EL COMERCIO ELECTRÓNICO
Algunas nociones de seguridad*

Gladys Stella Rodríguez **

Resumen

Una de las consecuencias de una red abierta como Internet son los problemas de seguridad y confidencialidad. Este trabajo se propone definir lo que es el comercio electrónico, *sus características, describir sus áreas de alcance y finalmente reconocer los beneficios de la aplicación de la Criptografía y la Firma Digital como mecanismos alternativos de seguridad en transacciones comerciales y en la transmisión de información delicada. Se parte de un estudio exploratorio-descriptivo y se concluye que se está en una era en que la globalización impone retos, especialmente en el área de la información, por lo cual debe ponerse en marcha un plan de reconstrucción de los sistemas de seguridad tradicionales, que necesariamente requerirán una adecuada normativa que complete el modelo de seguridad y confidencialidad. Este trabajo abarca la primera fase del referido modelo, es decir, el elemento técnico.*

Palabras clave: Comercio Electrónico, criptografía, firma digital, globalización.

Fecha de recepción: 22 de junio de 2001

* Avance del Proyecto de Investigación «Modelo alternativo de una Infraestructura de Seguridad y Confidencialidad informática frente al auge de los delitos en y contra Internet», financiado por el CONDES bajo el Nº 0095-2001.

** Abogada; Magistra en Planificación y Gerencia de Ciencia y Tecnología; Doctora en Derecho. Profesora e Investigadora de la Sección de Informática Jurídica y Derecho Informático del Instituto de Filosofía del Derecho «Dr. J.M. Delgado Ocando» y de la Cátedra de Derecho Internacional Público, Facultad de Ciencias Jurídicas y Políticas, Universidad del Zulia. Investigadora adscrita a la Fundación Venezolana del Sistema de Promoción al Investigador (PPI) Nivel I. Coordinadora de la Unidad de Propiedad Intelectual del Consejo de Fomento de la Universidad del Zulia, período: 2000. Secretaria Coordinadora del Instituto de Filosofía del Derecho «J.M. Delgado Ocando», 200-2002.

Abstract

One of the consequences of an open network as Intemet, are the problems of security and confidentialíty. This paper intends to define what the electronic commerce is, its characteristics; to describe the áreas of scope of the electronic commerce; and fínally, to recognize the benefits of the application of Cryptography and Digital Signature as alternativa mechanisms of security in commercial transactions and in the transmission of important information. This paper starts from an exploratory-descriptive study and concludes that we are in an era where globálization imposes challenges especially in the ínformatíon field, which sets in motion a reconstruction plan of the tradicional security systems which necessarily will require an adequate normativeness that completes the security and confídentiality model. This paper embraces the first stage of the aforementioned model, that is to say, the teclinical element.
Key words: Electronic commerce, cryptography, digital Signature, Globalization

INTRODUCCIÓN

Una de las consecuencias de una red abierta como Internet son los problemas de seguridad y confidencialidad. Debido al incremento de las transacciones comerciales y de la transmisión de información delicada (información financiera o datos protegidos por secreto profesional), usuarios, autores y hombres de negocios desean ser capaces de garantizar: la autenticidad, integridad, no revocación y confidencialidad de los mensajes.

Se está entonces en uno de los temas claves del comercio electrónico: el de la confianza y seguridad. En principio, se da por sentado que el medio utilizado es inseguro, lo cual crea un ambiente de preocupación: la posibilidad de que puedan ser interceptados datos que circulan por la Red de Redes, Internet, que básicamente constituye el medio de transmisión de datos por excelencia. Igual preocupación existe en la seguridad que se obtiene en las redes más pequeñas, como podría ser un servicio de red para el intercambio electrónico de datos. En estos casos, se desarrollan sistemas de protección que son incorporados al *software* ofrecido para cada servicio. Puede decirse entonces que para que el comercio electrónico pueda continuar desarrollándose y se consolide definitivamente, es necesaria la implantación de algunos mecanismos de seguridad informática que en su conjunto conformen un modelo alternativo de seguridad y confidencialidad que

aminore la inseguridad propia del medio por el que transita la información.

Por tal sentido, este trabajo se propone definir lo que es el comercio electrónico, sus características, describir las áreas de alcance del comercio electrónico, y finalmente reconocer los beneficios de la aplicación de la Criptografía y la Firma Digital como mecanismos alternativos de seguridad en transacciones comerciales y en la transmisión de información delicada.

