocía el uso de los medios electrónicos de manera universal, y en caso de un litigio el juez o tribunal tenia que allegarse de medios de prueba indirectos para determinar que una operación realizada por medios electrónicos fuese o no valida. Esta situación origino que algunas empresas frenaran sus inversiones orientadas a realizar transacciones por medios electrónicos, debido a la incertidumbre jurídica en caso de controversias.

Era necesaria una reforma legislativa, que se dio a mediados del año 2000[19], y que incluía las menciones necesarias para aprovechar los avances logrados no solo en el ámbito comercial, sino también en otros campos, para obtener una interacción en todos esos campos. El Decreto da valor probatorio al uso de medios electrónicos en los procesos administrativos y judiciales, sin que quede al arbitrio del juez considerar su validez probatoria en caso de controversia.

Se adecuo el marco jurídico mexicano para dar seguridad jurídica en el uso de los medios electrónicos, facilitar las transacciones por estos medios, y lograr la interacción de los campos en los cuales se utilizan los medios electrónicos. Fue una preocupación de los legisladores sentar

[19] "Decreto por el que se reforman y adicionan diversas disposiciones de Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, del Código Federal de Procedimientos Civiles, el Código de Comercio y de la Ley Federal de Protección al Consumidor", *Diario Oficial*, 29 de mayo del 2000, pp. 12-18.

bases jurídicas flexibles, que no puedan ser superadas por los nuevos avances tecnológicos que se pudieran alcanzar en el futuro.

En materia de Código Civil, se reconoce la posibilidad de que las partes puedan externar su voluntad o solicitar algún bien o servicio mediante el uso de medios electrónicos, e incluso dar validez jurídica al uso de medios de identificación electrónica. También se actualizaron los alcances de la legislación civil vigente en relación con los actos que requieren de la forma escrita otorgada ante un fedatario publico, y que pueden conservar e incluso fortalecer la seguridad jurídica en beneficio de los obligados, si se utilizan medios electrónicos, ópticos o cualquier otra tecnología, conforme a un procedimiento claro y particularmente descriptivo que acredite la atribución de información a una persona, y asegure que esta será susceptible de consulta posterior.

Con relación al Código Federal de Procedimientos Civiles, se agrego una disposición que concede efectos jurídicos, validez y fuerza probatoria a la información que consta en los medios electrónicos, y con ello, se reconocen efectos jurídicos a las obligaciones que de conformidad con el Código Civil, contraigan las partes mediante el uso de medios electrónicos.

En lo que se refiere al Código de Comercio, se agregaron disposiciones mercantiles innovadoras en aspectos informáticos, concediendo la posibilidad de que los comerciantes puedan ofertar bienes o servicios a través de medios electrónicos, y que conserven la información que por ley deben llevar mediante medios electrónicos.

Finalmente, si bien debe reconocerse la necesidad de contar con un marco jurídico que reconozca el uso de medios electrónicos, no se olvido en

esta reforma la protección del consumidor frente a estos medios. Consecuentemente, se incorporo a la Ley Federal de Protección al Consumidor las disposiciones mínimas que aseguren los derechos básicos del consumidor en las operaciones efectuadas a través del uso de medios electrónicos, ópticos, o de cualquier otra tecnología.

2.1.2 Los instrumentos contractuales

Sin tener que dar definiciones muy precisas, se pueden discernir dos categorías de instrumentos contractuales utilizados en el comercio electrónico: los códigos de conducta y los contratos modelo. Generalmente, los primeros instrumentos tratan de elaborar principios, y los segundos tienden a regir una relación entre dos partes, con una repartición más precisa y más práctica de las obligaciones.

2.1.2 .1 Los códigos de conducta

Es por medio de un código de conducta que existió el primer instrumento de comercio electrónico. En 1987, la Cámara Internacional de Comercio empezó la redacción de una guía acerca de la transmisión de mensajes electrónicos: el proyecto UNCID[20]. Hay que reconocer, sin embargo, que sus principios son relativamente tímidos, y que se nota cierta preocupación por la prudencia a lo largo de sus once artículos. Su influencia fue sin embargo notoria cuando se redactaron documentos ulteriores acerca del comercio electrónico, tanto en la Ley modelo de la CNUDMI como en algunos contratos modelo. A pesar de la generalidad de las medidas

enunciadas en este documento, así como la poca importancia que le da a la obligación de seguridad particularmente, las reglas UNCID constituyen los primeros fundamentos de la *lex electronica*.

Más recientemente, y en relación más directa con la "autopista de la información", hay que notar la existencia de algunos códigos de conducta que encontramos principalmente en las universidades norteamericanas bajo el nombre de "Acceptable Use Policies" (políticas de utilización aceptables). A pesar de su gran número, el carácter no comercial de estos códigos hace difícil intentar utilizar su contenido en el ámbito del comercio electrónico.

Finalmente, parece ser que un proceso de cooperación internacional para establecer un código de conducta, especialmente para lo que tiene que ver con el comercio electrónico, se está organizando.

2.1.2.1 Los contratos modelo

Cuando hablamos de contratos modelo en el ámbito de las nuevas tecnologías de la información, nos referimos generalmente a los contratos especialmente previstos para la comunicación por intercambio de datos informáticos (mejor conocido por su sigla inglesa de EDI – Electronic Data Interchange). El EDI clásico, que implica un contacto entre dos partes en el ámbito de una convención cerrada, tiene una antigüedad suficiente para que sea posible sacar algunas conclusiones importantes para discutir la elaboración de la *lex electronica*.

[20] UNCID (Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission)

De tal forma que, durante el año de 1990, varios Estados involucrados en las comunicaciones informáticas propusieron contratos-modelo a los hombres de negocios de su propio país, para volver más confiable el EDI. Sin ser totalmente exhaustivo, se habla de una decena de estos contratos: el modelo norteamericano, el ingles, el canadiense, el francés, el europeo, el australiano, el neozelandés, el alemán y el sudafricano.

Sin apegarnos demasiado a las estadísticas que parecen mostrar una utilización moderna de los contratos-modelo de EDI por los hombres de negocios, hay que tomar en cuenta también, a pesar de la dificultad en determinarla, la influencia que seguramente tuvieron sobre los contratos privados. Además, no hay que ignorar la influencia que los contratos modelo tuvieron los unos sobre los otros, según los sistemas jurídicos de los cuales provienen y, obviamente, de su fecha de elaboración respectiva. Estos documentos constituyen sin duda guías importantes en el ámbito más general del comercio electrónico, a pesar de que se previeron para un tipo de comunicación, la EDI, que posee su propia naturaleza.

2.1.3 Las instancias arbitrales especializadas

En el derecho del comercio internacional, las instituciones que emiten sentencias arbítrales ocupan un lugar primordial en el proceso de producción de las normas. El papel creador de estas instituciones es ampliamente evocado por la doctrina. En el ámbito del comercio electrónico, aunque la legitimidad de semejantes instituciones que se crearon recientemente necesita que pase más tiempo para establecerse adecuadamente, nos parece importante considerarlas. Entre los

experimentos de arbitraje que podemos constatar en el ciberespacio[21], cabe subrayar dos en particular.

El primer experimento empezó en marzo de 1996, con mucha publicidad: "el proyecto del magistrado virtual"[22]. Este proyecto norteamericano que reúne expertos juristas especializados, emite sentencias en línea a cualquier persona que acepte someterse a este foro. El proyecto fue lanzado, en primer lugar por varios profesores del *Villanueva Center for Information Law and Policy*. El *Cyberspace Law Institute* está también involucrado en este proceso. Además de estos organismos, esta nueva institución beneficia también del apoyo de la *American Arbitration Association*, sin duda la corte más influyente en los Estados Unidos de Norteamérica.

La idea fundamental es suscitar, con sus bajos costos, el entusiasmo de los usuarios, y así crear una práctica acerca del contenido de las decisiones y del procedimiento que acatar. Aunque hay que reconocer la celeridad de este grupo norteamericano en crear un arbitraje específico al ciberespacio, las sentencias emitidas han sido muy pocas. Una de las razones que puede tal vez explicar el éxito modesto de este proyecto, es la limitación impuesta por el "Virtual Magistrate" en su alcance: las cuestiones relativas al comercio electrónico no pueden ser estudiadas por este foro. Es una lástima, porque además de ignorar un amplio campo que esta tomando cada día mas importancia, esta negándose la oportunidad de atender a una comunidad de individuos (los comerciantes) que esta muy al pendiente de los usos que pueden surgir.

---

[21] Véase el articulo de Piette-Coudol, T., "Convention cadre pour le commerce électronique: commentaires et contrat" (1996) 2-2 *CyberNews* www.droit.umontreal.ca/CRDP/CyberNews/.

De tal forma que el Virtual Magistrate no puede desempeñar en este ámbito de actividad, el papel de catalizador de usos como uno se lo podía esperar. La otra crítica que es también posible formular, es que este proyecto tiene un acercamiento "adjudicativo": aunque el arbitraje es un procedimiento menos formal que los que encontramos en las instancias judiciales clásicas, sigue siendo un medio que opone una parte a otra. De tal forma que cuando un demandante considera que se están violando sus derechos en el ciberespacio, es difícil a menudo obligar al demandado que acate el laudo arbitral. Como no consintió a nada, éste solo vive en el miedo a que el quejoso se dirija a una instancia nacional. En muchos casos, esta amenaza es casi inexistente, por el precio de un juicio, el carácter internacional de los diferendos, lo irrelevante de la cuantía, etc.

Basándose en estos ejemplos, hay que mencionar una segunda experiencia en materia de reglamento de los diferendos en el ciberespacio: el "Cibertribunal"[23]. Empezada por la Facultad de derecho de la Universidad de Montreal en septiembre de 1996, esta experiencia se basa en el ejemplo del Virtual Magistrate para guiar su desarrollo. Pero, por empezar, el Cibertribunal beneficia de particularidades interesantes: por ejemplo, tiene la especificidad de ofrecer un servicio en francés e inglés.

Además, el Cibertribunal es el producto de una institución ubicada en un país de derecho mixto, cuyos juristas están enfrentados, de cerca o de lejos, a un biculturalismo jurídico. Esta doble influencia del derecho neorromanista y del Common law, es muy importante en un ámbito propenso a la comparación y al internacionalismo. Estas dos particularidades no dejan de ser importantes, si retomamos la afirmación

[22] Virtual Magistrate Project, www.vmag.law.vill.edu:8080/.
[23] www.Cybertribunal.org

trillada que las fronteras geográficas ya no existen, y que son remplazadas por fronteras culturales. El idioma y el derecho seguramente constituyen ejemplos de estas nuevas barreras que hay que tomar en cuenta.

Además de estas diferencias con el Virtual Magistrate, el Cibertribunal tiene un campo de aplicación más amplio. Aunque existen limitaciones inevitables, estas son mínimas: en primer lugar, solo se dictará sentencia en los casos en donde todas las partes hayan consentido a someterse a este foro. Luego, el Cibertribunal no decide de las cuestiones de orden publico. Finalmente, solo maneja las cuestiones relacionadas con el derecho de las nuevas tecnologías de la información.

Otra distinción importante con el proyecto norteamericano es que el Cibertribunal favorece la mediación previa al arbitraje. Esta propuesta de "ciberjusticia" esta al tanto del espacio cibernético, y trata no sólo de reglamentarlo, sino también de darle más eficiencia. Según este acercamiento, hay que evitar la intrusión de lo jurídico, que molesta a los usuarios de Internet que reclaman más auto-reglamentación, para que el ciberespacio pueda encontrar un organismo susceptible de ofrecerle los mejores servicios, al pendiente de los usuarios.

2.2 Las fuentes substanciales

Después de estudiar las normas insistiendo en sus orígenes, trataremos de ubicar el fenómeno normativo en su globalidad. La comunidad produce tendencias que, por ser repetidas, logran constituir

guías normativas. Veremos en primer lugar las tendencias que propone la práctica contractual, y luego investigaremos los principios de derecho más generales.

2.2.1 La práctica contractual

En esta parte apreciaremos las estipulaciones contractuales que podemos encontrar normalmente, o que se encuentran a veces ausentes, en los contratos que vemos en Internet. Con este objetivo, revisamos varios contratos de manera aleatoria, utilizando el motor de búsqueda "Altavista"[24].

2.2.1.1 La realidad del comercio electrónico

El comercio electrónico se encuentra en plena expansión. Es impresionante observar la evolución exponencial del número de sitios creados desde 1993. Un crecimiento semejante es de preverse en el valor de las transacciones comerciales a corto y largo plazos[25]. Sin embargo, este enorme potencial económico no se puede concretizar debido a un miedo real por parte de los usuarios.

Algunos estudios han sido publicados, y la seguridad parece ser la barrera más importante a la realización de contratos en línea[26]. Los

---

[24] www.altavista.digital.com.

[25] Se prevé que durante el año 2000, se venderán el equivalente de mas de 100 mil millones de dólares en productos en la red: www.cc.gatech.edu/gvu/user-surveys/survey-10-/996/.

[26] "Online Transactions: Risks and Options", www-personal.umich.edu/-sgupta/hermes/survey3/transact.html. Véase por ejemplo, en la pagina 1, donde se indica que 56% de las personas interrogadas consideran el problema de la seguridad como primordial.

usuarios miran, pero no compran mucho. Esto es más cierto aún cuando la transacción requiere la comunicación de informaciones acerca del pago. Una verdadera psicosis se manifiesta entonces, no siempre justificada, y los usuarios dicen tener más confianza en medios de comunicación tan poco seguros como el fax o el teléfono.

Si nos enfocamos en el contenido jurídico de los "contratos" en Internet, nos damos cuenta que el lugar que ocupa el derecho como herramienta para lograr la seguridad buscada es bastante discreta. Aunque es difícil atribuir porcentajes, podemos decir que la mayoría de los contratos que se forman en Internet contienen muy pocas estipulaciones de carácter jurídico. Prácticamente, muy a menudo una sola orden de pedido es llenada por el cliente quien la manda cliqueando en un icono, o escribiendo un correo electrónico por medio de un hipertexto predeterminado.

Los hombres de negocios, en Internet o en otros ámbitos, olvidan que la convención efectuada de esta manera constituye un acto jurídico. La trivialidad del intercambio, y la convivialidad de la comunicación desacralizan la operación. Nos encontramos cerca de una venta entre personas físicamente presentes, donde la transferencia del objeto es el elemento formal del convenio.

2.2.1.2 La naturaleza de los contratos

Es posible identificar tres grandes tipos de contratos disponibles en los nuevos ambientes electrónicos: el contrato de venta de bienes materiales, el contrato de servicios, y las licencias de utilización.

El contrato de venta de bienes materiales se reconoce por su facilidad de apreciación. Es un concepto bien conocido que podría ilustrarse por la venta de un disco compacto, de un libro, etc. Las nuevas redes de comunicación sólo son el medio de comunicación (y no el medio de intercambio del objeto). Encontramos también un caso particular de alquiler de bienes materiales[27] (en este caso Internet solo juega el papel de transmitir la información para la realización del contrato).

En segundo lugar, encontramos los contratos de servicios: es el contrato por medio del cual una persona se compromete a realizar una obra material o intelectual a cambio de un precio que la otra parte se compromete a pagarle. Podemos pensar por ejemplo en el contrato de publicidad.

Finalmente, existen las licencias de utilización que abarcan las obras del espíritu. Por ejemplo, el caso de un usuario que paga una cuota para tener acceso a una foto, un sonido, etc.

Esta noción de licencia plantea sin embargo algunos problemas en la medida en que nos enfrentamos a un concepto de derecho de autor que no cabe en el derecho común. Una licencia normalmente considerada como un derecho de utilización abarca más y más la cesión de derechos parciales. La doctrina clásica consideraba que había que distinguir entre licencia y cesión de derechos (acercándose así del concepto de venta); los autores más contemporáneos consideran que la distinción no es pertinente.

[27] Existe varios tipos mas de contratos en el Internet, como por ejemplo los de deposito, las subastas, y los contratos de intercambio.

La importancia de esta clasificación puede llegar a ser fundamental en la medida en que algunos textos de protección del consumidor establecen la lista de contratos a los cuales se aplican, de manera exhaustiva. Sin embargo esta cuestión sigue siendo teórica en muchos casos, en la medida en que los regímenes cubiertos por esto textos tienden a ser similares.

2.2.1.3 La deficiencia de las prácticas contractuales

Si es cierto que la práctica contractual es a menudo una fuente importante de información en el ámbito del comercio en general, hay que ser más prudente con esta afirmación en el caso del comercio electrónico. El carácter novedoso de este procedimiento de comunicación no siempre brinda la madurez que uno podría esperar de la práctica. Al contrario, cabe constatar la incongruencia de algunas cláusulas, como también la falta de estipulaciones específicas a la comunicación electrónica.

Entre los contratos que hemos repertoriados, la gran mayoría son contratos susceptibles de interesar al público en general. Nos encontramos en presencia de contratos de consumo, es decir muy dependientes del orden publico nacional a los que pertenecen. Obviamente, estos contratos, más que los entre comerciantes, deben responder a los imperativos impuestos por las disposiciones nacionales. Podemos identificar por lo menos dos ejemplo en los que el contrato podría estar en conflicto directo con las normas "extra-contractuales" aplicables en la práctica.

El primer ejemplo tiene que ver con las cláusulas aplicables en los contratos de consumo. Aunque estas cláusulas solo se encuentran en una minoría de casos identificados en el ciberespacio, algunos contratos

redactados por el comerciante, mencionan que el derecho aplicable será el derecho de su país.

Es necesario interrogarse sobre la legalidad de este tipo de estipulación, visto que los tratados, las leyes o la jurisprudencia las prohiben. En relación con los textos formales acerca de esta cuestión, podemos citar, por ejemplo, el artículo 5 de la Convención de Roma de 1980[28], y las convenciones de Bruselas[29] y Lugano[30], que prevén que no se puede privar el consumidor de las disposiciones de su derecho nacional cuando existe una de las tres condiciones mencionadas. Aunque estemos hablando aquí de un alcance casi exclusivamente europeo, varios países extra europeos tienen en su derecho interno, disposiciones semejantes o comparables.

Si hacemos un análisis literal de ellos, no parece para nada evidente que estas condiciones se aplican a la situación de Internet[31]. En este caso, las cláusulas aplicables en un contrato de consumo serían totalmente válidas. Sin embargo, desde un punto de vista más teleologico, parece claro que estos textos tenían como objeto proteger las situaciones en las cuales la vulnerabilidad de los consumidores es más evidente. El mundo del comercio electrónico necesita seguridad: el hecho de no poner el

---

[28] El articulo 5 menciona que la elección por las partes del derecho aplicable no puede tener como resultado privar el consumidor de la protección otorgada por las leyes de su país de residencia: si el consumidor hizo en este país los tramites necesarios para la conclusion del contrato; o si el comerciante recibió la orden de pedido en ese país; o si el consumidor compro en otro país, pero por incitación del comerciante. En estos casos, los contratos son regidos por las leyes del país de residencia del consumidor.

[29] "Convention concernant la compétence judiciaire et l'exécution des décisions en matiere civile et commerciale du 27 septembre 1968", citada en Gaudemet-Tallon, H., *Les conventions de Bruxelles et Lugano*, Coll. Droit des Affaires, Paris, LGDJ, 1993, p. 330. Ver los articulos 13 a 15.