Se parte de un estudio exploratorio – descriptivo, y se concluye que se está en una era en que la globalización impone retos, especialmente en el área de la información, poniendo en marcha un plan de reconstrucción de los sistemas de seguridad tradicionales que no tiene respuesta sólo desde el ámbito técnico, sino que necesariamente requerirán una adecuada normativa que complete el modelo de seguridad y confidencialidad. En este caso, este trabajo abarca la primera fase del referido modelo, es decir, el elemento técnico.

1. COMERCIO ELECTRÓNICO

Definición

En la era de la información, particularmente con el desarrollo de la electrónica y las comunicaciones, comienza la comercialización de productos de información que no sólo permite movilizar cantidades de átomos sino que comercializan cantidades de bits. Esta forma de realizar el comercio a través de bits de información pareciera que llegó para quedarse. Negroponte (1995) sostiene que el cambio de átomos a bits es irrevocable e indetenible. La era de la información electrónica sirve de marco para la realización de transacciones de productos compuestos principalmente de bits. Con el tiempo, las ventas de bienes y servicios en forma electrónica serán la base fundamental de la economía. La Internet es la encargada de transformar, a muy bajo costo, la manera como se ha realizado hasta ahora el comercio, ya que brinda la posibilidad de que las organizaciones publiciten sus productos, promuevan sus ventajas y se comuniquen con sus clientes localizados en diversas partes del mundo, a un costo mucho más bajo que si ocurriera en la forma tradicional. Esa nueva forma de hacer el intercambio de bienes a través de las redes de datos electrónicas es conocida como *comercio electrónico*.

El comercio electrónico es entendido como la venta y compra directa o indirecta de cualquier tipo de información, productos y servicios por medio de redes de computadoras, así como también, el apoyo brindado a cualquier tipo de transacción de negocios sobre una infraestructura digital. Es tal la

dimensión del comercio electrónico que no puede ser visto como un simple canal usado para mercadear los productos; ni tampoco puede ser visto como uno nuevo que sustituye o se agrega a los ya existentes minoristas, mayoristas e intermediarios. La audiencia que logra reunir el comercio electrónico supera cualquier otra forma de comercio hasta ahora conocida.

Aunque la Internet pareciera ser la infraestructura adecuada para generar comercio electrónico, no es un requisito para su existencia, pues en lo futuro pareciera que todo comercio electrónico será fusionado con nuevas tecnologías de tipo inteligente, multimedias y TV interactiva (Andrade, 2000).

Otra definición de comercio electrónico es la que ofrece Jay Tenenbaum, quien fue durante 1998 Presidente y Director Ejecutivo de *CommerceNet: «Un modelo que permite a las empresas intercambiar, de forma electrónica, información y servicios esenciales para sus negocios y que no involucra necesariamente transacciones monetarias».*

De igual modo Osío (2000) define lo que se ha llamado en inglés ***e-bussines*** o en español ***comercio electrónico***, la actividad de adquirir o enajenar a través de medios electrónicos bienes corporales o incorporales. Ahora bien, la Internet no sólo abarca la posibilidad de adquirir bienes corporales o incorporales, sino también la obtención de servicios, asistencia, información, entretenimiento que genera relaciones que crean obligaciones y derechos para las partes que han decidido interactuar «on line».

Finalmente, podemos definir comercio electrónico como: La actividad comercial que implica toda operación desarrollada a través de ordenadores distribuidos en forma reticular sin límites y sin fronteras, permitiendo estos medios telemáticos: la distribución de productos y servicios, la realización de pagos electrónicos, compras de obras audiovisuales, música, fotografías, libros de *software*, etc., la consolidación de proyectos de Teletrabajo y el establecimiento y desarrollo de tiendas virtuales *(virtual malls)* entre: *bussines/ consumer/ goverment* y de éstos entre sí.

2. CARACTERÍSTICAS

a. *Gran perspectiva financiera*

De la totalidad de las compras que se hicieron en Internet desde Venezuela durante el 2000, 77% se hizo en tiendas virtuales en el exterior.

Un estudio de la *International Data Corporation* señala que en el 2000 se movieron en el país unos 31,4 millones de dólares en transacciones comerciales en línea; para 2001 la cifra llegará a 73,7 millones, de acuerdo con las proyecciones de la empresa, mientras que en 2003 se alcanzará la abultada cifra de 302 millones de dólares.