[30] "Convention concernant la compétence judiciaire et l'exécution des décisions en matiere civile et commerciale du 16 septembre 1988", citada en Gaudemet-Taillon, H., *id.*, p.370. Ver los articulos 13 a 15.

[31] Una de las condiciones para que se pueda poner en tela de juicio una cláusula de derecho aplicable, es que el pedido del consumidor se haya recibido (por parte del vendedor) en el país del consumidor. Como con Internet, no existen limites geográficos, esta condición, entre otras, parece difícilmente realizable.

consumidor en presencia de su propio derecho nacional es un elemento en su contra, y los textos aplicables que acabamos de mencionar conllevan una duda que alimenta esta inseguridad.

Otro ejemplo de cláusula incompatible con el derecho aplicable y que seguido encontramos en los contratos del ciberespacio, es el de las cláusulas de limitación o exoneración de responsabilidad. Veamos este ejemplo según el derecho norteamericano[32]. La práctica, en muchos casos, es que esta cláusula, redactada por el vendedor (o el que presta sus servicios), excluye cualquier tipo de responsabilidad para los daños que pudieran ocurrir en el uso del producto.

Hay que saber que sin importar la situación, los artículos del *Uniform Commercial Code* que refieren a las nociones de "fitness", "merchantability" o "express warranties", se aplican[33]. También, es imposible en derecho norteamericano poner en tela de juicio las obligaciones de buena fe, diligencia, razonabilidad y cuidado[34]. Excepto estos casos de orden público, el comerciante podría limitar su responsabilidad en relación con las garantías implícitas (implied warranties)[35]. Habría también que tomar en cuenta el *Magnusson Moss Warranty Act* (1975)[36], que es una referencia básica en el derecho norteamericano del consumo. Este texto federal se aplica especialmente para proteger los consumidores de los vendedores (warrantors of products)[37].

---

[32] Cabe subrayar que existen disposiciones muy similares en cada derecho nacional.
[33] Los artículos 2-314, 2-313, y 2-302 UCC cubren específicamente estos conceptos de estado de la mercancía, bien comercial, y garantías expresas.
[34] Articulo 1-102(3) (1990) UCC.
[35] Artículo 2-315 UCC, que menciona que cuando el comprador depende del juicio del vendedor para seleccionar la mercancía, existe una garantía implícita que los bienes serán adecuados.
[36] 15 USC parr.2301, 88 Stat. 2183 (1975)

Además de estas incompatibilidades, hay también que constatar que, en muchos casos, existen muy pocas cláusulas específicas en relación con la comunicación por medios electrónicos. Por ejemplo, es posible mostrar en algunos casos que el contrato que se les proporciona a los usuarios de Internet ha sido simplemente "escaneado", y más probablemente es una reproducción de una versión en papel, que no se dirigía a las transacciones electrónicas.

En suma, como lo mencionábamos anteriormente, son raros los contratos que contienen una cláusula acerca del derecho aplicable. La ausencia de límites geográficos en el ámbito del Internet permite sin embargo la formación de contratos internacionales. A pesar de nuestras interrogaciones acerca de la validez de estas estipulaciones en relación con los contratos de consumo, se trata sin duda de una precaución muy sencilla que permite evitar conflictos a veces complicados de resolver en los contratos entre comerciantes[38].

Tampoco existe ningún procedimiento "formal" idóneo en relación con la formación del contrato. Claro, el contrato generalmente no requiere condiciones particulares de forma. Sin embrago, podría preconizarse, como en materia de EDI, un procedimiento de acuse de recibo y de confirmación del pedido. Esto sería de hecho facilitado por la rapidez del medio.

Otra ausencia es el hecho que los contratos nos mencionan como resolver la situación en la que un daño ocurriera como consecuencia de un error o un problema de transmisión de la información. De la misma manera,

---

[37] Véase, para unos ejemplos de cláusulas aplicables en el ciberespacio: Greguras, F., "Electronic Commerce: On-line Contract Issues", www.batnet.com/oikoumene/ec_contracts.html, p.12.

[38] Si no existe estipulación expresa, el criterio utilizado generalmente es la conexidad entre el contrato y el derecho aplicable. Véase por ejemplo el articulo 4 de la Convención de Roma de 1980.

casi no se encuentran cláusulas de responsabilidad en el caso de no comunicación de la información transmitida.

Finalmente, raros son los contratos que mencionan la especificidad de las firmas y los escritos electrónicos. Como no benefician del mismo trato según los sistemas jurídicos, sería pertinente insertar una cláusula según la cual un acto particular equivaldría a una firma o un escrito. Esto puede resultar importante especialmente en el ámbito del derecho del consumo donde varios derecho nacionales imponen estas exigencias. Además de estos elementos de validez del contrato, sería útil prever una cláusula relativa a la organización de la prueba de la transacción entre las partes, y esto especialmente cuando la transacción involucra comerciantes.

2.2.2 Los principios generales del derecho y las costumbres

Vimos, en la sección precedente, normas que son el producto de instituciones bien determinadas (Ley-modelo de la CNUDMI, convenciones internacionales, etc.). Aquí, el problema es distinto. Se trata de apreciar el poder de la comunidad cibernética de crear principios exclusivos del comercio electrónico.

Al principio, como lo vimos, puede parecer presuntuoso hablar de principios relativos a un campo que dispone de una existencia limitada. Prácticamente, los principios corresponden a menudo a una acción de cristalización que necesita tiempo y reconocimiento. Por ejemplo, en

derecho mercantil internacional, solo se ha podido identificar algunos principios, a pesar de la amplitud de la materia[39].

Pero, antes que todo, hay que tratar de circunscribir la noción de principios generales del derecho. Según Emmanuel Gaillard, existen dos acercamientos fundamentales. El primero es el dónde los usos "solo permiten, sin importar el derecho aplicable, interpretar la voluntad de las partes. Su papel es entonces, meramente supletorio"[40]. El segundo es más amplio y mientras abarca "las prácticas contractuales normales, también incluye las verdaderas reglas del derecho que se desprenden de la observación del derecho comparado o de otras fuentes internacionales. Los usos se confunden entonces en parte con los principios generales del derecho mercantil internacional"[41]. Los que se oponen a esta teoría plantean una pregunta interesante, acerca del alcance de los usos, y quieren determinar si son "voluntarios" o "normativos". No parece que se pueda encontrar una vía mediana.

Por empezar, la descripción de Emmanuel Gaillard acerca de la primera concepción, es decir el papel de los usos como forma de interpretación de los contratos, parece distinta de los ejemplos que proporciona. También, es obvio que la previsibilidad del negocio impone cierta seguridad acerca de los criterios necesarios a la determinación de los usos vigentes. Si existe silencio de las partes, como suele suceder, nos parece sano y justo remitirnos a lo que ocurre en la comunidad comerciante. La imbricación constante de los interventores entre ellos y la

---

[39] Véase: Mustill, M. "The New Lex Mercatoria: The First Twenty Five Years", (1988)
4 *Arbitration International*, p.86

[40] Véase Gaillard, E., "La distinction des principes généraux du droit et des usages du commerce international", *Etudes Pierre Bellet*, Paris, 1993, pp..203-206.

[41] *Id.*, pp.206-207.

fuerza del orden cibernético son las razones que motivan una mayor integración comunitaria en la esfera contractual.

Pero más allá de esas dimensiones teóricas, sobre el contenido de los usos como sobre su origen, es posible identificar, además de las fuentes institucionales que ya citamos, algunas normas producidas por la misma comunidad. Estas reglas conforman la "Netiqueta" a la cual nos referimos anteriormente en este trabajo. Como es fácil imaginárselo, esta expresión no siempre es bien recibida. Además de que la práctica no es muy convincente, como lo acabamos de ver, y el derecho es un poco refractario a la informalidad de las normas, la novedad de nuestro campo de estudio no facilita su cristalización. A pesar de estas importantes limitaciones, la Netiqueta se refiere normalmente a reglas sustanciales que las redes crean globalmente. Son el producto de varios ordenes que disponen de sus propios medios de coerción.

Si en nuestra búsqueda de juridicidad, la idea de que interfiera el concepto de comunidad nos parece interesante, sin embargo hay que delimitar su contorno con el fin de crear un nexo entre ella y los individuos que la conforman. Sin duda, Internet no es un grupo monolítico. Por lo mismo, más cerca estaremos de definir un grupo, más sencillo resultará determinar sus normas. Por esta razón es difícil utilizar la noción de "Netiqueta". Hay que constatar que el fruto de las fuentes estudiadas sigue siendo insuficiente.

Sin embargo, en el ámbito del comercio electrónico, tal vez sea más fácil determinar los actores y sus intereses. Además, el espíritu de cooperación característico de los negocios obliga a los interventores a reconocer los intereses de grupos concurrentes, como los consumidores o

los utilizadores. Este espíritu de conciliación, esta identificación más fácil de los grupos y de los intereses, son elementos favorables a la aparición de reglas eficaces en la comunidad mercantil. Los elementos existen, aunque todavía falta cierta madurez.

Capitulo 3:
Los sistemas de pago

Uno de los factores de importancia capital cuando pensamos en el mercado potencial que representa el comercio electrónico, es la definición de los métodos de pago más adaptados a Internet.

3.1 Los tipos de pago

Los usuarios de Internet tienen actualmente a su disposición los métodos de pago siguientes: el depósito en cuenta bancaria, la tarjeta de crédito, y el sistema de dinero electrónico. Las preocupaciones esenciales

relacionadas con estos distintos métodos son la protección de los datos y la preservación del anonimato[42].

3.1.1 El depósito en una cuenta bancaria

Es posible efectuar en Internet un depósito en una cuenta bancaria tradicional. Si beneficiamos de un servicio bancario en línea, es posible dirigir al banco una orden de depósito vía Internet. Sin embargo, esto se considera una transacción bancaria normal.

En este tipo de operación, el banco del deudor ejecuta la orden de éste de creditar la cuenta del beneficiario por el monto de la transferencia, según las condiciones normales del contrato relativo al sistema de depósito bancario: el banco del deudor transmite la petición al banco del beneficiario, sin comprometer su propia responsabilidad en relación con el éxito de la operación.

En el caso de este tipo de pago, la protección de los datos es muy cuestionable visto que la transmisión de las órdenes se hace vía Internet[43]. El conjunto del procedimiento requiere tiempo y ocasiona cuotas adicionales en el caso de transacciones transfronterizas.

---

[42] Sobre este tema, véase Benoussan, A. (Dir.), *Le commerce électronique. aspects juridiques*, Paris: Hermes, 1998, p.167.

3.1.2 La tarjeta de crédito

El método de pago más común actualmente es el pago con tarjeta de crédito. En las transacciones de comercio electrónico, el comprador de bienes o servicios transmite al vendedor su número de tarjeta de crédito. Cuando el vendedor ha recibido este número, la transacción se parece a una operación normal con tarjeta de crédito: el vendedor recibe su pago del banco emisor de la tarjeta, y éste le cobrará al consumidor el monto de la transacción en una fecha ulterior.

Si tomamos en cuenta que actualmente los números de tarjetas de crédito son normalmente mandados sin encriptación, el riesgo asociado con este tipo de pago es evidente. El riesgo no solo esta presente en el momento de la transmisión del número de la tarjeta de crédito, sino también al nivel de las computadoras de los comerciantes o de los proveedores de servicio, que pueden ser fácilmente el blanco de los piratas informáticos.

Más allá de los riesgos relacionados específicamente con el uso del Internet, los vendedores deben estar informados de los riesgos inherentes al pago por tarjeta de crédito: en las transacciones realizadas por Internet que involucran números de tarjetas de crédito, los términos y condiciones generales del contrato entre el establecimiento emisor de la tarjeta y los vendedores, que son la condición primordial de validez de una operación con tarjeta de crédito, no se encuentran satisfechos. Por ejemplo, si el tarjetahabiente niega la existencia de una transacción, el vendedor no tiene la posibilidad de mandar verificar la operación ya que no tiene la impresión de la tarjeta y la firma del tarjetahabiente.

---

[43] Schelling, J., *Cyberlaw Canada*, Vancouver: Self-Counsel Press, 1998, p. 58.

En tales casos, el comerciante puede verse obligado a regresar el dinero que recibió del banco emisor, y esto podría llevarlo a entablar una demanda contra el tarjetahabiente con el objetivo de recuperar su dinero. El vendedor tendría entonces la carga de probar que el tarjetahabiente era verdaderamente una de las partes en la transacción realizada en Internet, y esto podría resultar difícil. Además, el riesgo de la insolvabilidad del tarjetahabiente es siempre presente.

Para enfrentarse a los riesgos asociados al pago con tarjeta de crédito en Internet, las sociedades First Virtual Holding Inc., y Cyber Cash Inc., han desarrollado servicios de suplemento. En los dos casos, una precondición para que se pueda realizar el pago es que el tarjetahabiente y el comerciante hayan concluido un contrato con First Virtual Holding / Cyber Cash: en el caso de un pago que utilice First Virtual Holding, el tarjetahabiente da al vendedor un código que le ha sido atribuido por First Virtual (el "VirtualPIN"). El vendedor manda este código a First Virtual, indicando el monto que hay que cobrar. First Virtual se asegura de la realidad de la transacción, entrando en contacto con el tarjetahabiente por correo electrónico. First Virtual atribuye entonces el cargo a la tarjeta de crédito, y paga el vendedor. Con este sistema, las informaciones sensibles como los números de tarjetas de crédito no transitan por Internet, y las informaciones no necesitan ser encriptadas.

Al contrario, con Cyber Cash[44], los números de tarjetas de crédito pasan por Internet y consecuentemente, la criptología desempeña un papel decisivo. El tarjetahabiente transmite al vendedor en forma criptada, su número de tarjeta de crédito acompañado de su código de identificación que

le atribuyó Cyber Cash ("WalletID"). El vendedor, sin descifrar los datos que recibió, agrega los elementos relativos a la transacción, y regresa el conjunto a Cyber Cash. La misma compañía reformatea los datos y los transmite al tarjetahabiente para su aprobación. Si consiente, se le hace el cargo a su tarjeta.

3.1.3 El "dinero electrónico"

El "dinero electrónico" constituye la gran innovación en materia de pago en Internet. Este dinero electrónico esta conformado por un conjunto de datos numéricos que representan cierto valor monetario. Hay que distinguir dos tipos de dinero electrónico: el que se encuentra almacenado en el disco duro de la computadora del usuario (tipo "software") y el que esta almacenado en un chip electrónico de una tarjeta de memoria (tipo "hardware").

En octubre de 1997, la Deutsche Bank empezó un proyecto piloto llamado "ecash"[45], que utiliza el sistema de pago en dinero electrónico de tipo software desarrollado por Digicash. El cliente de un establecimiento bancario que desea utilizar el ecash tiene que abrir primero una cuenta ecash además de su cuenta normal, y transferir cierta suma de su cuenta tradicional hacia su cuenta ecash. Cuando luego efectúa un retiro en línea de "unidades ecash" de esta cuenta, y almacena estas unidades en su computadora, el monto es retirado de su cuenta ecash. El banco internamente, pone en reserva el ecash retirado en un "fondo común ecash"

---

[44] Véase el sitio www.cybercash.com.
[45] Para un estudio mas detallado, véase: Benoussan, A., *op cit.*, p. 179.

en el cual viene almacenada la globalidad de los montos retirados por todos los clientes del banco, hasta el pago final.

El cliente tiene entonces la posibilidad de pagar sus compras realizadas en Internet con unidades ecash, en el caso de un comerciante que también tenga una cuanta ecash. Cuando el vendedor recibe un pago en ecash de su cliente vía Internet, el manda las unidades recibidas al establecimiento bancario emisor para verificar su validez. Cuando se haya completado la verificación, el vendedor puede elegir entre pedir la conversión en dinero del ecash recibido, o hacer un depósito en su propia cuenta ecash.

Para preservar el anonimato, el sistema ecash utiliza la técnica de la "firma ciega"; las unidades ecash no son creadas en el banco sino en la computadora de cada usuario por medio de un programa ecash. Cada "paquete" de unidades es creado de tal forma que un número de serie especifico le es atribuido y es mandado al banco de manera criptada (en un "sobre numérico") cuando el cliente desea "retirar" dinero electrónico de su cuenta ecash. El banco otorga validez a las unidades ecash utilizadas, firmando con una clave secreta numérica a través del sobre numérico sin abrirlo, y los regresa a su cliente ("retiro"), debitando la cuenta ecash del cliente de un monto equivalente con este método. El banco no tiene la posibilidad de identificar las unidades en las cuales puso su firma.

Otra característica del ecash es la regla del "primero en tiempo, primero en derecho". Por el carácter anónimo del ecash, el banco emisor que recibe las unidades del vendedor solo es capaz de reconocer la autenticidad de su propia firma numérica y el número de serie de cada unidad. Para impedir la posibilidad de copiar unidades ecash, existe una

regla que obliga a que cada número de serie sólo se pueda utilizar una vez. Esto implica que un pago hecho en unidades ecash auténticas podrá ser rechazado si ya se utilizaron copias fraudulentas de estas unidades.

La "GoldKarte", puesta en el mercado por establecimientos bancarios alemanes, constituye un ejemplo de monea electrónica de tipo "hardware" que ya es realidad. Las tarjetas bancarias tradicionales, como la tarjeta "EC", ya son equipadas con chips electrónicos "IC", en los cuales el tarjetahabiente puede instalar datos digitales que representan un valor monetario de hasta 400 Deustche Marks, en las terminales de cargamento de cualquier banco, donde el monto correspondiente al cargamento será deducido simultáneamente de su cuenta bancaria. El pago con la GoldKarte puede ser efectuado off-line en las tiendas equipadas de terminales con lectores apropiados: los datos equivalentes al monto de la compra son deducidos del chip electrónico de la GoldKarte y cargados en la terminal. Estos datos son almacenados y mandados diariamente en línea al banco del comerciante.

Desde el punto de vista de la seguridad, una de las particularidades de este sistema es construir una cuenta "virtual" para cada Goldkarte. La cantidad de datos cargados en el chip y utilizados, es grabada en esta cuenta virtual, que al principio tiene un saldo nulo. Si el saldo de esta cuenta virtual llega a ser negativo, esto significa que se copiaron los datos y que un número más importante que el que fue inicialmente cargado, ha sido utilizado.

Acerca de los pagos en dinero electrónico, el riesgo siempre existe en teoría que el disco duro de la computadora o el chip electrónico de la Goldkarte del usuario estén dañados y que los datos cargados en ellos no

puedan ser recuperados, que los datos que transitan en Internet sean mandados por error a un tercero no identificado, o que piratas informáticos accedan ilegalmente a las computadoras de los usuarios.

3.2 Calificación jurídica del dinero electrónico

Para poder comprender el alcance del funcionamiento del dinero electrónico, es menester preguntarnos como el derecho concibe los nuevos métodos de pago, y la naturaleza de la relación que existe entre el banco y el cliente.

3.2.1 Adecuación del derecho a los nuevos métodos de pago

¿Cómo deberían las reglas actuales del derecho civil y mercantil aplicarse a los nuevos métodos de pago de la generación Internet? Una de las principales preguntas que existen es de saber si hay que considerar el dinero electrónico como un crédito no inscrito para con el banco, resultado del reconocimiento de una deuda abstracta (como lo manejan los artículos 780 y 781 del Código Civil alemán), o más bien como un título al portador (artículos 793 y 797)[46].