Para el año pasado, y según *International Data Corporation*, había en Venezuela 286.541 usuarios de Internet. La cifra crecerá a 389.000 personas a finales de este año, según los vaticinios de la empresa, y en 2003 el pico llegará a 598.000 personas. La mayor parte de los internautas se conectan desde sus hogares, según señala el estudio de la firma.

Pero no es lo mismo hablar de «internautas» que de «compradores en línea». En este último renglón se contaron en Venezuela 49.929 en 2000, mientras que para este año se espera que haya 73.622, de acuerdo con la tendencia que se ha venido marcando desde 1997, cuando el registro alcanzó apenas los 4.254. El gasto promedio por comprador, para 2000, fue de 965 dólares; para el año en curso se estima que subirá a 1.492 dólares, y en 2003 se ubicará en 2.612 dólares por persona (Cámel, 2000).

b. ***Transacción entre desconocidos***

Douglass North, Premio Nobel de Economía, sostiene que existen dos polos bien marcados dentro del espectro de las transacciones que tienen lugar en un sistema económico: por un lado, nos encontramos con transacciones en las que las partes se conocen mutuamente; por el otro, transacciones que se realizan entre desconocidos. En las primeras, los costos de la transacción generalmente son bajos; en las segundas, los costos son marcadamente más elevados. El comercio electrónico puede darse de diversas formas, mediante sistemas financieros, intercambio electrónico de datos (EDI), servicios *on line*. Una de las formas donde tiende a intensificarse es a través de Internet. Mientras la popularidad de Internet sigue creciendo a pasos agigantados, muchas empresas ya sienten la necesidad de sumergirse en esta nueva modalidad de comercio. Sin embargo, Internet continúa siendo un mundo sin reglas, un mercado en el que el comercio no puede florecer tranquilamente por carecer de normas que lo protejan. Para el funcionamiento del comercio electrónico, fundamentalmente Internet, hacen falta entonces tres requisitos. En primer lugar, se necesitan reglas relacionadas con la propiedad, a efectos de identificar los objetos del intercambio; en segundo lugar, es indispensable un sistema de pago seguro, y finalmente, algún mecanismo que permita castigar las transgresiones a dichas reglas. En este trabajo analizaremos los dos primeros, especialmente el de la seguridad, que merece un capítulo

aparte, en tanto el tercero quedará para futuros estudios.

c. *Limitaciones de la propiedad*

El comercio electrónico en general e Internet en especial fueron ideados para el intercambio de información. Sin embargo, en la actualidad se los utiliza en gran medida para transacciones que requieren el posterior transporte de la mercadería objeto de la transacción. En este caso, Internet es una simple alternativa comparable al teléfono, que no agrega nada nuevo al comercio. La tecnología base del comercio electrónico es solamente una parte de las transacciones. La compra electrónica será la comercializadora inevitable de la Internet, pero los que la defienden fervorosamente deberían tener en cuenta que los hábitos de los consumidores son difíciles de romper, ya que generalmente les gusta elegir y tocar la mercadería. Es razonable suponer que el comercio electrónico tendrá que superar algunas limitaciones, pues al realizar una compra de mercadería o servicios en general intervienen distintos factores: educación, interacción social, suerte para encontrar ofertas y posibilidad de probar lo que se quiere comprar. La compra electrónica no puede duplicar fácilmente estas experiencias. Esto nos sugiere campos tales como: comercio sobre dinero (finanzas), comercio sobre títulos y valores (bolsa) y, fundamentalmente, el comercio sobre información electrónica. Este último tendrá mucho futuro porque, en verdad, es el medio más apropiado para elegir, probar, sentir, enviar y embalar los productos electrónicos.

d. *La* **información** *es el principal bien del comercio electrónico*

La verdadera promesa de Internet radica en la venta de información. El *software*, por ejemplo, que es en esencia pura la información, es generalmente transferido a un medio físico (el disquete), empacado, transportado y vendido en negocios. Esta cadena encarece enormemente el costo de la información. Mucho más barato y eficiente es adquirir esa información vía Internet y recibirla directamente en el lugar, entorno y destino natural: la computadora del comprador (Devoto, Lynch,1997).

3. ÁREAS DE ALCANCE

Las Áreas o Mercados de *e-commerce* que dichos servicios pretende abarcar son:

a. ***Empresa-empresa o b2b (bussines to bussines):*** *e-commerce* entre empresas, que barca las relaciones comerciales de la empresa con sus proveedores

y distribuidores. Este mercado incluiría actividades de venta y compra entre empresas. Además incluirían sistemas de transacción e información relacionados con procesos comerciales entre proveedores, socios o canales, como puede ser pedidos, pagos, servicios básicos de adquisición, sistemas de ayuda a la distribución, gestión de la logística.

El objetivo primordial a este nivel es la automatización de la gestión de las facturas y la eliminación de sus costos asociados. Según muchos estudios publicados, la eliminación de estos costos permitiría duplicar o triplicar los beneficios de la mayoría de las grandes empresas, por ello supone un gran atractivo para cualquier gran organización. La principal dificultad que conlleva la aplicación de estas tecnologías es que tanto los proveedores como los clientes de la empresa deben utilizarla, y no siempre resulta posible debido a la gran inversión que ello supone.

EDI (Intercambio Electrónico de Datos) es un sistema ideado para automatizar la gestión de cobros, ventas y facturas entre empresas que han tenido una fuerte implantación en España en los últimos años. Con la llegada de Internet esta tecnología ha quedado obsoleta, ya que no funciona bajo el estándar TCP/IP, y por lo tanto debe utilizar su propio sistema de comunicaciones. A pesar de todo, los empresarios son reacios a modificar sus sistemas, ya que en la mayoría de los casos EDI ha supuesto una inversión que todavía no ha podido ser rentabilizada. Como respuesta a esta demanda han aparecido una serie de soluciones que encapsulan EDI en TCP/IP, lo que permite su utilización por Internet. Estas soluciones reciben el nombre genérico de EDIWeb. En España, IBM y Telefónica comercializan sistemas de este tipo.

b. ***Empresa-consumidor (bussines to consumer):*** *e-commerce* entre empresa y consumidores, donde estos últimos son considerados los compradores. Este es el tipo de relaciones a la que generalmente nos referimos cuando hablamos de Comercio Electrónico. La utilización de las nuevas tecnologías admite, en teoría, un contacto directo entre fabricantes y consumidores, lo que permitiría la eliminación de intermediarios en el proceso de compra. Esto repercutiría enormemente en el precio final del producto y se podrían ofrecer precios mucho más bajos.

La venta directa a través de Internet es una actividad que espera mover un volumen de negocio muy importante en los próximos años. Internet es sólo el primer paso hacia un nuevo concepto de economía en el que los consumidores podrán adquirir bienes desde sus casas sin necesidad de desplazarse a una tienda concreta. La televisión por cable permitirá

generalizar este tipo de negocio al llegar a un número mayor de consumidores potenciales. Uno de los puntos críticos que deben resolverse para garantizar las compras por medios electrónicos como Internet es la creación de un sistema de pago electrónico que permita realizar pagos seguros utilizando sistemas de comunicación inseguros.

En las ventas electrónicas podemos distinguir dos grandes tipos en función del tipo de producto que se comercialice: información digital y productos físicos. En el primer caso tendríamos los productos susceptibles de ser digitalizados y enviados por una red de comunicación de datos, como la música, videos, *software*, documentación, etc. La actividad se realizaría en su totalidad por una red como Internet sin necesidad de utilizar otro tipo de medio físico. Por el contrario, si el producto requiere de un traslado físico al domicilio del cliente, es obvio que la compra no se podrá realizar enteramente por Internet, por lo cual se tiene que recurrir a empresas de transporte y logística para realizar el envío. En este caso, la utilidad de la transacción electrónica se reduce a simplificar el proceso de compra, ya que existen otros medios de pago como el contra reembolso o el giro postal.

c. ***Intraempresarial***: posibles relaciones electrónicas en la actividad diaria de una empresa. A la hora de mejorar nuestra producción y gestión de la empresa es imprescindible una comunicación interdepartamental eficaz y fluida. Para ello es necesario crear una infraestructura de clave pública dentro de nuestra Intranet, con el propósito de que sepamos con rapidez y seguridad todo lo que ocurre en la empresa.

d. ***Empresa/consumidor-administración (bussines/consumer to goverment)***: el *e- commerce* se realiza con la administración, de modo que cualquier comunicación o trámite por parte del consumidor o la empresa se realiza con técnicas de *e- commerce* (Ramos, 2000).