En el primer caso, se trata de un crédito basado en una relación deudor–acreedor entre ciertas personas. Consecuentemente, si la calificación jurídica del dinero electrónico se percibiera de esta forma, el banco tendría que pagar al beneficiario de la transacción solamente en la

[46] Véase: Trudel, P., *Droit du cyberespace*, Montreal: Ed. Thémis, 1997, p.446.

medida que la hubiera notificado de la transferencia entre el antiguo detentor del dinero electrónico, y el nuevo. Esta situación no es compatible con el anonimato que es una característica del dinero electrónico, ya que el banco tiene que pagar la presentación de dinero electrónico lícito, sin importar si conoce o desconoce su procedencia. Además, si el dinero electrónico tuviera este reconocimiento, existiría una protección muy limitada acerca de la buena fe en el momento de la transferencia. Esto sería una barrera enorme a su facilidad de circulación.

El dinero electrónico puede considerarse como un título al portador. El problema radica en el hecho que el dinero electrónico no llena los requisitos de un documento, y entonces no puede ser inscrito. El dinero electrónico es sin embargo muy parecido a un título al portador: el banco tiene que pagar a cualquiera que presente dinero electrónico sin tener que cuestionar su procedencia; además para su transferencia, la atribución inmaterial no es suficiente para cederlo: la posesión tiene que ser entregada al beneficiario. En Alemania, por ejemplo, las disposiciones pertinentes del Código Civil relativas a los títulos al portador se aplican, *mutatis mutandis*, al dinero electrónico.

3.2.2 Calificación jurídica de la relación banco-cliente

El cliente puede libremente transferir el monto que desea de su cuenta bancaria a su cuenta ecash, y al revés, utilizando un orden de giro bancario normal. Las relaciones entre el banco y su cliente, para una cuenta de dinero electrónico, son idénticas a las de una cuenta normal.

Lo que hay que determinar es si hay que considerar las relaciones entre un banco y su cliente acerca del retiro de unidades ecash, como una venta o como un contrato de servicio de gestión remunerado bajo el cual el banco tiene que inscribir el monto de unidades ecash validas en crédito de la cuenta de la persona que las presenta en una fecha ulterior, o en el momento de la venta.

En el primer caso, el débito inscrito en la cuenta del cliente cuando retira unidades de pago ecash, debería considerarse como un pago anticipado relativo a los costos inherentes a la ejecución de los servicios en gestión.

Esta calificación como contrato de servicio de gestión remunerado no es congruente con el siguiente elemento: cuando el cliente retira unidades ecash de su cuenta ecash, no hay manera de saber quien presentará cada unidad al banco. Cuando las unidades de pago son finalmente presentadas al banco para su pago, por el anonimato de las unidades, el banco no puede determinar de cual cuenta provienen. Es el cliente quien asume solo los riesgos asociados a la pérdida de unidades ecash. La inscripción al débito de la cuenta del cliente, del monto de un retiro de unidades ecash en el momento de este retiro, debería ser definitiva. El retiro de unidades ecash de la cuenta del cliente debería ser considerado como una venta de la cual obtiene dinero ecash, es decir un título al portador numérico, cuyo precio él paga en contraparte al debitar el mismo monto de su cuenta ecash.

3.3 Enfrentarse a los riesgos

Para proteger los sistemas de pago utilizados en Internet, se esta haciendo varios esfuerzos basados en la protección contra la falsificación, la certificación ante terceros de confianza, y el uso de la criptografía.

Sin embargo, los usuarios de Internet no deben ni pueden contar con el desarrollo de la tecnología y del derecho para erradicar los riesgos. La lucha entre la "buena" y la "mala" tecnología es sin fin, y las leyes son generalmente consecutivas a la aparición de los problemas.

Cada usuario de Internet tiene que identificar con mucho cuidado los riesgos asociados con cada método de pago, y enfrentarse a ellos dentro de su autonomía, es decir a través de convenios razonables – términos generales y condiciones – con la otra parte contratante. Por ejemplo, las condiciones generales de las cajas de ahorro en Alemania estipulan que los valores monetarios cargados en el chip electrónico de una GoldKarte extraviada no serán reembolsados a los usuarios, mientras el convenio que existe entre las federaciones de establecimientos bancarios estipula que el banco emisor de una Goldkarte tiene que pagar una transacción realizada por medio de dinero electrónico falsificado.

Es también necesario tener en cuenta las varias reglas de cada jurisdicción, especialmente las que tienen que ver con protección del consumidor.

Capitulo 4:
La prueba y el comercio electrónico

El comercio electrónico descansa en dos características que conducen a un trastorno de las prácticas jurídicas tradicionales: si el comercio tiende a comercializarse desde hace unas décadas, el comercio es Internet es el "global village" que anunciaba hace más de 20 años el sociólogo estadounidense Marshall Mc Luhan. El comercio electrónico significa también una desmaterialización total de las relaciones, los clientes y los comerciantes no se ven, la transacción no puede materializarse por la firma de un escrito y los métodos tradicionales de pago (efectivo, cheques, firma de una factura, etc.), son obsoletos.

Para los juristas, el reto que pone el comercio electrónico consiste en tener que inventar nuevos métodos de prueba aceptables en el plano

internacional, tomando en cuenta esta doble constatación: el comercio electrónico, a raíz de la desmaterialización de las relaciones que provoca, requiere pruebas adicionales que son inútiles en el comercio tradicional[47]; porque los métodos de prueba tradicionales son totalmente inadaptados a la desmaterialización de las relaciones.

Después de identificar los obstáculos al comercio electrónico creados por los sistemas jurídicos tradicionales, los prácticos del derecho deben, en la espera de legislación apropiada, inventar soluciones prácticas para reforzar la seguridad del comercio electrónico.

4.1 Un sistema probatorio tradicional inadecuado

Es necesario que nos demos cuenta que los sistemas probatorios en un gran numero de Estados siguen siendo mal adaptados a las necesidades del comercio electrónico, ya que varios obstáculos complican su desarrollo.

4.1.1 Los dos sistemas probatorios existentes

Los regímenes de prueba vigentes en los distintos países descansan generalmente en los principios básicos del sistema anglosajón de la Common law, o en los principios básicos del derecho neorromanista de Europa continental.

[47] Cuando uno compra un disco compacto en una tienda, que paga inmediatamente en efectivo, las partes no tienen necesidad de preconstituirse ninguna prueba. Si el mismo disco compacto es comprado en Internet, la seguridad de la transacción supone el uso de un sistema probatorio complejo.

4.1.1.1 El Common law

El sistema anglosajón da a las partes una facultad de iniciativa importante en la búsqueda y la presentación de la prueba. Las varias técnicas de "discovery" que ofrece este sistema facilitan considerablemente la búsqueda de la prueba. De esta forma, la comunicación de los elementos de prueba y los interrogatorios dan a las partes la oportunidad, entre otras cosas, de estudiar los documentos que la parte contraria quiere presentar durante el juicio, o interrogar a la parte adversa. Este mecanismo preliminar permite a las partes obtener de su adversario hechos e informaciones relacionados al caso, que les ayudan en la preparación del juicio, les permite conocer más profundamente el expediente, o llegar a un acuerdo.

Existen básicamente tres tipos de pruebas en el derecho anglosajón: la prueba testimonial, que es la declaración de testigos bajo juramento y que se considera como el método privilegiado de prueba en esta familia jurídica; la prueba literal, que consiste en la presentación de un escrito a la corte, y la prueba material, es decir la prueba que se basa en objetos materiales, y que hay que disociar de las declaraciones de los testigos acerca de dichos objetos.

Estos tres tipos de prueba son, por naturaleza admisibles mientras presentan un interés en relación con la litis, son pertinentes, es decir auténticos y con valor probatorio, y que no son excluidos por reglas especiales. Las tres barreras principales para la admisibilidad de las pruebas literales son la autenticidad, la regla de la "mejor prueba" y la regla de la prohibición de la prueba por testimonio de oídas.

En un sistema jurídico de Common law, la primera dificultad que plantea el uso de documentos informáticos como método de prueba es la autenticidad de tales documentos. Esto causa un problema en materia de comercio electrónico. Por empezar, el documento no es manuscrito. Además, los datos informáticos no son inalterables. Los datos introducidos en una computadora por una persona pueden ser modificados por otra persona, y hasta por la misma computadora cuando guarda automáticamente los datos. Es por eso que la doctrina y la jurisprudencia han considerado estos documentos informáticos como inadmisibles en la medida en que nadie puede atestiguar su autenticidad, visto el número de personas que tomaron parte en su creación.

La prohibición de la prueba por testimonio de oídas constituye también un obstáculo a la producción de documentos informáticos como método de prueba. El fundamento esencial de la exclusión de la simple prueba por testimonio de oídas es la imposibilidad por la parte contraria de interrogar al autor de la declaración. Sin embargo, la regla de la prueba por testimonio de oídas no se aplica cuando el documento forma parte de la "business records exception" (excepción para los archivos comerciales), y hasta ha sido totalmente abolida en algunos de los principales países de Common law, como el Reino Unido.

Además, en virtud de la regla de "la mejor prueba", un escrito no es, normalmente, aceptable a menos de ser presentado en su versión original. Para los documentos informáticos, esta obligación de presentar el original es difícil de respetar, visto que el original es definido como el conjunto de datos contenidos en la memoria de la computadora, y la impresión que produce la maquina es una simple transcripción de estos datos.

Como estas reglas de principio se oponen a la admisibilidad de los documentos informáticos como método de prueba, el legislador y las jurisdicciones anglosajonas han buscado mediante unos suavizamientos legislativos y una evolución de la jurisprudencia, aceptar más fácilmente los documentos informáticos como métodos de prueba admisibles.

4.1.1.2 La familia neorromanista

Los sistemas que descansan en el derecho neorromanista atribuyen la carga de la prueba a una de las partes, el demandante, porque le corresponde a la persona que invoca un derecho, probarlo. En muchas jurisdicciones, con el afán de mantener una buena administración de la justicia, el juez puede – con el pretexto que todos tienen que cooperar para determinar la verdad – obligar una de las partes a presentar un elemento de prueba que detiene.

Por lo tanto, en Europa continental, Dinamarca es el único país que tiene un sistema con una total libertad de prueba. España y Portugal, como también Alemania, tienen en cambio un sistema de prueba legal. El derecho nacional determina los métodos de prueba que pueden utilizarse, y las condiciones de admisibilidad. Ningún otro método de prueba que el prescrito por la ley será aceptado.

Entre estos dos tipos de legislación totalmente distintos, Bélgica, Luxemburgo y Francia tienen un sistema de prueba mixto, según la naturaleza civil o mercantil de la transacción, y el monto más o menos

elevado de ésta. Italia, Holanda y Grecia se caracterizan por un régimen de libertad de la prueba con algunas excepciones en algunas materias.

En todos estos Estados, el escrito, si no es exclusivo, es la forma dominante de presentar la prueba.

4.1.2 Tres obstáculos

Si, independientemente de toda la legislación existente, intentáramos organizar los métodos de prueba necesarios para atestiguar la existencia de transacciones electrónicas, su contenido y la integridad de la información intercambiada, llegaríamos a la interpretación de un sistema que respondiera a las normas del intercambio electrónico de datos (EDI), donde las pruebas se basan en mensajes grabados y conservados por unos sistemas informáticos.

Pero la ejecución de este tipo de sistema se opone a tres principales obstáculos jurídicos: la exigencia frecuente de un documento escrito; la importancia que se le atribuye a la firma manuscrita en algunos regímenes de prueba; y la célebre regla según la cual la prueba de un acuerdo entre dos partes no puede ser constituida por una sola parte.

4.1.2.1 Documentos informáticos y el concepto de "escrito"

En el Reino Unido, la adopción de la Ley sobre prueba en materia civil (*Civil Evidence Act* – CEA) en 1995 ha quitado todos los obstáculos que se oponían a la presentación de documentos informáticos como prueba. La

CEA ha eliminado la prohibición general de la prueba por testimonio de oídas. En este contexto, la cuestión ya no tiene que ver con la aceptabilidad de los documentos electrónicos sino en el peso que los jueces darán al documento. Por lo tanto, todos los medios legales y prácticos que inciten a los tribunales a dar mas importancia a los documentos informáticos, son útiles.

En los Estados Unidos de Norteamérica, hace mucho que se ha utilizado la excepción a la prohibición de la prueba por testimonio de oídas para permitir la presentación de documentos informáticos sin que su autor tenga que testificar personalmente. Es suficiente el testimonio del encargado del sistema informático, o de cualquier otro empleado que conozca el sistema. Esta excepción, conocida bajo el nombre de "Business Records Exception" (excepción para los archivos comerciales), ha sido codificada en la *Ley Federal de 1975* (art. 803–6 del *Federal Rules of Evidence*), y la mitad de los estados han adoptado reglas similares. Sin embargo, una docena de estados, incluyendo California y Nueva York, han adoptado leyes que obligan al juez a verificar si el método y el momento de la grabación comercial pueden justificar su aceptabilidad.

Por lo que atañe a la regla del original, la noción de no disponibilidad ha sido interpretada de manera muy flexible, de tal forma que la presentación de documentos informáticos parece posible. Sin embargo, su aceptación depende de la posibilidad de demostrar su autenticidad e identificar su autor. Por lo tanto, si la aceptabilidad de los mensajes que respetan las reglas del EDI parece fácil, la fuerza probante del simple correo electrónico parece mucho más aleatoria. En los Estados Unidos de Norteamérica, algunas disposiciones requieren un escrito para que un documento sea valido o ejecutable. El *Statute of Frauds* especifica los

contratos que solo son ejecutables bajo la condición de haber sido materializados en un escrito firmado. La mayoría de los estados ha adoptado en su Common law o en su *Uniform Commercial Code* (UCC) las disposiciones del *Statute of Frauds*.

En varios países de la familia anglosajona, algunos tipos de contratos deben materializarse en un acto escrito y firmado para ser validos, como por ejemplo los contratos relativos al matrimonio y a la venta de bienes raíces. En el caso de la venta de bienes, el UCC, que ha adoptado su propio *Statute of Frauds* prevé que para que la venta de bienes de una cuantía igual o superior a $500 sea ejecutable, es necesario que se presente las cantidades de bienes vendidos.

Por lo tanto, se exige una prueba escrita para la mayor parte de los contratos. Sin embargo, la evolución de la jurisprudencia y una interpretación amplia de la noción de "escrito" han logrado ablandar estas reglas.

En el sistema jurídico alemán, el escrito es definido en el Código Civil como "la expresión de un pensamiento" en una "forma directamente legible". Algunos documentos informáticos son desde luego excluidos por esta definición, como por ejemplo los que contienen exclusivamente instructivos de programación. Pero según la jurisprudencia, estos documentos son considerados como "observaciones", es decir uno de los cinco métodos de prueba legales que, para ser aceptados supone que el juez llegue a la convicción que el documento es auténtico, gracias a "su propia percepción concreta". Entonces, si es cierto que este tipo de prueba no siempre tiene la calidad de escrito, si tiene algún valor probatorio.

En los sistemas jurídicos belga y francés, la prueba puede ser presentada libremente en materia comercial y civil mientras la cuantía en litigio no rebasa cierto monto[48]. Mas allá de esta cuantía, la prueba de los actos jurídicos es administrada por medio de un acto notariado, o un acto sin legalizar, es decir un documento escrito que contiene una firma original.

Para adquirir la calidad de una prueba perfecta, el escrito debe entonces necesariamente ser original y firmado. Sin embargo, el original del documento informático se apoya en un medio electrónico y no es, por naturaleza, accesible al sentido humano. Lo que se presenta en las cortes no es entonces el documento sino una copia de éste. La calificación de prueba perfecta parece entonces imposible para los documentos de origen informático.

Estas dificultades se encuentran también en el sistema jurídico belga. En efecto, la doctrina se encuentra dividida acerca del hecho de saber si la noción de escrito abarca el documento informático.

En algunas legislaciones, puede haber una excepción a la necesidad de producir un escrito en algunas circunstancias, como por ejemplo cuando nos encontramos en el caso de imposibilidad de encontrar un escrito, o cuando un escrito ha sido destruido, pero existe una copia fiel e infalsificable con respaldo informático[49].

Sin embargo, el recurso a estas excepciones solo raramente es una solución a la prueba en el comercio electrónico. Prácticamente, no es la

[48] 5,000 Francos franceses en Francia, y 15,000 Francos Belgas en Bélgica.
[49] El articulo 1348 del Código civil de Luxemburgo, por ejemplo, prevé que cuando una parte no conservo sus originales y presenta reproducciones micrograficas y grabaciones informáticas a partir de los originales,

imposibilidad de procurarse un escrito, sino una voluntad de deshacerse del escrito. Los documentos que uno desea utilizar para probar las transacciones electrónicas no son copia fiel e infalsificable de documentos escritos, porque nunca hay etapas anteriores que pasan por el escrito.

De la misma manera, el hecho de que se pueda derogar a la exigencia de un escrito, si uno dispone de un "comienzo de prueba escrita" no es una solución para el comercio electrónico en los países en los cuales el escrito es "un papel escrito" porque, en este caso, es muy difícil que se acepte un documento que no es en papel como un comienzo e documento en papel.

4.1.2.2 La exigencia de una firma[50]

En los países de Common law, la firma esta muy lejos de tener la misma validez que en los Estados de tradición neorromanista, y esto parece lógico visto que el escrito no es el modo de prueba predominante. En el Reino Unido por ejemplo, no es suficiente para autenticar el documento y probar en un juicio la autenticidad de su contenido – se necesitan otros elementos que conforman el "genuineness of authorship" (autenticidad de proveniencia). La firma electrónica es entonces y en principio, admisible, pero no tendría más validez que la firma manuscrita.

La firma de un documento, en la familia neorromanista, es a la vez un procedimiento de identificación que manifiesta la adhesión de quien la

---

tendrán la misma validez probatoria que los escritos de los cuales se presume que son una copia fiel, si llenan los requisitos previstos por reglamento.

[50] Para un estudio mas profundo del tema de la admisibilidad de la firma en el ámbito del comercio electrónico, véase el capitulo 5 de este trabajo.

inserta, y un elemento que manifiesta la adhesión de quien la utiliza. En la mayor parte de los países de tradición neorromanista, aunque esto no siempre resulte de la ley, la firma es tradicionalmente concebida como la reproducción manual de un nombre, y esto es una barrera a la aceptación de la firma electrónica.

En Francia[51], por ejemplo, la firma electrónica ha sido aceptada por las cortes de manera muy reciente, y solamente en los ámbitos en los cuales la prueba puede ser presentada libremente, o cuando se concluyó un convenio entre las partes acerca de la prueba que otorgue una fuerza probatoria a la firma electrónica. Esta jurisprudencia se ha presentado en materia de pago por medio de tarjetas bancarias, las cuales contienen una firma compuesta de un microchip y de un código secreto cuya validez ha sido reconocida por la Corte de Casación francesa. Pero la relevancia de la prueba presentada de esa manera es dejada a la libre apreciación del juez: es necesario convencer al juez de la fiabilidad del sistema de la firma electrónica utilizada, que debe permitir la identificación del autor del mensaje.

A este nivel, el uso de los sistemas de criptografía permite garantizar la seguridad de la transmisión en la red Internet, de las firmas electrónicas que se basan en la composición de un código confidencial. De esta forma gracias a la criptografía, el código confidencial puede volverse una firma electrónica no solamente en las transacciones "off line", sino también en las transacciones en línea.

[51] Al momento de acabar la redacción de este trabajo, los legisladores franceses están estudiando la posibilidad de introducir una iniciativa de ley para reglamentar el uso de la firma digital, conforme a la Directiva europea que se emitió en noviembre de 1999.

En Alemania, una ley relativa a la firma electrónica fue adoptada el 1ro de agosto de 1997. Esta ley federal da una definición de la "firma electrónica" que se basa a la vez en una clave privada y una pública. Esta ley rige la actividad de las autoridades de certificación, es decir la actividad que consiste en emitir certificados que llevan el nombre exacto de la persona asociada a la clave pública utilizada como firma, y que son disponibles para otros para verificación. El ejercicio de esta actividad requiere una autorización especial.

Aunque esta ley constituye un adelanto positivo, su interés sigue siendo limitado ya que la prueba de miles de actos jurídicos alemanes tiene que encontrarse en un escrito que lleva una firma manuscrita, y la ley de 1997 no elimina estas reglas de prueba.

En Bélgica, un anteproyecto de ley sobre la firma electrónica está en preparación. Afortunadamente, este proyecto va más allá de la ley alemana, y prevé la modificación de las reglas de prueba, especialmente las disposiciones del Código Civil que exigen un documento de papel y una firma manuscrita como métodos de prueba.

4.1.2.3 El principio por el cual "la prueba de un convenio entre dos partes no puede ser el hecho de una sola parte"

Cuando un cibercomerciante quiere aportar la prueba de una transacción que hizo con uno de sus clientes quien la impugna, los primeros elementos de prueba en los cuales piensa son obviamente las grabaciones informáticas conservadas por su sistema informático. Sin embargo, estos elementos de prueba parecen chocar con el principio general según el cual

no se puede oponer a un co-contratante elementos que provienen de la persona que pretende utilizarlos como prueba.

Esta jurisprudencia fue reafirmada recientemente en Francia por la Corte de Casación en un asunto donde la sociedad de ferrocarriles quería aportar la prueba del respeto de su obligación de seguridad para con un viajero que había tenido un accidente en un tren, basándose en parte en las declaraciones de un empleado de dicha sociedad, y por otro lado en unas grabaciones informáticas efectuadas automáticamente por los trenes.

Esta regla puede ser muy severa pero este obstáculo presenta la ventaja, a diferencia del escrito y de a firma manuscrita, de ser más fácilmente superado por la utilización de soluciones prácticas independientes de las reformas legislativas. De hecho, veremos que la utilización de sistemas informáticos gestionados por terceros certificadores es probablemente una buena manera de superar este obstáculo.

4.1.3 Unas reformas legislativas inevitables

Bajo la presión de las necesidades relacionadas con la voluntad de permitir un florecimiento del comercio electrónico, varios países están en el proceso de preparar o adoptar reformas legislativas.

Hace más de veinte años, las primeras discusiones acerca de este tema se basaban en la idea de supresión de la necesidad de un escrito. De tal forma que el 11 de diciembre de 1981, el Consejo de Europa elaboró una Recomendación dirigida a los Estados miembros, invitándoles a suprimir las exigencias del escrito y a reconocer el valor probatorio de las grabaciones

informáticas cuando satisfacen cierto número de condiciones particularmente acerca de la naturaleza del documento original, de la identidad de la persona que realiza la grabación, etc. Una propuesta de la CNUDMI hecha en 1986 buscaba estos mismos resultados.

Hoy en día no se piensa tanto en suprimir el escrito o la firma sino introducir en los sistemas legislativos una ampliación de la noción de escrito o de la firma, con el objetivo que un escrito no tenga que ser forzosamente en papel, y que la firma no sea necesariamente manuscrita.

Este es el sentido del proyecto de ley elaborado por el gobierno belga. Este proyecto tiene como principal ambición la de adaptar el orden jurídico belga a la era numérica. Con este objetivo, propone entre otras cosas modificar las disposiciones del Código Civil relativas a la prueba agregando los documentos informáticos a la lista de las pruebas perfectas, y reconociendo una fuerza probatoria a los documentos que presentan una firma electrónica.

Este proyecto propone también organizar la actividad de las autoridades certificadoras por un sistema de licencias, ya que estas autoridades ejercen su actividad ante el público en general (y no ante un circulo limitado de personas), y también reglamentar el uso de la firma electrónica en el sector público.

En Francia, un grupo de trabajo está estudiando las modalidades de una eventual adaptación de las disposiciones del Código Civil relacionados con la prueba, sin traicionar el espíritu del Código Civil; la idea principal sería insertar los rastros informáticos en el sistema de prueba legal.

En Alemania, la ley federal del 1o de agosto de 1997 ha adoptado cierto número de modificaciones acerca de la firma electrónica, con el objetivo de garantizar una mejor forma la confidencialidad y la integridad de un documento informático, pero esta ley se considera insuficiente porque no modifica las reglas de prueba previstas por el Código de procedimientos civiles.

Sin embargo, visto el carácter internacional del comercio electrónico, estas iniciativas nacionales son insuficientes. Por eso las organizaciones internacionales también consideran nuevas reglas de prueba adaptadas al comercio electrónico y armonizadas en el plano internacional.

La CNUDMI por ejemplo ha submitido a la comunidad internacional su *Ley modelo sobre el comercio electrónico* que contiene varias disposiciones relacionados con la prueba, y adaptadas a la desmatrialización. En efecto, propone entre otras ideas, que se considere satisfecha la exigencia del escrito cuando las informaciones requeridas sean "accesibles para ser consultadas posteriormente"[52]; la exigencia de la firma se considera satisfecha cuando se utiliza un método confiable para identificar la persona y aprobar el contenido; se considera satisfecha la condición de original cuando existe por un lado una garantía confiable de la integridad de la información y que por otro lado, la información se puede enseñar a la persona a quien debe ser presentada.

La Comisión Europea adoptó, por su lado, el 30 de julio de 1997, una Recomendación acerca de las transacciones que se hacen por medio de instrumentos de pago electrónico, que propone reglas más flexibles, como la asimilación de un documento electrónico a un documento escrito.

4.2 Soluciones practicas para minimizar los riesgos

Los prácticos del derecho no son magos que pueden hacer que desaparezcan las leyes problemáticas. Pero muy seguido son buenos para construir relaciones que, en la espera de reforma legislativas, permiten reducir las desventajas de las leyes existen.

De esta forma, existen tres vías que pueden elegir: ubicar la actividad del cibercomercio en un país donde las reglas de prueba no son demasiado inapropiadas; establecer convenios sobre prueba que permitan, basado en el fundamento del principio sagrado de la libertad contractual, organizar entre las partes un régimen de prueba adecuado; desarrollar un régimen probatorio basado en la intervención de un tercero certificador.

4.2.1 Elegir las reglas de determinación del derecho aplicable a las transacciones internacionales

Los particulares tienen algunas soluciones a su disposición, para sacar mas ventajas del comercio electrónico.

4.2.1.1 Elegir la ley aplicable en el contrato

El derecho internacional hace normalmente que prevalezca sobre cualquier otra regla (con excepción de las leyes de policía), la ley de las partes, es decir los términos de los contratos que acuerden. Por lo mismo,

---

[52] Articulo 6.

según la Convención de Roma[53] y la Convención de La Haya[54], debe prevalecer lo que elijan las partes en el contrato.

4.2.1.2 Ubicar la actividad donde existe una ley sobre prueba

Para los contratos concluidos en el web, cuando se puede manejar el uso de un contrato marco, es útil determinar la ley aplicable a la prueba, ya que la admisibilidad del documento informático depende de ello.

Si no existiera elección por las partes en el contrato mismo, este se regirá por la ley del país con el cual tenga los vínculos más estrechos. Obviamente, la ubicación del sistema informático que alberga la actividad del comerciante debe desarrollar un papel significativo. El cibercomerciante podrá querer instalarlo en un país donde las reglas de prueba le parezcan adaptadas al comercio electrónico.

A este nivel, hay que distinguir el objeto (lo que hay que probar), y también la carga (quien tiene que probar), como la admisibilidad de la prueba (determinación de los medios). Por lo que corresponde a las reglas aplicables al objeto de la prueba, son principalmente tomadas de la ley que rige el derecho cuya exigencia es debatida, es decir la ley del fondo, la ley del contrato. Lo mismo pasa con la carga de la prueba, y este concepto es retomado por el artículo 14 de la Convención de Roma.

En lo que atañe a la admisibilidad de los métodos de prueba de los actos jurídicos, la regla es más compleja, y aunque pareciera que en principio son los métodos aceptados según la ley del foro que predominan,

[53] Convención de Roma del 19 de junio de 1980, sobre el derecho aplicable a las obligaciones contractuales.
[54] Convención de La Haya del 15 de junio 1955, sobre leyes aplicables a las ventas de carácter internacional.

parece posible que existan varias leyes aplicables, como la ley del foro, la ley del fondo o también la ley que rige la forma del acto. La Convención de Roma enuncia en su articulo 14, que los actos jurídicos pueden probarse a través de cualquier método de prueba que sea permitido por la ley del foro, o por una de las leyes previstas en el articulo 9 [55].

La admisibilidad de los documentos informáticos podrá regirse según los casos, por estas distintas leyes, y esto podrá incitar una de las partes a aplicar en el ámbito de un litigio, una ley – mas severa o mas flexible según el caso - que no es la que regiría en principio el contrato. Por ejemplo, si el contrato fuera regido por una ley cuyas reglas probatorias son muy restrictivas, el co-contratante extranjero podría preferir referirse a la ley del país de formación del contrato o a la ley del foro que le sea más favorable, en lugar de la ley del contrato.

4.2.1.3 Las limitaciones en la elección del derecho

Siempre es posible invocar el orden público internacional en contra de la admisibilidad de un método de prueba previsto en la ley extranjera aplicada al litigio.

En efecto, el derecho internacional privado reconoce la primacía de algunas leyes, que se llaman leyes de policía, y que se definen como las leyes cuya observación es necesaria para la salvaguardia de la organización política, social o económica del país. Estas leyes que tienen carácter imperativo pueden entonces ser el vector de un mínimo de respeto para las disposiciones contractuales. Como se encuentra limitada por las

[55] El artículo 9 reenvía a la ley que rige el fondo del contrato.

leyes de policía, la deslocalización de la actividad del comerciante en un país que se preocupa poco de las reglas de forma, no permitiría que se evitaran algunas reglas del foro.

En la mayoría de los países europeos, las reglas relacionadas con la protección de los derechos del consumidor son leyes de policía. De tal forma que la ubicación de una actividad de comercio electrónico en algún país, basada en su régimen probatorio, sólo tendrá interés alguno en las relaciones con los consumidores, si no entra en conflicto con las reglas de protección al consumidor de los países donde se encuentren.

Además hay que subrayar que para algunos países como Francia, el derecho internacional reconoce otro principio que protege el orden público internacional, el principio de fraude a la ley. Este principio – que sin embargo no se encuentra presente en todos los Estados de la Unión Europea – tiene como pretensión frenar toda deslocalización cuyo único objetivo sea evitar una regla jurídica. Pero esto supone dos elementos constitutivos.

Por una parte, un elemento material que es la transferencia del vínculo con el país. Los nuevos métodos de operación facilitan esta transferencia ya que un servidor puede fácilmente transportarse. Esta regla podría sin embargo encontrar una limitación en el seno de la Unión Europea, visto que los principios de libertad de establecimiento y de prestación de servicios son la esencia misma de la Unión.

Hay que notar sin embargo que la jurisprudencia llamada "anti-evitacion" tiene el efecto de difundir este principio en el territorio europeo[56]. En efecto, esta jurisprudencia niega el beneficio de las disposiciones del derecho comunitario a los miembros que utilizan la Convención de Roma con el único objetivo de evitar los reglamentos nacionales normalmente aplicables. Sin embargo, hay muy pocas deslocalizaciones en el territorio Europeo con el objetivo de evitar una ley nacional, ya que las reglas protectoras del contratante son generalmente parecidas de un país a otro, porque a menudo son adoptadas en cumplimiento de una directiva comunitaria.

Por otro lado, es necesario un elemento moral, la intención de utilizar una regla de conflictos con el único objetivo de evitar una disposición imperativa.

4.2.2 Los convenios sobre la prueba

Aunque estos convenios son, en principio, validos, no son una solución milagrosa porque su aplicación se enfrenta a cierto número limitaciones jurídicas y prácticas.

4.2.2.1 La validez de los convenios

Como lo prevé el artículo 14 de la Convención de Roma, cuando la ley del contrato – elegida por las partes o, en ausencia de elección de las

[56] Corte de Justicia de las Comunidades Europeas, 3 de diciembre de 1974, Van Binsbergen, *Rec.. CJCE* 1974, p. 1299; CJCE 3 de febrero de 1993, Veronica, *Rec. CJCE* 1993, p. 487.

partes, aplicable en base a las diversas convenciones internacionales - no prohibe la aplicación de un convenio sobre prueba, este tipo de convenio es lícito y muy útil.

En todos los países europeos, parece que en general el derecho de prueba aplicable a la conclusión de los contratos no depende del orden público, y podemos deducir que las convenciones sobre prueba son, en principio, validas a excepción de algunos tipos de contratos como por ejemplo, las ventas inmobiliarias en las que el escrito es una condición básica de validez del contrato.

Es en los países de la familia jurídica neorromanista, donde la prueba de los contratos debe ser presentada por un escrito que lleve la firma manuscrita, que encontramos el interés práctico de estos acuerdos. En este caso, los convenios sobre prueba constituyen la única forma de no tener que acatar esas reglas.

Obviamente, esto no es posible cuando se requiere un escrito no solo en calidad de prueba sino también como requisito de validez.

El convenio sobre pruebas presenta otras ventajas que la de la elección de la ley aplicable. Por ejemplo, cuando varios tipos de prueba son admisibles para probar el mismo asunto, el acuerdo puede especificar los documentos que prevalezcan. También puede indicar bajo cuales condiciones se admita un documento electrónico como método de prueba en las relaciones entre partes.

Al adoptar este tipo de disposiciones, las partes limitan el poder de los jueces en lo que se refiere a la apreciación del valor probatorio de los

documentos electrónicos presentados. El acuerdo puede también prever, en el caso en que naciera un litigio entre las partes acerca de un elemento de prueba, cual sería el método de arreglo entra las partes más idóneo (selección de un arbitro o experto por ejemplo).

4.2.2.2 Las limitaciones a la aplicación de tales convenios

Cuando las partes deciden adoptar una convención sobre la prueba, esto presupone cierta complejidad, aun leve, relacionada con la necesidad de hacer un contrato según la forma tradicional (un escrito sobre papel y firmado) con el objetivo de poder evitar luego estas mismas reglas, en el ámbito de transacciones futuras hechas vía Internet.

Parece difícil imaginar, prácticamente la conclusión de convenciones sobre la prueba para transacciones muy puntuales o para cuantías modestas, ya que el esfuerzo realizado para la negociación del convenio sobre la prueba podría ser desproporcionado en relación con los riesgos asociados a la transacción y a los montos involucrados.

Este inconveniente puede ser limitado si el comercio electrónico se efectúa a través de una "galería comercial" que reúna varios comerciantes. De hechos, en este caso, un solo convenio sobre la prueba podría regir todas las relaciones comerciales intervenidas a través de esta "galería comercial".

Las disposiciones acerca de las cláusulas abusivas también pueden limitar la organización de las reglas de prueba que las partes quieran aplicar.

La Unión Europea adoptó una Directiva en 1993 sobre las cláusulas abusivas en los contratos pasados con consumidores[57]. Esta Directiva, que limita su campo de aplicación por un lado a los contratos entre profesionales y consumidores, y por otro lado a los contratos que no se hayan obtenido tras un negociación individual, considera como abusivas las cláusulas que "a pesar de la exigencia de buena fe, crean en detrimento del consumidor, un desequilibrio significativo entre los derechos y las obligaciones de las partes que resultan del contrato".

Este texto fue reiterado en el derecho francés con la ley del 1ro de enero de 1995 que modificó el artículo 132–1 del Código francés de protección a los consumidores, y su texto prevé un anexo que establece una "lista indicativa y no exhaustiva de cláusulas que pueden verse como abusivas si satisfacen a las condiciones mencionadas en el primer párrafo...". En esta lista, se consideran cláusulas abusivas, las que tienen como efecto u objeto el de "suprimir u obstaculizar el ejercicio de una acción legal o de vías de recurso para el consumidor (...), limitando indebidamente los métodos de prueba que pueda utilizar el consumidor, o imponiéndole una carga de prueba que debería de corresponderle normalmente a otra parte en el contrato".

De la misa manera, en Alemania, el párrafo II subpárrafo 15 de la *Ley sobre las condiciones generales*, estima que son inválidas las cláusulas que modifican la carga de la prueba en desventaja de un consumidor.

Así, las convenciones sobre prueba concluidas con consumidores pueden permitir derogar a la regla del escrito, fijar un valor probatorio para

un documento informático, pero de ninguna manera pueden llegar a tener como efecto el de invertir la carga probatoria en detrimento de un consumidor.

La Unión Europea adoptó el 20 de mayo de 1997 una Directiva[58] acerca de la protección de los consumidores en materia de contratos a distancia.

Este texto cuya principal ambición es adaptar la protección del consumidor a las nuevas técnicas de comunicación a distancia, propone una definición extensiva del contrato concluido a distancia, ya que incluye: "cualquier contrato acerca de bienes o servicios que se concluye entre un proveedor y un consumidor en el ámbito de un sistema de venta o de prestación de servicios a distancia organizado por el proveedor, que para este contrato utiliza exclusivamente una o más técnicas de comunicación a distancia hasta la conclusión del contrato, incluyendo la misma conclusión del contrato".

Este texto acerca de los contratos a distancia, que parece tratar de adaptarse a las nuevas tecnologías de comunicación y favorecer el desarrollo del comercio electrónico prevé sin embargo, lo que es antinómico, la confirmación por escrito de algunas informaciones acerca del contrato. Sin embargo, la Directiva admite que se pueda sustituir al documento en papel "cualquier otro soporte duradero".

---

[57] *Diario Oficial de las Comunidades Europeas*, del 21 de abril 1993, No. L 95.

4.2.3 La intervención de un tercero de confianza

La intervención de un tercero de confianza (o tercero certificador) resulta útil, sin importar que se haya logrado un convenio sobre la prueba o no. En efecto, en todos los casos, la intervención de un tercero certificador permite evitar que los documentos informáticos presentados por un cibercomerciante sean declarados inadmisibles porque provendrían de su propio sistema informático.

Generalmente, el sistema de tercero certificador se apoya en un mecanismo técnico que permite asegurar la integridad del mensaje enviado o autenticar un emisor y / o destinatario de informaciones según una arquitectura segura (claves, algoritmos). Además el tercero certificador puede constituir certificados que indiquen que el mensaje fue enviado, y que constaten electrónicamente que se realizó una operación en la cadena segura. Podemos distinguir varios tipos de terceros certificadores, según su papel en la creación de la prueba:

- Las autoridades certificadoras tienen como tarea entregar a una persona los certificados gracias a los cuales un cocontratante puede verificar la autenticidad de su firma electrónica a través de la grabación electrónica que identifica esta persona;

- La actividad de otros terceros certificadores puede consistir en la creación de otros tipos de pruebas, por ejemplo conservando para las dos partes una copia del contenido de los mensajes intercambiados, y

[58] Directiva 97/7/CE del Parlamento europeo y del Consejo del 20 de mayo de 1997, *Diario Oficial de las Comunidades Europeas* del 4 de junio de 1997, No. L 144/19.

certificando que estos mensajes fueron recibidos, así como la hora a la cual fueron intercambiados.