4. ALGUNAS CONSIDERACIONES PREVIAS PARA UNA *SEGURIDAD TECNOLÓGICA GLOBAL*

El desarrollo de las redes de datos, y la conexión de éstas entre sí, ha creado una gran red a nivel mundial conocida como Internet, que nos permite intercambiar información con cualquier persona conectada a dicha red. Entre los usos principales de Internet pueden mencionarse: el correo electrónico, el acceso a información en bases de datos, la transferencia de archivos entre computadoras y la posibilidad de realizar el comercio electrónico. Por tal motivo, Internet ofrece nuevas posibilidades, mayor

rapidez y mayor economía para comerciar electrónicamente, de un lado, a través del almacenamiento y reenvío de mensajes (correo electrónico) y, por otro, a través de transacciones electrónicas interactivas (*on line*). Sin embargo, aun cuando lo anterior configura su mayor virtud, también es su principal riesgo, pues por ser una red abierta cualquier persona puede acceder a ella. Circunstancia que justifica la necesidad de establecer mecanismos de seguridad tanto técnicos como jurídicos (Núñez, 2000).

Es indudable que en este marco situacional un factor imprescindible es el de la seguridad, la lucha contra el fraude informático que involucra a cada uno de los eslabones activos de la comunicación global, a saber:

- ***Los bancos de datos informacionales*** y la enorme data manejada por las empresas insertadas en este mundo informático requieren de políticas estructurales en lo técnico y normas jurídicas para establecer límites a los abusos.

- ***La propiedad intelectual y del software*** y el permanente crecimiento de actividades tendientes a la explotación excesiva de los recursos derivados de la *world wide web* que estimulan actividades ilegales basada en la piratería y la copia de *software*.

- ***Las relaciones contractuales informatizadas*** han transformado los antiguos parámetros y requieren de una infraestructura normativa en su propio ámbito, fundamentalmente para la puesta en funcionamiento real. La seguridad en las transacciones depende hoy de la estructura legal que le están brindando los países del mundo globalizado, que por separado han creado la normativa para sentar su validez legal.

La seguridad viene apoyando la iniciativa de la firma digital como alternativa de solución a la necesidad de dar validez a los contratos y documentos electrónicos, pero aún no se generan los soportes reales técnicos a nivel institucional para su implementación.

- ***Nuevas tecnologías estratégicas*** creadas a efectos de solucionar el riesgo informático, siendo lo más reciente los denominados *certificados digitales*. Se trata de credenciales electrónicos que contienen la identificación de la persona o compañía, su localización, su clave pública, entre otros. Son emitidos por una autoridad certificadora confiable y firmados digitalmente. Otra técnica es la *criptografía*, que estudia la ocultación de la información –de ella se hablará en detalle

más adelante– y se basa en el uso de claves secretas. La tendencia es que la utilización de certificaciones digitales sobre los activos digitales y demás elementos de la cadena comercial intenten lograr un mayor equilibrio entre los responsables integrantes del *e-business* en forma pareja, y activar el complejo mecanismo de protección para cada sector.

Y es que el estudio de una «nueva tecnología» y la verdadera o mejor comprensión de la misma nos llevará al estudio del comportamiento jurídico necesario para una respuesta acorde y equilibrada (Dorrego, 2000).

Y es que son indetenibles los riesgos informáticos derivados del intercambio de información a través de redes, entre los más comunes: que el autor y fuente del mensaje sean suplantados; que el mensaje sea alterado, de forma accidental o de forma maliciosa, durante la transmisión; que el emisor del mensaje niegue haberlo transmitido o el destinatario haberlo recibido; y que el contenido del mensaje sea leído por una persona no autorizada (Martínez, 1998).

Por lo tanto, desde el punto de vista jurídico es necesario asegurar: que el mensaje proviene de la persona que se dice que lo envía; que no ha sido alterado en el camino; que el emisor no podrá negar su envío ni el destinatario su recepción y, en su caso, garantizar su confidencialidad.

Y para garantizar la satisfacción de estas exigencias jurídicas lo que se impone es la aplicación de determinadas soluciones técnicas como la criptografía y la firma digital, capaces, conjuntamente con las autoridades de certificación, de garantizar: la autenticidad, la integridad, el no rechazo y la confidencialidad de los mensajes (Delpiazzo, 2000).

5. CRIPTOGRAFÍA Y FIRMA DIGITAL: *ALGUNOS BENEFICIOS*

Con base en los requerimientos de autenticación, integridad, no rechazo y confidencialidad, se desarrollaron dos instrumentos técnicos. El primero es la criptografía, que es la disciplina que estudia el modo de transformar un mensaje (texto original) en un texto en cifra(criptograma) mediante una operación de cifrado que hace imposible a un tercero tener conocimiento del contenido del mensaje. De acuerdo con el *Diccionario de la Real Academia*, la *criptografía* se define como: «el arte de escribir con clave secreta o de un modo enigmático». Etimológicamente, el término quiere decir «escritura secreta», proviene del griego *kryptos*, que significa «esconder», y *gráphein*, «escritura».