En el caso de los convenios sobre prueba, el uso de terceros certificadores podría evitar que la cláusula que incluye un convenio sobre prueba se considere abusiva según la definición de la Directiva de 1993.

En efecto, si no se utiliza la figura del tercero certificador, es posible que la cláusula que prevé que las grabaciones provenientes del sistema informático del cibercomerciante sirven como método de prueba de la transacción, se perciba como una disposición que crea en detrimento del consumidor un desequilibrio significativo, justificando así que se niegue su aplicación.

En resumen, el tercero certificador, como un cibernotario, mejora la calidad de la prueba presentada al juez. Las partes emplean esta figura para certificar y / o autentificar una operación computarizada, como emplean el sistema del correo recomendado con acuse de recibo para asegurarse que el mensaje llegó a su destino. El tercero certificador es un tipo de acuse de recibo electrónico, y hasta más ya que puede, a diferencia del servicio de correo normal, probar el contenido del mismo documento.

Para que una operación de certificación no sea impugnada, tiene que ser emitida por un organismo independiente. La calidad de tercero es desde luego fundamental en la noción de "tercero calificador".

A priori, se debería considerar que puede beneficiar de esta calidad de tercero cualquier entidad que no tenga un interés directo o indirecto en que una parte a la transacción u otra pueda o no presentar la prueba de los

derechos y obligaciones en juego. Parece ser más la ausencia de interés que da esta calidad de tercero de confianza, que una ausencia total del vínculo.

Por ejemplo, un organismo como Visa podría considerarse como un tercero en relación con los bancos de los portadores de tarjetas Visa y los bancos de los comerciantes que aceptan estas tarjetas, en el ámbito de los litigios de las ordenes de pago - dadas para el pago de transacciones electrónicas – y arregladas a través del sistema de pago que Visa maneja. En efecto, Visa no tiene más interés en que el banco de un tarjetahabiente o el banco de un comerciante gane tal litigio.

Esta actividad todavía hoy en día carece de reglamentación; descansa actualmente más en mecanismos contractuales. Es dentro de un marco contractual que se encuentra la noción de "Trustee Third Party" prevista en el proyecto de norma ISO.

Sin embargo, si esta actividad se desarrolla, los Estados tratarán probablemente de reglamentarla. Así en Bélgica un proyecto de ley organiza un sistema de licencia para los terceros certificadores que ejercen su función para el público en general. En Alemania, la ley federal del 1ro de agosto de 1997[59] reglamenta la actividad de tercero de embargo, instaurando un sistema de licencia. Sin embargo, este sistema de autorización se limita en prever que una entidad se encargará de certificar y de controlar la atribución de una clave pública utilizada como firma electrónica y sello dando fe a la fecha y la hora. Así las demás actividades de los terceros certificadores se quedan afuera del ámbito del sistema de licencia.

En los Estados Unidos de Norteamérica, la American Bar Association adoptó consignas que definen las funciones de las autoridades certificadoras.

[59] www.iid.de.

Capitulo 5:
La firma electrónica

5.1 Consideraciones preliminares

Para entender el alcance de la firma electronica, es menester que nos percatemos de la necesidad de tener seguridad en Internet, a través de un sistema de firmas eficaz. Antes que todo, sin embargo, debemos definir la firma electronica, con sus funciones y características.

5.1.1 Funciones y características de la firma tradicional

El comercio y las infraestructuras jurídica y comercial que lo acompañan han desarrollado a lo largo de un periodo sustancial de tiempo, un grupo de reglas bien definidas acerca del uso de las firmas tradicionales. Sin embargo, debido al desarrollo de la era digital, el comercio y los legisladores se enfrentan a un nuevo punto de partida. El sendero que lleva a las soluciones de los problemas relacionados con las transacciones comerciales electrónicas hará que algunos de los procedimientos tradicionales utilizados en la firma de documentos en formato de papel se vuelvan obsoletos. Se establecerán métodos nuevos y mejorados que tomen en cuenta el desarrollo de las tecnologías para efectos de la firma de documentos electrónicos.

Los autores de libros de doctrina en este ámbito sugieren que las firmas electrónicas serán el fundamento de este nuevo comercio global, si pueden llegar a poseer no menos que las características de seguridad mínimas que se atribuyen a las firmas tradicionales. Si una firma electrónica no posee estas características mínimas, entonces no podrá beneficiar del respaldo y la confianza del comercio y del poder judicial, y los beneficios potenciales de esta tecnología serán afectados.

Visto que las firmas tradicionales son utilizadas por los particulares de manera casi universal, el origen de su reconocimiento, uso y significado son raramente considerados. Sin embargo, estos orígenes parecen ofrecer unas pistas de reflexión interesantes para la era digital. Según una autoridad eminente[60]:

Los obscuros orígenes del arte de la escritura tienen que considerarse como remontándose a las escrituras que aparecieron primeramente en las paredes de las grutas de los períodos medio y final del paleolítico. Antes que estos pictogramas pudieran ser considerados como escritura, sin embargo, era necesario que pasaran a través tres etapas bien definidas del desarrollo. Primeramente, los dibujos se habían vuelto convencionales, así que siempre tenían la misma apariencia y se referían al mismo objeto.

Era necesario que no sólo se refirieran a un objeto concreto, sino que también llegasen a ser los símbolos de conceptos abstractos. Finalmente, era esencial que estos símbolos convencionales pasaran a esta etapa con una representación combinada de una concepción abstracta con el sonido de la voz humana. Esta última etapa paso a través de varios desarrollos.

Entonces, antes que un ambiente apropiado en el ámbito comercial y jurídico se forme, que adopte el concepto de firmas electrónicas, es previsible que se realice una convencionalización de las firmas electrónicas. La primera etapa en este proceso es el amplio reconocimiento de que el equivalente en la era digital de las firmas tradicionales, es disponible.

Dada la importancia central de las firmas en el procedimiento tradicional, es muy probable que la convencionalización (estandarización) de las firmas electrónicas sea un paso indispensable en el establecimiento de procedimientos electrónicos e infraestructura comparables. Hasta que esto ocurra, parece dudoso que los comerciantes y el poder judicial adopten ampliamente esta tecnología.

---

[60] Véase: Barnes, H.E., *History of Historical Writings*, Londres: Dover Publications, 1890.

Además, es razonable pensar que las personas que hagan transacciones comerciales van a requerir garantías que la firma de documentos electrónicos será por lo menos tan segura como los métodos tradicionales, si no es que más. Sin tales garantías, es probable que la gente no contrate tan libremente de forma electrónica como lo pudiera hacer por otros medios convencionales, en los que pueden depositar su confianza en la seguridad, virtual o percibida, de ese proceso. Se argumenta que el elemento de confianza es fundamental.

En este sentido, la confianza incluye tres elementos: la confianza comercial, la confianza tecnológica, y la confianza comportamental. Su importancia y relación con la naturaleza y el papel de las firmas no puede subestimarse ya que son una parte integral para establecer la confianza en los procedimientos utilizados en el comercio. Además, esta confianza no puede establecerse en una ley, sino que tendrá que lograrse a través de la aceptación de los participantes en el comercio, de que este nuevo paradigma comercial satisface por lo menos las exigencias funcionales mínimas de las firmas tradicionales.

De manera sorprendente, se han publicado muy pocas investigaciones acerca del significado jurídico de la firma. Se han hecho algunos trabajos acerca del concepto de firmas de testigos y en particular de notarios[61], pero en general es un tema que parece haberse tomado por hecho.

Sin embargo, en un precedente de la jurisprudencia australiana, el ministro de la Corte Higginbotham comenta acertadamente:

> El objetivo de todas las leyes que requieren que un particular firme un documento es autenticar el origen del documento. Una firma es solamente una marca, y cuando la ley solo requiere que se firme un documento, los requisitos de la ley son cumplidos con la prueba de que se apunto la marca en el documento por el signatario o su representante legal. De la misma forma, cuando la ley no exige que la firma sea un autógrafo, el nombre escrito de una parte quien debe firmar el documento es suficiente (...) o la firma puede ser impresa en el documento por un sello de un facsímile de la firma normal de la persona que debe firmar (...) Pero la prueba en estos casos debe darse que el nombre impreso en el sello fue ratificado por la persona, o que esta persona reconoció que se utilizo el sello bajo su autoridad[62].

Este caso establece tres puntos importantes. En primer lugar, es un reconocimiento que la firma de una persona, para que se encuentre vinculada con el contenido del documento, no requiere el acto físico de que escriban con su puño y letra, ya que es posible pasar a través de un agente o el uso de un medio mecánico, como un sello impreso que lleve un facsímile de la firma de la persona. En el caso de una compañía, visto que es una entidad jurídica artificial y solo puede actuar a través de un agente humano, debería de existir un requisito general de identificar la persona que

[61] Véase por ejemplo: Ready, N.P., *Brooke's Notary*, Londres: Sweet & Maxwell, 1992.
[62] R. v. Moore (1884) 10 VLR 322. En este caso, el comprobante de un prestamista no había sido firmado por el dueño del negocio según la legislación correspondiente, sino por un agente autorizado, aunque el nombre del prestamista aparecía impreso en el comprobante.

fije el sello de la compañía, no solo por su nombre sino también por una marca distintiva.

En segundo lugar, la cita determina que el objetivo de una firma que aparece en un documento es para autentificar la procedencia genuina del documento.

Finalmente, menciona que una persona, para ser vinculada, debe de tener la intención y voluntad de firmar el documento, y no solamente firmar un autógrafo.

Cuando se pone un autógrafo a un documento, existe por parte del signatario una falta de intención de ser vinculado por el contenido del documento, o de ser asociado con el contenido del documento[63]. Por esto, una marca en un documento no va a ser considerada como firma en la mayoría de los países, a menos que exista la necesaria intención de ser vinculado por el contenido del documento, o de ser asociado con él.

Entonces una firma, si es ejecutada correctamente, y no existen circunstancias que la puedan viciar jurídicamente, como en el caso del dolo o fraude, tendrá el efecto de vincular el signatario al contenido del documento, aun cuando no lo haya leído.

Una firma puede cumplir varias funciones como:

- identificar el signatario;

- confirmar el involucramiento personal de una persona en particular en el acto de la firma;

- asociar una persona en particular en el contenido del documento;

- dar fe de la intención de una persona de ser vinculada por el contenido de un documento;

- dar fe de algún acuerdo escrito que puede haber sido redactado por un tercero que no es parte al acuerdo vinculante[64].

Las características físicas generales de la firma tradicional son que:

- puede ser fácilmente producida por la misma persona;

- es fácilmente reconocible por terceros;

- es relativamente difícil de falsificar por terceros;

- se vincula con el documento de tal forma que el objeto físico y su contenido así como la firma se convierten en un objeto físico (tinta sobre papel);

---

[63] Además, la marca de un testigo no involucra necesariamente la intención de estar vinculado por el contenido del documento. Consecuentemente, la firma del testigo es identificada como tal, para que no quepa ningún tipo de confusión acerca de quien queda vinculado por el contenido del documento.

[64] Véase: UNCITRAL Working Group on Electronic Commerce, *Planning of Future Work on Electronic Commerce: Digital Signatures,, Certification Authorities and Related Legal Issues*, 31st session, New York, 18-28 de febrero de 1997.

- es de manera comparativa un estándar para todos los documentos firmados por la misma persona[65]; y

- es relativamente difícil quitarla sin dejar rasgo[66].

Las características jurídicas generales de una firma tradicional son que:

- cualquier tipo de marca es aceptable si es puesta por la persona o algunas personas autorizadas por la persona que se supone que debe ser vinculada[67];

- a menos que exista algún requisito legislativo específico, la marca puede ponerse con algún medio electrónico;

- la marca puede ser altamente insegura, como la que es efectuada por un lápiz;

- en el momento en que pone la marca, el signatario debe de tener la intención necesaria de ser vinculado por el contenido del documento o, en el caso en que fuera un testigo, debe de tener la intención necesaria de ser asociado con el documento en calidad de testigo; y

---

[65] Hagan, W., *A Treatise on Disputed Handwriting and the Determination of Genuine from Forged Signatures*, Londres: Sweet & Maxwell, 1894.

[66] Sin embargo, es posible borrar una firma tradicional sin dejar rasgos, utilizando una tecnología basada en el láser; el costo seria sustancialmente mas elevado que borrar una firma digital de un documento electrónico, que necesitaría por lo menos un editor de textos.

[67] *Blackstone's Comentaries on the Laws of England*, Londres: The Legal Classics Library, 1983, Libro II, p. 305.

- la marca puede ser ubicada en cualquier parte del documento y no tiene que aparecer al pie de éste, a menos que sea un requisito legislativo para su forma, que especifique donde tiene que ponerse.

5.1.2 La necesidad de seguridad en Internet

El desarrollo del comercio electrónico ha planteado una cantidad impresionante de cuestiones acerca de las reglas existentes, y el sistema jurídico. Uno de los asuntos más importantes para los partidarios de esta nueva forma de hacer negocios, es la eliminación de las barreras al comercio electrónico, que constituyen hasta cierto punto los vestigios de un sistema de derecho mercantil basado en el papel. Los requisitos jurídicos, como los que tienen que ver con los conceptos de "escrito", "firma" y "original" tienen que ser reconsiderados en el contexto del comercio electrónico.

En varios ámbitos, sin embargo, los legisladores están recibiendo mucha presión para ir más allá de la eliminación de barreras y "apoyar" el desarrollo del comercio electrónico con el establecimiento de un marco jurídico que aliente y promueva su utilización. El argumento se basa en que el derecho debería ayudar a fortalecer la confianza en el sistema, presentando reglas que apoyen y promuevan estas nuevas formas de hacer negocios.

De alguna forma estas exigencias son fáciles de comprender, porque combinan dos necesidades. La primera es la necesidad aparente que existan reglas que guíen la conducta en Internet. El público y la prensa han estudiado la tecnología y monitoreado sus avances, y la han calificado de

"revolucionaria". El hecho de calificar el ciberespacio como algo nuevo y ajeno crea en la gente un temor de que es verdaderamente desconocido y desconocible, y la gente desconfía de lo desconocido. El resultado es una preocupación acerca de lo que gobernará este territorio desconocido.

Algunas personas han opinado que el Internet es una jurisdicción única, y como tal debería de ser sometida a su propio cuerpo de leyes[68], mientras que otros han intentado resolver asuntos relacionados con el Internet haciendo analogías con otras ramas del derecho[69]. El verdadero desafío es examinar la necesidad de tener reglas especificas en el contexto, y determinar si el problema considerado es suficientemente distinto en un contexto de Internet o en línea para justificar un conjunto de reglas distinto al que ya existe[70].

La segunda necesidad es la de la seguridad. En gran parte, la novedad de la tecnología, la falta de familiaridad con el funcionamiento de Internet, y el potencial para el fraude y el error, han dado lugar a preocupaciones acerca de la "confiabilidad" del sistema. De hecho, la seguridad es una palabra clave del contexto del comercio electrónico; esta preocupación se encuentra presente en varios ámbitos: jurídico, tecnológico, teórico, y de los negocios.

---

[68] Shapiro, L., "The Disappearence of Cyberspace and the Rise of Code", 8 *Seton Hall Const. L.J.*, 703 (1998). El autor concluye que el Internet es simplemente una tecnología de comunicaciones alternativa, y que no es mas necesaria una "ley del ciberespacio" que lo fue una "ley del alfabeto".

[69] Véase: Geist, M., "The Reality of Bytes: Regulating Economic Activity in the Age of the Internet", 73 *Wash. L. Rev* 521 (1998).

[70] Véase: Stein, A., "The Unexceptional Problem of Jurisdiction in Cyberspace", 32 *Int'l Law* 1167 (1998).

Las preocupaciones acerca de la seguridad, que sean reales o percibidas, tienen que ponerse en perspectiva[71]. La seguridad no puede ser "legislada". Es una combinación de factores: la tecnología utilizada, su aplicación en el comercio y el estado de desarrollo, y la estructura jurídica. Hacer negocios de manera "segura" en la carretera de la información no es una simple cuestión de desarrollar las tecnologías adecuadas para "encerrar" la información que uno quiere mandar electrónicamente, para protegerla contra el robo o la alteración, y tampoco es el simple hecho de desarrollar técnicas de autenticación que nos permita determinar con una precisión extrema el verdadero emisor o creador de un mensaje.

El comercio electrónico "seguro" no puede lograrse solamente legislando las circunstancias en las cuales se requiera algún grado de seguridad. Más bien, la "seguridad" que los hombres y las mujeres de negocios buscan cuando hacen negocios electrónicamente, requiere la creación de una infraestructura entera – jurídica, social, económica, y política – basada en una práctica que reconoce y apoya el comercio electrónico.

En el ambiente electrónico, lo que sin duda hace falta en este momento es una estructura social y jurídica discernible, que permita a las partes determinar adecuadamente los riesgos del comercio electrónico, y de responder tomando decisiones inteligentes acerca de sus propios derechos y responsabilidades, incluyendo la distribución de los riesgos en sus transacciones con otras personas. Por ejemplo, sin una estructura jurídica apropiada que reconoce el comercio electrónico, la presencia de todos los instrumentos de autentificación en el mundo no podrán dar a los

[71] Existe un punto de vista, generalmente compartido por las personas del medio tecnológico, que en algunos ámbitos, la tecnología tiene la capacidad de ofrecer mas seguridad en las transacciones comerciales, que los

comerciantes la seguridad que necesitan par hacer negocios en el ambiente electrónico.

La estructura jurídica tiene que incluir leyes que reconozcan la habilidad de contratar electrónicamente, ratificar convenios pasados electrónicamente, y adoptar las reglas aplicables a la transacción reconociendo al mismo tiempo la posibilidad para las partes de determinar los términos y elegir el derecho aplicable. Este tipo de seguridad – la seguridad jurídica – se desprende de un marco jurídico que puede ser que ya exista, en gran parte, pero como la aplicación de este marco al medio de las transacciones en línea no parece ser muy clara, el sentido de seguridad resultante puede ser afectado. Hay que reconocer, sin embargo, que la "seguridad jurídica" solo es una parte de toda la problemática sobre seguridad.

El deseo de tener seguridad en el comercio electrónico se ha manifestado de forma bastante tradicional. Al principio, debido a la ausencia de reconocimiento legislativo y judicial y de la aceptación más general del comercio electrónico, y la falta correspondiente de estándares comunes a toda la industria, de costumbres para guiar la conducta, se intentó establecer un conjunto de normas para el comercio electrónico a través de "convenios" entre socios comerciales ("trading partner agreements") que realizaban actividades comerciales electrónicas[72].

Varios convenios modelo regionales y nacionales se desarrollaron para ofrecer a los comerciantes un marco contractual para facilitar la adopción y el uso de prácticas comerciales electrónicas, y dando así a las

---

sistemas basados en el papel.

partes algún grado de certidumbre acerca de los términos aplicables para sus transacciones. Aunque existían diferencias entre los varios convenios, un ingrediente clave de casi todos era la articulación por las partes de las medidas que se iban a utilizar en las transacciones electrónicas, y la delineación de las circunstancias bajo las cuales cada parte resultaría vinculada por los mensajes que de ella originaran.