El uso de la criptografía data desde la antigüedad y es caso tan antiguo como la escritura, pero ha renacido en nuestros días con un inusitado vigor debido a su aplicación por medio sistemas informáticos y el desarrollo de nuevos métodos y algoritmos de cifrado de la información, lo cual ha asegurado algunos beneficios fundamentales, tales como:

- *Seguridad:* certeza de que el texto del mensaje sólo puede ser leído por el destinatario.

- *Integridad:* certeza del mensaje, asegura que no ha existido ninguna manipulación posterior de los datos.

- *Autenticidad:* certeza del remitente, acredita quién es su autor.

- *No rechazo:* no se puede negar la autoría de un mensaje enviado (Pasacale, 2000).

Hoy existen métodos criptográficos modernos, desarrollados a partir de la II Guerra Mundial, cuando empiezan a aparecer los primeros computadores, y son conocidos como: Los Sistemas Criptográficos Asimétricos[1] y los Sistemas Criptográficos Simétricos[2].

De los dos sistemas mencionados, el Sistema Criptográfico Asimétrico o de Clave Pública ha resultado más beneficioso para garantizar el cumplimiento de los requisitos legales y superar la desventaja del Sistema de Criptografía Simétrico, según el cual, al tenerse acceso a la clave secreta se puede descifrar el mensaje.

¿Cómo funciona entonces la Criptografía Asimétrica para enviar un mensaje cifrado?

[1] Sistema de cifrado basado en claves privadas; tanto el que envía el mensaje como el que lo recibe conocen y utilizan la misma clave secreta tanto para encriptar el mensaje como para desencriptarlo.

[2] Son los sistemas creados en 1976 en la Universidad de Standford, Estados Unidos, se basan en la utilización de dos claves diferentes por cada usuario: la clave pública y la clave privada. Ambas claves, aun cuando son completamente diferentes, trabajan a dúo para encriptar y desencriptar mensajes. El mensaje se encripta con clave privada y se desencripta con clave pública y viceversa.

- *Paso 1*

El emisor da a conocer a todos los usuarios (receptores) con quienes comparte información su clave pública. Lo mismo hace el receptor.

- *Paso 2*

Cuando el emisor quiere enviar un mensaje al receptor, y desea que solamente sea visto por este último, deberá cifrar el mensaje, haciendo uso de la clave pública del receptor, mediante un programa que obtiene en forma gratuita en Internet.

- *Paso 3*

El mensaje cifrado es enviado por medios no seguros: E-mail, correo postal, fax, etc.

- *Paso 4*

El receptor recibe el mensaje y la única forma de descifrarlo es haciendo uso de su clave privada.

Cualquier persona que intercepte el mensaje leerá una gran cantidad de garabatos y la única forma de descifrarlo será con la clave privada del receptor, ni siquiera con su clave pública.

Ahora, ¿cómo funciona un sistema criptográfico asimétrico para asegurar la autenticidad de un documento?

Supongan que el emisor del mensaje sospecha que hay personas que se hacen pasar por él y están enviando documentos con su nombre.

- *Paso 1*

El emisor envía el documento al receptor y lo cifra con su clave privada, que solamente él conoce.

- *Paso 2*

Cuando el receptor recibe el documento, solamente lo puede descifrar con la clave pública del emisor.

Si el documento es descifrado, entonces se pude decir que proviene de quien dice provenir.

Y, finalmente, ¿qué ocurre si el mensaje que quería enviarse era confidencial?

En el caso anterior, cualquier persona con la clave pública del emisor podía comprobar que el documento es auténtico, pero el documento queda expuesto a cualquiera que tenga la clave pública del emisor.

Entonces, para que el mensaje además de auténtico sea confidencial se deberá:

- *Paso 1*

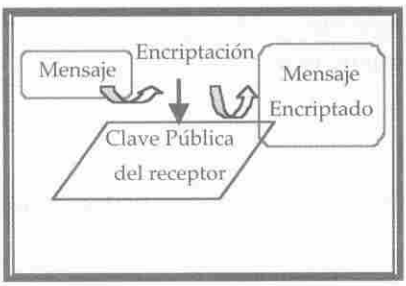
El emisor cifra su mensaje con su clave privada, lo cual permite que sólo sea descifrado por su clave pública.

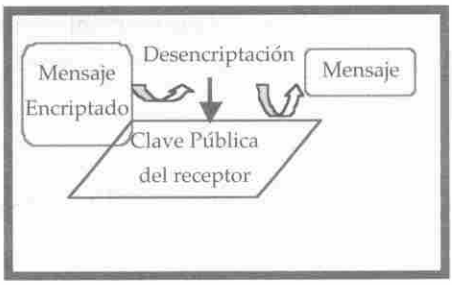
- *Paso 2*

Luego el emisor vuelve a cifrar el mensaje ya cifrado con la clave pública del receptor.

- *Paso 3*

El receptor descifra el mensaje solamente con su clave privada y lo autentica con la clave pública del emisor.





Fuente: RSA Security Inc.

No obstante los beneficios de la criptografía asimétrica, se ha determinado que los algoritmos[3] de encriptación asimétrica son cien veces más lentos que los algoritmos de encriptación simétrica. Por ello, los algoritmos actuales encriptan el mensaje mediante claves simétricas y envían la propia clave simétrica dentro del mensaje pero encriptada según algoritmos de claves asimétricas.

Así, de la criptografía llegamos a la Firma Digital.

¿Qué es una *Firma Digital?*

La firma digital está basada en la utilización de la criptografía de clave pública, es decir, en algoritmos matemáticos que operan a través del juego de un par de claves, privada y pública, las cuales se encuentran íntimamente vinculadas.

Toda persona que quiera «firmar» digitalmente información para su posterior transmisión debe generar su propio par de claves. La bondad de la criptografía de clave pública radica en que no se necesita compartir la clave: la clave privada queda en poder del usuario y es la utilizada para «firmar». Sólo la clave pública se publicita y es utilizada para verificar la firma.

La firma digital no se asemeja en nada a la firma tradicional. Por ello es conveniente determinar ¿cómo se crea o realiza la Firma Digital?

El proceso de creación de par de claves lo realiza un *software* especial: en general, la clave privada queda almacenada en el *hardware* del usuario y se activa por medio de una contraseña, aunque también puede ser almacenada en otros dispositivos como una tarjeta inteligente.

Las *claves* no son otra cosa que una combinación de letras y números, es decir, un conjunto de *bits* que a su vez constituyen un conjunto de ceros y unos.

La creación de una Firma Digital implica combinar los caracteres que conforman la clave privada del usuario con los caracteres del documento o información al que se le quiere adosar la «firma». Este nuevo conjunto de caracteres obtenidos a partir de la mezcla de los caracteres del documento/

[3] *Algoritmos* es el conjunto de operaciones que permite hacer incomprensible el mensaje descomponiéndolo en una secuencia de caracteres no inteligibles inmediatamente.

información con los de la clave privada, es lo que constituye la firma digital. En dicha mezcla quedan comprendidos todos los caracteres que conforman el documento, incluso los espacios en blanco, de forma tal que cada combinación (clave privada más documento, es decir, firma) es única para cada documento. Como se advierte, también es muy importante la longitud de la clave.

Entre los algoritmos más utilizados para esta creación se encuentra el RSA[4].

Una vez obtenida la «firma», el suscriptor/emisor la transmite conjuntamente con el documento. Asimismo, transmite su clave pública para ser utilizada en el proceso de verificación.

Ahora, ¿cómo se comprueba la *validez* de la Firma Digital?

El destinatario recibe el documento con la firma digital y la clave pública del suscriptor. Procede entonces a iniciar el proceso de verificación de la firma digital adosada al documento recibido. Aplica la clave pública del suscriptor a la firma digital. Como resultado de este proceso se obtiene una serie de caracteres que son comparados con los que conforman el documento transmitido. Si los caracteres coinciden, la «firma» es válida, ya que garantiza que fue aplicada por el titular de la clave privada, que se corresponde con la clave pública utilizada para la verificación y que el documento no ha sido alterado.

Cabe señalar que todo este proceso se realiza automáticamente y en pocos segundos.

CONCLUSIÓN

El advenimiento del comercio electrónico es hoy una realidad insoslayable. Al igual que en otras muchas áreas, la combinación de lo que denominamos Nuevas Tecnologías está transformando el comercio de tal manera que resulta indispensable comenzar a imaginar los distintos campos en que estos cambios influyen e influirán en un futuro muy próximo.