En las situaciones en las que las partes no hubiesen estado en contacto con anterioridad, o cuando las transacciones no fueran de naturaleza tal que la negociación previa de estos convenios llegara a ser imposible o impráctica, se adoptaban modelos contractuales alternativos. Una táctica era la articulación de los términos aplicables por una de las partes al contrato, por ejemplo publicando los términos en un sitio web, o haciendo referencia a un conjunto de prácticas en particular.

Una variante de este tipo de contrato era el desarrollo de reglas operativas dentro de sistemas definidos, y que tenían como objetivo vincular a todos lo participantes en el sistema. El establecimiento de "códigos de conducta" voluntarios, y el desarrollo de estándares de la industria son dos opciones más que se han venido explorando. Otro proyecto ha sido establecer un conjunto común de "términos electrónicos jurídicos" ("eterms") que las partes puedan incorporar en sus mensajes electrónicos, para brindar la estructura jurídica privada que guíe la transacción. Además, se ha podido notar un movimiento cuyo objetivo es favorecer la certidumbre a través del uso de varias leyes y cláusulas, y el deseo correspondiente de fortalecer la aplicabilidad de estas cláusulas en el comercio electrónico.

---

[72] Véase: Boss, A., "Electronic Data Interchange Agreements: Private Contracting Toward a Global Environment", 13 *Nw J. Int'l L. & B.* 31 (1992).

En 1997, la Casa Blanca publicó un informe con el título "Un marco para el comercio electrónico global"[73], que presentaba las políticas de la administración Clinton en relación con el derecho del Internet. La administración de la Casa Blanca enfatizó firmemente que en el ámbito del comercio electrónico, el sector privado debería impulsar los cambios deseados, y la regulación gubernamental debería desempeñar un papel supletorio solamente. Los gobiernos estatales recibieron indicaciones de no poner trabas que pudieran restringir el florecimiento del comercio electrónico, y de alentar la creación de nuevos modelos comerciales y productos. Se especifica en este documento que si y cuando la intervención gubernamental fuera necesaria para facilitar el comercio electrónico, el objetivo del gobierno tendría que ser apoyar y aplicar un medio jurídico predecible, minimalista, congruente y sencillo, al comercio[74].

La Casa Blanca reconoció que a pesar de la preferencia para el liderazgo del sector privado, podría existir la necesidad de elaborar algunas reglas acerca del comercio electrónico global. En este punto, enfatizó la importancia de la eliminación de barreras administrativas y de regulación, y el reconocimiento de algunos principios fundamentales. El primer principio es obviamente, la libertad de contratar, la habilidad para los vendedores y compradores bien informados, de determinar su propias reglas. De misma importancia fue el llamado de la administración Clinton para que cualquier legislación o regla fuera "tecnológicamente neutra", es decir que las reglas no deberían requerir o presumir una tecnología en particular, y ser lo suficientemente flexibles para permitir el desarrollo de nuevas tecnologías en el futuro.

---

[73] Véase: Clinton, W., y Gore, A., "A Framework for Global Electronic Commerce", www.ntf.nist.gov/eleccomm/ecomm.htm.

[74] Dos principios mas también fueron mencionados: que los gobiernos deberían reconocer la calidades únicas del Internet, y que se debería de facilitar el comercio electrónico de manera global.

En reconocer la necesidad de legislar, pero al mismo tiempo la importancia de adoptar un enfoque minimalista, la Casa Blanca se hacia el reflejo de las discusiones en los círculos comercial, académico y político de los últimos años.

5.1.3 La necesidad de las firmas en Internet

Visto que las firmas son un elemento vital del comercio, los consumidores deben desarrollar la habilidad de firmar documentos transmitidos vía Internet. La naturaleza del Internet, donde todas las comunicaciones son tecleadas en lugar de ser manuscritas, no se presta a las nociones tradicionales de "firmas". No es suficiente en el Internet, como ya lo vimos, que se utilice el método tradicional de poner la firma de uno al final de un documento, ya que éste método no puede satisfacer los requisitos de autentificación.

Primeramente, la firma no puede llenar el requisito de la autentificación del signatario, ya que la firma no poseerá ninguna característica específica que pueda asegurar la identidad del signatario[75]. Visto que todas las comunicaciones en Internet son tecleadas, no existe la posibilidad de evaluar la unicidad de una firma para determinar si es auténtica. Además, las nociones tradicionales de un notario que revise el documento firmado, son imprácticas por no estar el notario en una mejor postura para autentificar la firma que las mismas partes contratantes.

[75] Véase: Jaksetic, E., "How to Ensure the Intgrity of Digitally Transmited Documents", *Corp. Legal Times*, Agosto de 1996, p 21.

De la misma forma, la autentificación de documentos es más difícil de lograr en el Internet. Como lo mencionábamos anteriormente la validez de los datos contenidos en un pedazo de papel es más fácil de confirmar examinando el documento para buscar posibles alteraciones. Sin embargo, los documentos digitales son relativamente fáciles de reproducir y alterar, y tales modificaciones son casi imposibles de detectar. Además, resulta casi imposible determinar si el documento fue alterado antes o después de su firma.

Como el comercio electrónico no puede funcionar bajo las nociones tradicionales de la verificación de las firmas, ha sido menester desarrollar un nuevo régimen de verificación para tal comercio. Varias alternativas existen actualmente con el objetivo de resolver ese problema de firma en Internet. Una solución propuesta es el uso de una tecnología de encriptación para asegurar la integridad de la comunicación. Eso permite al signatario de "cifrar" el documento firmado. Solamente la parte receptora podría entonces descifrar el documento mediante el uso de un código especial llamado "clave pública".

El uso de un esquema de encriptación con clave pública permite al receptor de un mensaje encriptado verificar la integridad del mensaje, y asegurarse que no ha habido ningún tipo de alteración, satisfaciendo así el requisito de autentificación de la firma del documento. Sin embargo, como este sistema utiliza "claves públicas" disponibles para un número importante de personas, y no "claves privadas" que solo puede utilizar una sola persona, no hay manera de verificar la identidad del signatario. De tal manera que la encriptación no tiene ningún peso jurídico para "vincular" la parte que encripta al contenido del documento, y no satisface la condición de autentificación del signatario.

Una segunda solución posible es el concepto de firma "digital", que se basa en la creación de un criptosistema asimétrico. Un particular que quisiera utilizar este sistema debería de desarrollar dos claves criptográficas que serían distintas para ese individuo. Las "claves" son prácticamente dos algoritmos matemáticos distintos pero relacionados, que pueden ser desarrollados utilizando un sistema de computadora apropiado. El individuo encripta su mensaje utilizando la primera clave "privada", que sólo él conoce. A estas alturas, el receptor recibe el mensaje en la forma encriptada.

El receptor recibe la ubicación de la segunda, una "clave pública" para descifrar el mensaje. Una tercera parte neutral detiene y entrega esta clave "pública" al receptor cuando se la pide. El receptor utiliza entonces la clave "pública" para descifrar el mensaje para poderlo leer.

Un procedimiento tecnológico llamado función de asignación única (el "hash function")[76], es el secreto del éxito de la "firma digital". Una función de asignación única es un algoritmo que produce una representación digital única, o "huella" llamada el resultado de asignación ("hash result"), que se encuentra incorporada en el texto del documento firmado. El resultado de asignación esta basado en la utilización de la "clave privada" y el mensaje específico por firmar. Es imposible que dos resultados de asignación sean idénticos ya que cualquier cambio en la clave privada o en el texto del mensaje tiene como resultado un resultado de asignación distinto. La naturaleza de la función de asignación única hace que sea imposible derivar el mensaje original a partir del resultado de asignación solamente, o alterar el contenido del mensaje sin cambiar el resultado de asignación.

La utilización por el receptor de la "clave pública" revierte el proceso de crear el resultado de asignación. El hecho de utilizar la clave pública y el resultado de asignación contenidos en un mensaje recibido, tiene como resultado que el receptor "recrea" el mensaje original. Sin embargo, si el mensaje fue falsificado desde el comienzo (una clave privada que no corresponde a la clave pública fue utilizada para firmar el mensaje), la clave pública no interactuará correctamente con el resultado de asignación, y el receptor no podrá acceder al mensaje. De la misma forma, si alguien altera el mensaje antes de su recepción, entonces alterará el resultado de asignación, y no se podrá recrear el mensaje original a partir de la clave pública.

La "firma digital" con su sistema, cumple los requisitos necesarios de autenticación para que la firma sea jurídicamente vinculante. Para que el sistema funcione, hay que utilizar claves privada y públicas correspondientes para permitir que el receptor confirme la identidad del signatario. Visto que solamente el signatario tiene la posesión de la clave privada, esta persona es la única que va a poder "firmar digitalmente" un documento de tal forma que pueda ser descifrado por el receptor. Por lo mismo, los requisitos de autentificación del signatario se encuentran llenados.

De manera semejante, una alteración del mensaje sería fácilmente identificable porque la clave pública no interactuaría exitosamente con el resultado de asignación del mensaje. Es posible garantizar al receptor que no ha habido ninguna alteración durante la transmisión del mensaje, permitiéndole recuperar el texto encriptado. Consecuentemente se llenarían los requisitos de autentificación de documento.

---

[76] Véase: Saxby, S., *Encyclopedia of Information Technology Law*, Londres: Sweet & Maxwell, 1990, p. 587.

Las firmas digitales parecen ser el método a través del cual el comercio electrónico en Internet puede llenar los requisitos de la "firma" necesarios para las transacciones comerciales. La creación de un sistema uniforme para aplicar esta tecnología es la manera de integrar rápidamente a los nuevos usuarios en el sistema, y crear las entidades necesarias para la buena operación del sistema de firmas digitales.

En 1996, el Comité sobre la seguridad de la información de la *American Bar Association* adoptó unas Reglas sobre las firmas digitales ("Digital Signature Guidelines") para tratar de encontrar un método de autentificación de firmas en el Internet. Si es cierto que las Reglas ofrecen una estructura técnica y jurídica para un sistema de firmas digitales, no tienen como objetivo servir como modelo para una ley sobre firmas digitales. Son más bien un punto de partida para el diseño de un sistema "confiable" y una ley apropiada sobre este asunto.

5.1.4 El sistema de criptografía asimétrica

A continuación, describiremos en detalles las etapas de la organización de este sistema que promete facilitar la seguridad de las transacciones en el comercio electrónico. Es menester considerar tres entidades distintas en el esquema de funcionamiento de la firma digital: el suscriptor, la autoridad certificadora, y el receptor.

Para empezar el procedimiento, el suscriptor, quien es el signatario potencial, tiene que crear un par de claves (una pública y una privada)

utilizando un programa computarizado apropiado[77]. Ya que el par de claves es reutilizable, el suscriptor puede realizar un número ilimitado de firmas con estas mismas claves. El suscriptor entrega una copia de la clave pública, junto con una prueba de su identidad, a la autoridad certificadora. El suscriptor, sin embargo, se quedará con su clave privada y no la divulgará a nadie, incluso al tercero certificador.

La autoridad de certificación sirve como intermediario entre el suscriptor y el receptor. Es responsabilidad de la autoridad confirmar la identidad del suscriptor y la validez del par de claves del suscriptor[78]. De esta forma, la autoridad certificadora tiene una función similar a la de un notario: actuar como un agente verificador imparcial para la firma del suscriptor.

El tercero certificador tiene que elaborar un certificado que contiene información acerca del suscriptor y de su clave pública. La autoridad certificadora presenta luego el certificado al suscriptor quien "acepta" el certificado verificando la exactitud de la información contenida. Una vez "aceptado" el certificado, el suscriptor puede empezar a utilizar el par de claves para firmar digitalmente los documentos que quiera.

La autoridad certificadora recopila todos los certificados que emitió para ponerlos a disposición de los receptores potenciales, que pueden consultarlos en línea. Además, la autoridad certificadora debe publicar en el mismo sitio una declaración sobre su práctica de certificación. Este

[77] Según los autores consultados, este programa tiene que ser confiable ("trustworthy"), es decir que tiene que reunir los siguientes requisitos: ser razonablemente seguro para prevenir las intrusiones y el mal uso; dar un nivel razonable de disponibilidad y buen funcionamiento; adherir a los principios generalmente aceptados de seguridad.

[78] Visto que el suscriptor retiene su clave privada, la autoridad certificadora tiene que encontrar alguna forma de verificar que las claves – publica y privada - del suscriptor, funcionan como par.

documento explica los métodos generales empleados por el tercero certificador para verificar los suscriptores. La declaración incluye también referencias a otras fuentes confiables que pueden verificar la autenticidad de la misma autoridad certificadora.

El receptor, tras la recepción del documento encriptado, puede acceder a la recopilación de certificados de la autoridad certificadora, y ver el certificado del suscriptor. Si no existe ningún certificado válido para el suscriptor, el recipiente será notificado de que la integridad de la firma digital puede ser dudosa, y que la firma podría ser una falsificación. Sin embargo si existe un certificado válido en la recopilación, el receptor puede utilizar la clave pública mencionada en el certificado para leer el mensaje firmado.

5.2 La admisibilidad de la firma electronica

En la mayor parte de los países de las familias de derechos neorromanista y del Common law, la cuestión de la admisibilidad de la firma electrónica se caracteriza por una falta de reconocimiento legislativo expreso. Sin embargo, sería inexacto concluir de esta constatación que este tipo de firma no goza de cierto reconocimiento jurídico.

5.2.1 Los países de derecho neorromanista y México

De manera general, podemos distinguir la existencia de dos grandes sistemas probatorios: el de la prueba "libre", en el cual cualquier procedimiento que pueda convencer al juez puede ser utilizado, y el de la prueba legal en el cual las formas aceptables son enumeradas de forma limitativa en la legislación.

En los países de derecho neorromanista, estos dos sistemas coexisten. En principio, la prueba de todo acto jurídico debe, en materia civil y mercantil, hacerse por escrito, limitando así los métodos de prueba admisibles. En Francia, la reforma del derecho probatorio que se operó en 1980[79], además de extender el ámbito de la libertad de prueba, introdujo varias excepciones al principio de la necesidad del escrito. La prueba podrá hacerse libremente en los casos siguientes:

- la cuantía es inferior a cierto monto;

- existe una imposibilidad material o moral de encontrar el escrito ("la ausencia de prueba escrita que resulta del uso de los nuevos métodos de transferencia de datos puede constituir una imposibilidad material");

- las partes se ponen de acuerdo para renunciar a la aplicación de la regla del escrito a través de una convención sobre prueba;

- cuando se trate de un contrato entre comerciantes dónde la regla del escrito no tiene aplicación.

En suma, las varias derogaciones mencionadas tienen como efecto atenuar considerablemente la aparente rigidez del principio del escrito. Es lo que concluye Michel Flammée en el "Informe Belga" acerca de los nuevos métodos de reproducción, cuando escribe:

> La aplicación de la regla de derecho civil de preeminencia del escrito (...) solo en raras ocasiones encontrará aplicación. Es probablemente lo que explica la ausencia de decisiones jurisprudenciales en la materia[80].

Es menester que nos interesemos ahora en las implicaciones de este principio para la admisibilidad de la firma electrónica. Para estos efectos, cabe notar en primer lugar que la prueba documental puede establecerse por dos tipos de escritos: el acto auténtico y el acto sin legalizar. Este último es el que contiene un acto jurídico, lleva la firma de las partes, y fue establecido sin la presencia de un oficial público; no se supone que debe llenar ningún requisito de forma adicional.

No se exige la firma en el escrito para que el acto tenga validez, ya que la formación de los contratos es, en principio, consensual. El escrito solo juega su papel como método de prueba cuando ha sido firmado por las partes. En virtud de la primacía del escrito, la mayoría de los autores franceses llegan a la conclusión que esta firma debe ser manuscrita, a pesar de que el derecho sustantivo no impone de ninguna manera tal obligación:

---

[79] Ley no. 80-525 del 12 de julio de 1980 sobre de la prueba de los actos jurídicos.
[80] Flamee, M., "Rapport belge", *Les nouveaux moyens de reproduction*, Paris: Economica, 1986, p.140.

> La exigencia de un escrito como tal (independientemente de toda firma) no esta claramente especificada en la ley. Sin embargo, no cabe duda que se desprende de la noción misma del acto, la firma tiene su razón de ser en la existencia del escrito al cual corresponde[81].

El autor francés considera sin embargo que la "necesidad de un escrito" no hace referencia a ningún soporte en particular. Por lo mismo, la firma tampoco tiene que ser manuscrita. Según este autor, el derecho francés solo exige en esta materia un procedimiento de identificación por medio del cual la persona que lo utiliza manifiesta su consentimiento.

Existen en Francia varios fallos que han tratado de la aceptabilidad de los modos alternativos de firma. Sin embargo, en cada uno de estos fallos, los mecanismos de firma considerados han sido considerados aceptables, porque fueron utilizados en un contexto de prueba libre, o porque las partes se encontraban vinculadas por un convenio. Estas decisiones demuestran de todas formas la voluntad pragmática de los magistrados de adaptar los sistemas de pruebas a la era de la nueva tecnología.

Por otro lado, aunque ningún texto jurídico francés reconoce el intercambio de datos informático, el derecho francés prevé una excepción notable al formalismo jurídico: cualquier declaración de una empresa que sea dirigida a una administración gubernamental puede hacerse por vía

[81] Hollande, A., *Droit de l'informatique et de la télématique*, Paris: J. Delmas et Cie, 1990, p. 143.

electrónica, y tendrá la validez de una declaración escrita que tenga el mismo objeto[82].

El mensaje electrónico se substituye entonces al documento escrito correspondiente, de tal forma que cualquier consideración de prueba solo se pueda aplicar al mensaje electrónico. Como lo explica Thierry Piette–Condol, "esta disposición del derecho francés es más general acerca del vector de la transmisión; al hacer referencia a la vía electrónica, abre ampliamente el uso de todos los tipos de tecnologías de la información y de la comunicación"[83], y esto obviamente incluiría la firma electrónica.

En México, se opto por legislar en materia de firma electrónica en base al derecho común, y no estableciendo una ley especifica sobre la materia, como por ejemplo en los casos de España y Colombia[84].

5.2.2 Los sistemas de Common law

En la mayoría de los países del Common law, la admisibilidad de la prueba informática descansa por empezar en leyes específicas, como el *Computer Evidence Act* de Sudáfrica[85], o también en varias disposiciones incluidas en las leyes generales sobre prueba.

Pero sin importar si emanan de leyes específicas o generales, las disposiciones legislativas en relación con la admisibilidad de la prueba informática tienen en común el hecho de abordar esta cuestión únicamente

[82] Ley no.94-126 del 11 de febrero de 1994 sobre la iniciativa y la empresa individual, en su articulo 4.
[83] Véase: Piette-Coudol, T., "L'echange de données informatisé selon la loi francaise", *CyberNews*, www.droit.umontreal.ca/crdp/CyberNews/Art3_No195.html.
[84] Véase el Decreto publicado en el *Diario oficial*, precitado.

en un marco muy general. De tal forma que normalmente, no encontramos disposiciones particulares acerca de la firma electrónica. Por eso es más bien en las reglas del Common law (el derecho común jurisprudencial), que tenemos que enfocar nuestro análisis.

El Common law no propone ninguna definición formal de la noción de firma. Según Sydney Lowell Phipson, nada en el Common law deja suponer que ésta debe ser manuscrita para producir sus efectos: "Como regla general, hasta cuando la firma se requiere por ley y para documentos solemnes, una firma manual no es necesaria"[86].

Ian Wolder, apoyándose en la definición común de la noción de firma, opina lo mismo:

> El concepto reconocido de la firma implica la escritura manual del nombre del signatario en el documento de que se trata. Es claramente imposible firmar un documento producido y transmitido por telemática de esta forma (...) ¿Es posible idear y reconocer jurídicamente un equivalente telemático de la firma? El *Concise Oxford Dictionary* define "firmar" como "reconocer o garantizar (carta, deuda, cuenta, etc.) como la propia producción de uno o como teniendo la autoridad o el consentimiento de uno como fijando o habiendo fijado el nombre o las iniciales de uno o una marca reconocida". No es por lo tanto necesario que una firma consista en el nombre del signatario o que sea

[85] Computer Evidence Act, No. 57 of 1983
[86] Phipson, S., *Phipson on Evidence*, Londres: Sweet & Maxwell, 1990, no. 35-04.

> manuscrita, y verdaderamente este enfoque viene reflejado por los casos en los cuales las cortes han tenido que considerar el significado de los requisitos de la firma en varios contextos[87].

Las cortes han efectivamente afirmado, en varias ocasiones, que la firma puede presentarse bajo una forma que sea otra que la manuscrita, como una marca, una estampilla, o iniciales. Solo basta con que los atributos básicos de la firma sean presentes, es decir:

- una marca cualquiera;
- única del signatario;
- fijada a un documento firmado;
- puesta con la intención de expresar un consentimiento y de autentificar el contenido del acto firmado.

Cuando todos estos atributos están reunidos, nada se opone a la admisibilidad de la firma electrónica:

> A la luz de estas autoridades (...) pareciera que las comunicaciones telemáticas podrían tener firmas si los elementos esenciales de la firma pueden ser duplicados (...). Si un equivalente electrónico satisface los requisitos básicos de singularidad y de intención de

[87] Walden, I. (Dir.), *EDI and the Law*, Londres: Blenheim Online, 1989, p. 33.

autentificar, debería de poder ser reconocible por la ley[88].

Sin embargo, es importante mencionar que varias leyes exigen de manera expresa la utilización de técnicas de autenticación tradicionales, como el sello o la firma manuscrita. Según la mayoría de los autores, varias modificaciones legislativas son necesarias para remediar esta situación.

En esencia, los obstáculos legislativos que existen en los países de Common law acerca de la admisibilidad de la firma electrónica, son ampliamente compensados por la actitud liberal de los tribunales y de la doctrina. Es razonable opinar que estos obstáculos serán removidos por vía legislativa en varios países en un futuro cercano.

5.2.3 El caso de los Estados Unidos de Norteamérica

Históricamente, el derecho de los Estados Unidos se ha mostrado generalmente abierto frente a las nuevas tecnologías. La recepción que los tribunales norteamericanos han tradicionalmente reservado a los adelantos tecnológicos permite hoy en día una interpretación amplia y liberal del concepto de firma.

A este punto, cabe sin embargo notar que pareciera que dos leyes están de alguna forma obstaculizando la admisibilidad de la firma electrónica: el *Statute of Frauds* y el *Federal Rules of Evidence*.

[88] Saxby, S. (Ed.), *Encyclopedia of Information Technology Law*, Londres: Sweet & Maxwell, 1990, p. 5069.

5.2.3.1 El *Statute of Frauds*

No es posible hablar de la admisibilidad de la firma electrónica en Estados Unidos de Norteamérica sin enfocarse en las exigencias del *Statute of Frauds*, incorporadas en las disposiciones del *Uniform Commercial Code* (UCC) de los Estados Unidos. El artículo 2–201 en su primer párrafo condiciona en efecto la validez de varios actos a su firma:

> 2–201. Salvo que se disponga de otra forma en este artículo, un contrato para la venta de bienes para el precio de $500 o más no puede ser impugnado por una acción o una defensa a menos que haya algún escrito suficiente para indicar que se ha hecho un contrato de venta entre las partes, y firmado por la parte en contra de la cual se busca la ejecución o por su agente o corredor autorizado.

La exigencia de un escrito, como lo prevé esta disposición parece constituir un obstáculo jurídico importante a la desmaterialización de transacciones como la venta de bienes, y la utilización de mecanismos de firma electrónica. Sin embargo, la definición de firma, enunciada por el UCC, parece amplia y liberal. Según el artículo 201 (39), la firma incluye cualquier símbolo ejecutado o adoptado por una parte con la intención de autenticar un acto.

Apoyándose en esta definición, la jurisprudencia norteamericana reconoce, como la mayor parte de los sistemas jurídicos analizados anteriormente, las manifestaciones siguientes de la firma: la

mecanografiada, la facsimilada, las iniciales, una "X", una estampilla. Esta enumeración no es exhaustiva.

En la apreciación de la aceptabilidad de las firmas no manuscritas, los tribunales tienen también en cuenta los usos y las costumbres comerciales correspondientes al medio utilizado para contratar. Según el UCC, los tribunales deben en esta materia, tomar en cuenta las prácticas comerciales usuales, y utilizar su sentido común. Según un autor, la reticencia de los tribunales en intervenir en las prácticas comerciales es un factor favorable a la admisibilidad de la firma electrónica[89].

El análisis de los fallos de los tribunales norteamericanos permite enfocar la más importante exigencia relacionada con la firma, es decir: la identificación formal de los signatarios según las modalidades determinadas por las partes contratantes. La admisibilidad de las firmas no manuscritas depende, prácticamente, de la voluntad expresa o tácita manifestada por esas partes.

Su admisibilidad depende, por lo menos en parte, de la prueba de esta intención. Depende también de la capacidad del método de firma determinado por las partes, de verdaderamente realizar su función primordial de identificación. Sin embargo, ninguna disposición del *Statute of Frauds* del UCC especifica el nivel de seguridad necesario a la realización de esta función. En lo que atañe a esta cuestión, nuestro análisis debe enfocarse más bien en las reglas del Federal *Rules of Evidence*.

[89] Thomas, J., "Legal Responses to Commercial Transactions Employing Novel Communications Media", (1992) 90 *Mich L .R.*. 1145.

5.2.3.2 El *Federal Rules of Evidence*

Aunque las exigencias del *Statute of Frauds* y del Federal Rules of *Evidence* son independientes, siguen siendo íntimamente vinculadas. En el derecho federal de los Estados Unidos, las reglas que nos interesan particularmente se encuentran en los artículos 901 y 902 del *Federal Rules of Evidence*. La fracción (a) del artículo 901, que rige de forma general la exigencia de autenticación de la prueba, menciona que esta exigencia está satisfecha cuando la prueba es suficiente para apoyar las pretensiones de la parte. La fracción (b) de este artículo prevé varios ejemplos de procesos de autenticación o de identificación.

El artículo 902 consiste por su lado en una lista de documentos calificados "self-authenticating", es decir que no necesitan prueba alguna acerca de su autenticidad. Algunos documentos comerciales, los documentos públicos extranjeros, así como las publicaciones oficiales son por ejemplo considerados como tales. Aunque de forma hipotética, es razonable imaginar algunos documentos autenticados gracias a un mecanismo de firma electrónica, como "self-authenticating" por presentar garantías inherentes de seguridad, la enumeración del artículo 902 sigue siendo precisa y limitativa. En esta óptica, solo una enmienda legislativa permitiría integrarle los documentos autenticados electrónicamente.

Sin embargo, cabe terminar este análisis subrayando que a pesar de la existencia de algunos obstáculos, los tribunales norteamericanos adoptan para con el *Federal Rules of Evidence*, un acercamiento liberal consecuente con la admisibilidad de la firma electrónica.

5.2.4 Los esfuerzos de codificación

Hablaremos aquí de los esfuerzos de codificación realizados en Estados Unidos. Analizaremos el *Utah Digital Signature Act*[90] y también las *Digital Signatures Guidelines* de la American Bar Association, así como la reciente ley federal impulsada por el Presidente Clinton.

5.2.4.1 El *Utah Digital Signatures Act*

Vigente desde el 1ro de mayo de 1995, esta ley constituye la primera legislación dedicada exclusivamente a la firma electrónica, y que reconoce su admisibilidad de manera expresa. El Utah Act prevé en efecto que un documento firmado de forma electrónica es tan válido como un documento realizado mediante un papel.

Cabe notar el carácter limitativo de la expresión "firmado electrónicamente", ya que en el Utah Act, la criptografía asimétrica o firma numérica, constituye el único mecanismo de firma electrónica que permite firmar electrónicamente un documento. La noción de firma electrónica viene de hecho definida con una referencia precisa al funcionamiento técnico de este mecanismo:

> "firma digital" significa una transformación de un mensaje utilizando un criptosistema asimétrico tal que una persona que tenga el mensaje inicial y la clave pública del signatario puede precisamente determinar: (a) si la transformación fue creada usando la clave

privada que corresponde a la clave pública del signatario; y (b) si el mensaje fue alterado desde que se hizo la transformación[91].

Esta definición deja muy poco lugar a la interpretación. Impone a la criptografía asimétrica como mecanismo único de firma electrónica, excluyendo cualquier otro mecanismo basado por ejemplo en la biometría o el uso de códigos secretos.

La utilización de la criptografía asimétrica no es sin embargo suficiente en sí para asegurar la realización de las funciones de la firma, es decir la identificación del signatario y la manifestación de su voluntad para adherir el acto que firma. Para lograrlo, el Utah Act prevé en efecto la utilización de los servicios de autoridades certificadoras encargadas de emitir certificados de identificación[92].

Según el Utah Act, algunas presunciones importantes se desprenden del uso de certificados. Por ejemplo, las firmas numéricas verificadas (descifradas) exitosamente mediante el uso de una clave pública encontrada en un certificado se presumen haber sido fijadas por el signatario, y son reconocidas como tal[93]. Por otro lado, cuando es verificada exitosamente con el uso de la clave pública complementaria, una firma numérica realizada gracias a una clave privada se presume puesta por el signatario con la intención de autentificar el mensaje, y expresa su voluntad de adherir al contenido del mensaje[94].

---

[90] www.state.ut.us/ccjj/digsig/.
[91] *Id.*, artículo 103(10).
[92] *Id.*, artículo 401.
[93] *Id.*, artículo 405.

Cualquier firma realizada con el auxilio de una clave privada, y verificada por la clave pública complementaria se presume válida, y podemos entender fácilmente la necesidad para el tenedor de una clave privada, de preservar el control y la confidencialidad de ésta. En caso de que se utilizara de manera no autorizada una clave privada, correspondería a su verdadero dueño rechazar la presunción de que la firma realizada gracias a esta clave constituye una firma autorizada que refleja verdaderamente su deseo de adherise al mensaje firmado.

El Utah Act dispone en este sentido que una clave privada es propiedad de su tenedor y que por esta razón, tiene que ejercer una diligencia razonable para conservar su control y confidencialidad.

5.2.4.2 Las *Digital Signatures Guidelines*[95]

Este documento, elaborado por expertos de la American Bar Association, tiene como objetivos favorecer el florecimiento de legislaciones acerca de la firma electrónica en los Estados Unidos como en el extranjero[96]. Uno de los objetivos de este proyecto es proponer principios de derecho aplicables en la mayor parte de los sistemas jurídicos. Por lo mismo, los autores del documento vienen de varios países europeos y de Canadá, sumándose a los juristas norteamericanos especializados en seguridad.

---

[94] *Id.*, artículo 406(b).
[95] American Bar Association, "Digital Signature Guidelines", 5 de octubre de 1995.
[96] Cabe de hecho mencionar que este texto ha sido traducido al castellano, con el objetivo que se adoptara en los países de habla hispana.

La importancia de este trabajo es innegable, y seguramente tendrá repercusiones en la redacción de varias leyes en los próximos años. Hay que notar también que estos expertos han colaborado con las autoridades gubernamentales del estado de Utah, así que no hay que sorprenderse de las semejanzas que encontremos con el *Utah Digital Signatures Act.*

En este sentido, las *Digital Signatures Guidelines* le dan a la firma electrónica una validez jurídica plena. Se considera también que, en presencia de una regla de derecho que imponga la firma de un acto o que prevea algunas consecuencias por falta de firma, esta regla jurídica esta satisfecha con el uso de una firma electrónica.

El mecanismo de firma electrónica al cual se refieren las *Digital Signatures Guidelines* es definido, de forma exclusiva como la criptografía asimétrica o firma numérica.

Debido a esta posición, el documento esta expuesto a las mismas críticas que mencionábamos anteriormente acerca del carácter restrictivo del Utah Act. Sin embargo, a diferencia de éste último, cabe notar que las *Digital Signature Guidelines* no desechan la posibilidad de utilizar otros "mecanismos de firma" admisibles en relación con otras leyes norteamericanas como el *Uniform Commercial Code.*

El uso de servicios de autoridades de certificación es, por otro lado, obligatorio para realizar las funciones de la firma. A menos de disposiciones contrarias, la validez de una firma numérica solo se reconoce si puede ser verificada por el uso de la una clave pública que se encuentre en un certificado de identificación válido y disponible.

Varias presunciones se desprenden del uso de una firma numérica y de un certificado de identificación. Principalmente, se presume que toda la información confirmada por una autoridad de certificación y contenida en un certificado válido, es exacta. Por otro lado, se presume que una firma electrónica verificada a través de una clave pública contenida en un certificado, constituye la firma de la persona identificada en el certificado.

La confidencialidad de la clave privada que permite realizar la firma asume, aquí también, una gran importancia. Las *Digital Signature Guidelines* manifiestan de hecho que esta obligación de confidencialidad se mantiene en todo momento.

5.2.4.3 El *Electronic Signatures in Global and National Commerce Act*

Pareciera que desde el 1° de octubre del 2000, el paisaje jurídico norteamericano relativo a las firmas digitales se ha modificado, con la entrada en vigor de la Ley sobre las firmas electrónicas en el comercio global y nacional.

Cuando el Presidente Clinton firmo esta Ley – con una "smart card" y una pluma normal – él hizo posible que los Norteamericanos firmen algunos contratos con fuerza jurídica vinculante, como prestamos para la compra de una casa, hipotecas, a través de sus computadoras. Sin embargo, los testamentos, contratos de adopción, y los convenios de divorcio y las leyes todavía tendrán que ser firmados con plumas normales. La Ley es neutral por lo que atañe a la tecnología, dejando en el aire la forma en la cual las firmas digitales serán puestas en operación.

Según la Ley, una firma digital es "un sonido, símbolo o proceso electrónico vinculado a, o lógicamente asociado con, un contrato u otro archivo y ejecutado o adoptado por una persona con la intención de firmar el archivo".[97] Para dar el ejemplo, Clinton firmo la Ley en soporte de papel en Filadelfia, y luego inserto una tarjeta ("smart card") en una computadora, y tecleo una clave para que apareciera su firma en la pantalla. Clinton afirmo que los contratos en línea tendrán ya la misma validez jurídica que los contratos escritos en un soporte de papel.

Esta Ley ha sido fuertemente criticada por los defensores del derecho a la privacidad, frente al temor que los gobiernos o la industria puedan utilizar las firmas para construir enormes bancos de datos de consumidores o ciudadanos sin su consentimiento y conocimiento. Según los expertos, la misma tecnología tiene problemas intrínsecos, el mas importante de los cuales seria que no existe una forma absolutamente segura de crear firmas digitales, o que una persona pueda utilizarlas.

Las firmas son tan seguras como la computadora con la cual son utilizadas. Esto quiere decir que no son normalmente muy seguras, según Nestor Zwyhun, director de asuntos tecnológicos de TradeCard, una empresa que utiliza las firmas digitales para concluir muchas transacciones de comercio electrónico en Internet: el algoritmo matemático mas poderoso de este mundo es inútil si descansa en un sistema operativo que tiene fallas[98].

---

[97] www.abcnews.com/sections/tech/Daily News/digitalsignatures000628.html.
[98] *Id*

Los expertos dan una larga lista de formas en las cuales las firmas digitales pueden ser robadas, y no tienen necesariamente que ver con descifrar el código de la firma. Si las claves privadas son almacenadas en los discos duros, es posible que algún virus u otro programa maligno pueda mandarlas a criminales, como el virus "Love bug" intento hacerlo con las claves de Internet. Es también factible que un programa maligno haga que una persona firme cosas que no quiere firmar, poniendo en la pantalla un documento, y firmando digitalmente otro que nunca apareció en la pantalla.

No es solamente el algoritmo que conforma la firma digital que puede ser la fuente de problemas, sino todo el medio en el que se encuentra uno cuando quiere firmar un documento digitalmente.

5.2.5 La experiencia europea

La Unión Europea ha adoptado una Directiva sobre un marco comunitario para las firmas electrónicas[99]. Es la primera ilustración concreta del acercamiento flexible e integrado de la Comisión Europea para crear un marco europeo de desarrollo del comercio electrónico. Esta nueva legislación hará que se extienda el reconocimiento jurídico a las firmas electrónicas.

Los principales elementos de la Directiva son:

- el reconocimiento jurídico: la Directiva prevé que una firma electrónica no puede ser descartada jurídicamente por la única razón

[99] "Directive 1999/93/CE du 13 decembre 1999 sur un cadre communautaire pour les signatures electroniques", www.europa.eu.int/comm/internal_market/fr/media/sign/99-915.htm.

de su forma electrónica. Si el certificado y el proveedor del servicio, como la misma firma, llenan una serie de especificaciones, la firma será automáticamente considerada como teniendo la misma validez que una firma manuscrita. Además, las firmas electrónicas adquirirán fuerza probatoria en los procedimientos judiciales;

- la libre circulación: todos los productos y los servicios relacionados con las firmas electrónicas podrán circular libremente, y solamente serán sometidos a la legislación y al control del país de origen. Los Estados miembros no podrán someter la prestación de servicios relacionados con las firmas digitales, a un régimen de autorización obligatorio;

- responsabilidad: la legislación prevé un mínimo de reglas de responsabilidad que incumben a los proveedores del servicio, especialmente en lo que atañe al contenido del certificado. Este acercamiento asegura la libre circulación de los certificados y de los servicios de certificación en el seno del mercado interno, refuerza el sentimiento de confianza de los consumidores y alienta los operadores a desarrollar sistemas seguros, sin que existan legislaciones demasiado restrictivas o apremiantes;

- un marco tecnológicamente neutral: dada la rapidez de las innovaciones tecnológicas, la Directiva prevé el reconocimiento de las firmas electrónicas sin importar la tecnología empleada (por ejemplo, las firmas digitales que emplean la criptografia asimétrica o biometrica);

- ámbito de aplicación: la legislación cubre la expedición de certificados al publico con el objetivo de identificar el expedidor de un mensaje electrónico. De acuerdo con los principios de la autonomía de las partes y de la libertad de contratar, la legislación autoriza sin embargo el funcionamiento de sistemas regidos por contratos de derecho privado, como redes Intranet de empresas o de sistemas bancarios, donde una relación de confianza ya existe, y donde no existe una necesidad evidente de reglamentación;

- dimensión internacional: con el afán de promover un mercado global del comercio electrónico, la Directiva incluye mecanismos de cooperación con terceros países, en el fundamento de un reconocimiento mutuo de certificados, o de acuerdos bilaterales o multilaterales.