[4] RSA es uno de los sistemas criptográficos más utilizados; fue desarrollado por Rivest, Shamir y Adleman y publicado en septiembre de 1978. La patente de *RSA Laboratories* sobre el algoritmo recién ha venido haciendo público el uso de los algoritmos y modificaciones, lo cual permitirá a los especialistas en criptografía utilizar el código libremente para reforzarlo aun más.

Por lo tanto, se debe dotar a los ordenamientos jurídicos, ya sea nacionales y regionales, de herramientas acordes con estas novedades tecnológicas y darles empleo adecuado.

Por el momento se han desarrollado más los sistemas tecnológicos de seguridad, hasta el punto que la criptografía, con el desarrollo de Internet, ha emergido de la oscuridad y hoy puede emplearse inclusive para crear firmas digitales, para autenticar mensajes electrónicos y para verificar su integridad, lo cual en el contexto de los negocios electrónicos es vital.

De allí que para que este tipo de comercio exista no es suficiente la presencia de dos personas que deseen contratar por esta vía: hacen falta una infraestructura de seguridad y confidencialidad y una línea coherente; uniforme y armónica que conjugue un esfuerzo normativo supranacional conjuntamente con los gobiernos y el sector industrial

REFERENCIAS

ANDRADE, J. «Formación de Precios de los Productos de Información en Redes Digitales». En: *Revista Venezolana de Gerencia*, Año 5, N° 11, 2000, p. 209-228.

TENENBAUM, J. «La Empresa en el Mundo de las Tecnologías de la Información», citado por Fernando Ramos, «La Seguridad Jurídica en el Comercio Electrónico: la Firma Electrónica». *Ponencia presentada en el Primer Congreso Sobre Aspectos Legales en Internet*. Universidad de Buenos Aires (Argentina), 1998. Formato Electrónico: www.ecomder.com.ar.

OSÍO, M. «Comercio Electrónico: Los Mitos de una Ley sobre la Materia». Trabajo presentado en *Seminario Profesional y Empresarial: Aspectos Jurídicos de Internet*. Caracas, 2 de noviembre del 2000.

CÁMEL, E. «En la Red está el Negocio». En: *El Nacional*, cuerpo E/1, 18 de febrero de 2001.

DEVOTO, M. y LYNCH, H . (1997). «Banca, Comercio, Moneda Electrónica y la Firma Digital». En: *Revista Jurídica la Ley* N° 21, abril de 1997. Buenos Aires, Argentina.

RAMOS, F. «La Seguridad Jurídica en el Comercio Electrónico: la Firma Electrónica». Ponencia presentada en el *Primer Congreso sobre Aspectos Legales en Internet*. Universidad de Buenos Aires (Argentina), 2000. Formato electrónico: www.ecomder.com.ar.

NÚÑEZ, J. «Regulación Jurídico Informática del Comercio Electrónico e Internet en el Perú». En: *Memorias VIII Congreso Iberoamericano de Derecho e Informática*. México, 21 al 25 de noviembre del 2000. Formato electrónico: comunidad.derecho.org/congreso.

DORREGO, C. «Hacia una Protección no diversificada en dos Mundos Convergentes». En: *Memorias VIII Congreso Iberoamericano de Derecho e Informática*.

México, 21 al 25 de noviembre del 2000. Formato electrónico: comunidad.derecho.org/congreso.

MARTÍNEZ, A. *Comercio Electrónico, Firma Digital y Autoridades de Certificación.* Madrid, Civitas, 2000.

DELPIAZZO, C. «Relevancia Jurídica de la Encriptación y la Firma Electrónica en el Comercio Actual». En: *Memorias VIII Congreso Iberoamericano de Derecho e Informática.* México, 21 al 25 de noviembre del 2000. Formato electrónico: comunidad.derecho.org/congreso.

PASCALE, M. «Firma Digital». En: *Memorias VIII Congreso Iberoamericano de Derecho e Informática.* México, 21 al 25 de noviembre del 2000. Formato electrónico: comunidad.derecho.org/congreso.

FARESE, G. «Criptografía, Protocolos de Seguridad, Firmas y Certificados Digitales». En: *Aspectos Jurídicos de Internet.* Caracas, 2 de noviembre del 2000.

PALAZZI, P. *Derecho y Nuevas Tecnologías.* Buenos Aires, Ad- Hoc, srl, 2000.