5.3 Propuestas para una ley eficaz

Aunque las *Digital Signature Guidelines* son un punto de partida interesante para tratar de reglamentar el uso de las firmas electrónicas, muchos expertos consideran que tiene algunas fallas que es imprescindible remediar. Para ser exitosa, una legislación sobre firmas electrónicas tiene que considerar por lo menos tres puntos fundamentales: la verificación de la información personal, el establecimiento de la clave, y la confiabilidad para el receptor.

5.3.1 Verificación de la información personal

Este es probablemente el elemento más crítico de un sistema de firma digital[100]. La autoridad certificadora tiene que verificar la información personal del suscriptor. El receptor va a confiar en gran parte en la revisión por parte del tercero certificador, de la identidad del suscriptor. Si la autoridad no logra verificar adecuadamente la identidad del suscriptor, un impostor podría usurpar la identidad del signatario, obtener un par de claves, y empezar a ejecutar contratos utilizando esta falsa identidad. El receptor ignoraría este fraude hasta después de haber adherido al contrato y buscado sus efectos.

Ya que la integridad del sistema descansa ampliamente en la veracidad de las representaciones hechas por la autoridad certificadora en el certificado, ella tiene que adoptar los métodos suficientes para confirmar la identidad del suscriptor y la integridad de sus claves.

Para permitir cierto grado de flexibilidad, una ley eficaz debería autorizar varios métodos alternativos para la verificación de la identidad[101], que sean confiables sin ser una carga demasiado pesada para el suscriptor. Por ejemplo, la autoridad podría confirmar la identidad a través del contacto con otra autoridad certificadora. Si el suscriptor ya posee un conjunto de claves por parte de otra autoridad, ésta ya habría emitido su propio certificado acerca del suscriptor. La segunda autoridad podría entonces confiarse en la existencia de este certificado y su contenido para su propia verificación de la identidad del suscriptor. Obviamente, la confiabilidad del segundo certificado sería dependiente de la calidad de los procesos de

[100] Véase Saxby, S., *op. cit.*, p. 566.
[101] Trudel, P., *op. cit.*, p. 344.

verificación utilizados en la primera certificación. Además, dependiendo en la regulación de las autoridades certificadoras que se podrían dar, la primera autoridad certificadora podría falsificar el certificado del suscriptor, si es una "mala" autoridad.

Una alternativa sería requerir una verificación del suscriptor en persona. Sería como la práctica de comparecer en persona frente a un notario, con la documentación personal correspondiente[102]. La autoridad certificadora le pediría al suscriptor que se presentara en su oficina antes de emitir un certificado. Esto seguramente limitaría los episodios de fraude, pero al mismo tiempo iría en contra de la misma idea de un contrato en línea. La premisa básica del comercio electrónico y de las firmas digitales, es permitir al usuario manejar sus negocios sin tener que viajar físicamente a ningún lado. Aunque este proceso de verificación solo tendría lugar una vez, algunos puristas del Internet podrían pensar que los objetivos de los contratos electrónicos son defraudados por este inconveniente.

Otro aspecto imprescindible acerca de la identificación del suscriptor es la necesidad de confirmar constantemente la veracidad de la información. Además de la verificación inicial, la autoridad certificadora tiene que volver a verificar esta información durante el período de validez del certificado. Durante este período, el hombre y la dirección del suscriptor pueden cambiar. Un certificado es inútil si los datos que aparecen son exactos al principio, pero luego contiene datos falsos o incorrectos.

Para un sistema eficaz, el receptor tiene que poder confiar en cualquier momento de la vida útil del certificado. Esto obliga a una nueva

[102] Adam, N., *Electronic Commerce: Technical, Business and Legal Issues*, New Jersey: Practice Hall, 1999, p. 121.

verificación de la información, a través de los mismos métodos utilizados para verificar la información originalmente. Una disposición que obligara el suscriptor a notificar la autoridad en caso de cambios no parece tener el mismo alcance que el control continuo de la autoridad certificadora.

Esto es congruente con la analogía del notario: un signatario tiene que presentar una prueba de identidad cada vez que quiere utilizar sus servicios para algún acto. La notarización se aplica solamente para el documento adjunto, y no puede ser utilizada para cualquier otra transacción.

Es importante ponernos en el lugar del receptor para comprender que si no existe en la ley una obligación para que la autoridad tenga que volver a verificar la información contenida en el certificado con intervalos regulares, la popularidad del sistema de firmas digitales podría ser profundamente afectado. Sería oportuno que la autoridad mencionara, en el certificado del suscriptor, la fecha de la última verificación. De esta forma, el receptor podría considerar la confiabilidad de la firma digital que recibió, en base al tiempo que ha transcurrido desde la última certificación.

5.3.2 Establecimiento de las claves

El siguiente elemento para el éxito del sistema de firma digital es el establecimiento de las claves. Ya que la operabilidad del sistema depende del funcionamiento adecuado del par de claves, que impidan el acceso indebido de un tercero a los documentos firmados, una ley eficaz tiene que ser explícita sobre la manera de generar estas claves, y los estándares informáticos con los cuales se pueda juzgar la seguridad de las claves.

Por empezar, parece evidente que no se puede permitir que el suscriptor genere sus propias claves. Si este caso fuese permitido, el suscriptor podría generar un sistema de claves que le permitiría alterar documentos firmados digitalmente, después de su transmisión. Aunque un par de claves pueda ser "impropio", la autoridad certificadora no necesariamente sería capaz de detectar la irregularidad, y podría considerar las claves y el sistema utilizado para generarlas como "confiable"[103]. La carga de algún daño financiero quedaría en la responsabilidad del receptor, ya que la autoridad certificadora no podría hacer nada.

Aunque el suscriptor genere las claves de buena fe, la falta de estándares para el sistema de generación podría afectar seriamente la operación del sistema de firmas. La solución a este problema pareciera ser la creación de una entidad que se encargaría exclusivamente de generar claves. Este servicio podría ser regulado por la misma ley, de forma semejante a la autoridad certificadora, y sería operado por un tercero neutral cuya tarea única sería generar pares de claves, utilizando un estándar de firmas digitales apropiado. El suscriptor utilizaría este servicio para generar sus claves en conformidad con los estándares utilizados por su autoridad certificadora.

El requerimiento de utilizar un sistema independiente de generación de claves no tendría repercusiones sobre la popularidad de las firmas digitales. El costo de compra de las claves sería mínimo, y aseguraría las partes interesadas de la integridad del par de claves, ya que el tercero neutral no tendría interés en generar un par de claves no confiables. Este servicio además ayudaría al suscriptor a determinar el estándar optimal que utilizar para sus necesidades particulares.

[103] Véase Jaksetic, *op. cit.*, p. 21.

Finalmente parece importante establecer una vida útil para las claves. Como la tecnología sigue avanzando, las claves más viejas, que tal vez eran invulnerables en la época de su creación, pueden llegar a ser vulnerables. Además, más tiempo dura una clave, y más grande es la probabilidad que sea revelada accidentalmente a un tercero. Una ley que obligara el suscriptor a volver a generar nuevas claves regularmente, aseguraría una alta calidad en estas claves, sin comprometer el uso del sistema de firmas digitales.

5.3.3 Confiabilidad para el receptor

Otro obstáculo importante para el éxito de una ley sobre firmas digitales es la presencia de riesgo para el receptor del documento firmado. El receptor es la persona que puede perder más en el caso de un documento falsificado o de alguna otra forma impropio. Por lo mismo, antes que un sistema pueda ser utilizado ampliamente en las transacciones comerciales, los receptores deben estar seguros que recibirán una protección jurídica adecuada en el ámbito de una ley sobre firmas digitales. Los redactores tienen que incluir unas protecciones fuertes en el sistema para que el receptor pueda confiar en el documento firmado, y creer que las cortes reconocerán el contrato y su validez, y obligarán al signatario a cumplirlo.

La ley ideal aseguraría que la responsabilidad de verificar la autenticidad de las firmas recayera en la autoridad certificadora, por ejemplo. Esta entidad se encuentra en la mejor posición para valorar la credibilidad de la información del suscriptor y de la integridad de las claves,

los dos componentes esenciales del sistema de firmas digitales. Además, las autoridades certificadoras son las que más tienen que ganar de un sistema funcional y confiable.

Obviamente, si un receptor esta enterado que una firma es falsificada o que no es confiable por alguna otra razón, parece normal que se le impida recibir cualquiera compensación en calidad de daños y prejuicios.

Conclusiones

Las investigaciones que hicimos para la redacción del presente trabajo, no llevan a formular las siguientes conclusiones:

PRIMERA – Las practicas comerciales y las costumbres del derecho del comercio electrónico no se han cristalizado todavía, y por esta razón existen todavía incertidumbre y desconfianza que hacen que varios usuarios de Internet no quieran hacer transacciones electrónicas.

SEGUNDA – Entre los sistemas de pago por Internet, algunos están recibiendo una aceptación creciente, como es el caso del dinero electrónico, que minimiza los riesgos de fraude y de robo, aunque queda la posibilidad remota de una acción ilícita por "piratas informáticos"

TERCERA – En varias jurisdicciones, el sistema probatorio carece de reconocimiento del documento informático como una prueba aceptable. Sin embargo, en varios Estados se concede a los particulares la posibilidad de negociar un convenio privado sobre la prueba, que permita tomar en cuenta los documentos informáticos. También existe la posibilidad para los contratantes de elegir un derecho que reconoce los documentos informáticos, como aplicable al contrato.

CUARTA – La mayoría de las jurisdicciones que han legislado para su territorio acerca del comercio electrónico, han tomado en cuenta la necesidad de proteger al consumidor, especialmente frente al desarrollo muy rápido que conoce el Internet comercial.

QUINTA – La firma electrónica parece ser la forma más segura de realizar negocios en Internet, aunque todavía existe mucha incertidumbre acerca de cómo hay que reglamentarla (hasta un país tan vanguardista como Estados Unidos de Norteamérica no menciona en su reciente Ley sobre la aceptación de las firmas electrónicas, la manera en la cual se podrán generar para ser utilizadas). Sin embargo, los expertos del medio están de acuerdo para afirmar que la computadora a partir de la cual se utilizan no es normalmente inviolable, y existe la posibilidad de que una persona llegue a firmar un documento al cual no quería ser vinculado.

SEXTA – El sistema de criptografia asimétrica (con una clave publica, y una privada) constituye la manera más aceptable de lograr una firma electrónica funcional, ya que permite llenar los requisitos de autentificacion

del documento. La intervención de una entidad certificadora independiente en el proceso (como un cibernotario) es una buena garantía del sistema, cuando viene utilizada en conjunción con una computadora confiable.

SEPTIMA – Una ley eficaz en materia de firma electrónica tendría que articularse en torno a tres ejes principales: la verificación de la información personal de la persona que quiere detener una firma electrónica (para corroborar que la firma corresponde a la persona que la ostenta); el establecimiento de las claves por un ente imparcial; y una confiabilidad aceptable para el receptor, que pueda estar seguro que la autenticidad de la firma del suscriptor fue verificada.

OCTAVA – Una forma de crear mas seguridad en el ámbito del comercio electrónico es a través de la armonización de las legislaciones, y de la cooperación judicial. Con una mayor uniformidad a nivel de las normas de fondo, de las normas procesales, y de las normas de conflictos jurisdiccionales, los usuarios se sentirán mas confiados en hacer transacciones comerciales en Internet. Existirá una mayor transparencia y previsibilidad del derecho. Cuando se hayan desarrollado métodos totalmente confiables para garantizar la validez de los contratos electrónicos, el contrato de papel se transformara en la carroza con caballo del nuevo milenio.

Bibliografía

1. Publicaciones oficiales

- Canada, *Stratégie canadienne sur le commerce électronique*, Ottawa, 1998.

- Estados Unidos de Norteamérica, *Economic Impact of the Information Technologies*, Washington, 1999.

- Estados Unidos de Norteamérica, *A Framework for Global Electronic Commerce*, www.iitf.nist.gov/eleccomm/ecomm.htm.

- OCDE, *Electronic Commerce: Opportunities and Challenges for Government*, Paris, 1997.

- OCDE, *The Economic and Social Impact of Electronic Commerce: Preliminary Findings and Research Agenda*, Paris, 1999.

- OMC, *Le commerce électronique et le rôle de l'OMC*, Ginebra, 1998

- UNCITRAL Working Group on Electronic Commerce, *Planning of Future Work on Electronic Commerce: Digital Signatures, Certification Authorities and Related Legal Issues*, 31st session, 1997.

• UNCITRAL, *Report by the Secretariat, Legal Value of Computer Records*, A/CN.9/269 (1985).

• UNCITRAL, *Reviews of Definitions of "writing", "signature" and "document" Employed in Multilateral Conventions and Agreements Relating to International Trade*, 1994.

2. Libros

• Adam, N., *Electronic Commerce: Technical, Business and Legal Issues*, New Jersey: Prentice Hall, 1999.

• Arrellano Gracia, C., *Métodos y técnicas de la investigación jurídica*, Mexico: Ed. Porrua, 1999.

• Barnes, H., *History of Historical Writings*, Londres: Dover Publications, 1890.

• Barrios Garrido, G., *Internet y derecho en Mexico*, Mexico: Ed. McGraw-Hill, 1998.

• Benoussan, A. (Dir.), *Le commerce électronique: aspects juridiques*, Paris: Hermès, 1998.

• Bertrand, A. y T. Piette-Coudol, *Internet et le droit*, Paris: Presses Universitaires de France, 1999.

• Blackstone, C., *Blackstone's Commentaries on the Laws of England*, Londres: The Legal Classics Library, 1983.

• Boele-Woelki, K. y C. Kessedjian (Eds.), *Internet: Which Court Decides? Which Law Applies? Quelle court decide? Quel droit s'applique?*, La Haya: Kluever Law International, 1998.

• Carrascosa Lopez, V., *El documento electrónico como medio de prueba*, Madrid: Ed. Comares, 1997.

• Chamot, C., *L'échange de données informatisé*, Paris: Presses Universitaires de France, 1997.

• Chissick, M., *Electronic Commerce: Law and Practice*, Londres: Sweet & Maxwell, 1999.

• Eco, U., *Como se hace una tesis*, Barcelona: Gedisa Ed., 1997.

• Gaudemet-Tallon, H., *Les conventions de Bruxelles et de Lugano – Compétence internationale, reconnaissance et exécution des jugements en Europe*, Paris: Librairie Generale de Droit et de Jurisprudence, 1993.

• Hagan, W., *A Treatise on Disputed Handwriting and the Determination of Genuine from Forged Signatures*, Londres: Sweet & Maxwell, 1894.

• Hance, O., *Leyes y negocios en Internet*, Mexico: McGraw-Hill, 1996.

• Linant, X., *Droit de l'informatique et de la télématique*, Paris: J. Demas et cie., 1990.

• Loshin, P. y P. Murphy, *Electronic Commerce: Online Ordering and Digital Money*, Rockland (Massachussetts): Charles River Media, 1997.

• Ouellet, C., *Qui fait la loi sur l'Internet?*, Quebec: Presses de l'Université Laval, 1998.

• Phipson, S., *Phipson on Evidence*, Londres: Sweet & Maxwell, 1990.

• Parisien, S. y P. Trudel, *L'identification et la certification dans le commerce électronique*, Cowansville (Quebec): Ed. Yvon Blais, 1996.

• Ready, N., *Brooke's Notary*, Londres: Sweet & Maxwell, 1992.

• Reboul, P. y D. Xardel, *Le commerce électronique: techniques et enjeux*, Paris: Eyrolles, 1997.

• Ruth, J. (Ed.), *The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues*, Washington: The Computer Law Association Current Issues Publications Series, 1996.

• Saxby, S., *Encyclopedia of Information Technology Law*, Londres: Sweet & Maxwell, 1990.

• Schelling, J., *Cyberlaw Canada*, Vancouver: Self-Counsel Press, 1998.

• Shaw, M., *International Law*, Cambridge: Cambridge University Press, 1997.

• Smith, G., *Internet Law and Regulation*, Londres: Sweet & Maxwell, 1999.

• Tellez, J., *Derecho informático*, Mexico: McGraw-Hill, 1996.

• Trudel, P., *Droit du cyberespace*, Montreal: Ed. Thémis, 1997.

• Walden, I. (Dir.), *EDI and the Law*, Londres: Blenheim Online, 1989.

• Witker, J., *Como elaborar una tesis en derecho*, Madrid: Ed. Civitas, 1986.

3. Artículos

• Austin, J., "The Law of Electronic Commerce and Digital Signatures: An Annotated Bibliography", 17 *J. Marshall J. Computer & Info. L.* (1999).

• Boss, A., "The Internet and the Law: Searching for Security in the Law of Electronic Commerce", 23 *Nova L. Rev.* (1999).

• Boss A., "Electronic Data Interchange Agreements: Private Contracting Toward a Global Environment", 13 *Nw.J.Int'l L. & Bus.* (1992).

• Flammée, M., "Rapport belge", en *Les nouveaux moyens de reproduction*, Paris: Economica, 1986.

• Gaillard, E., "La distinction des principes généraux du droit et des usages du commerce international", Paris: Etudes Pierre Bellet, 1993.

• Geist, M., "The Reality of Bytes: Regulating Economic Activity in the Age of the Internet", 73 *Wash. L. R.* (1998).

• Greguras, F., "Electronic Commerce: On-line Contract Issues", www.batnet.com/oikoumene/ec_contracts.html.

• Jaksetic, E., "How to Ensure the Integrity of Digitally Transmitted Documents", *Corp. Legal Times*, Aug. 1996.

• O'Rourke, M., "Progressing Toward a Uniform Commercial Code for Electronic Commerce or Racing Towards Nonuniformity?", 14 *Berkeley Tech. L. J.* (1999).

• Piette-Coudol, T., "L'échange de données informatisé selon la loi francaise", *CyberNews*, www.droit.umontreal.ca/crdp/CyberNews/Art3_No195.html.

• Piette-Coudol, T., "Convention cadre pour le commerce électronique: commentaires et contrat", (1996) *CyberNews*, www.droit.montreal.ca/crdp/CyberNews/.

• Robertson, R., "Electronic Commerce on the Internet and the Statute of Frauds", 49 *S.C. L. Rev.* (1998).

• Rocher, G., "Pour une sociologie des ordres juridiques", (1988) *Cahiers de Droit* 91.

• Smedinghoff, T., "Moving with Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce", 17 *J. Marshall J. Computer & Info. L.* (1999).

• Shapiro, A., "The Disappearence of Cyberspace and the Rise of Code", 8 *Seton Hall Const. L.J.* (1998).

• Stein, A., "The Unexceptional Problem of Jurisdiction in Cyberspace", 32 *Int'l Law* (1998).

• Thomas, J., "Legal Responses to Commercial Transactions Employing Novel Communications Media", 90 *Mich. L. R.* (1992).

4. Sitios web de interés

- www.abanet.org
- www.findlaw.com
- www.Cybertribunal.org
- www.oea.org
- www.oecd.org
- www.strategis.ic.gc.ca
- www.lafirmadigital.com
- www.lawbytes.com