V. TERCER PROBLEMA: PROTOCOLOS O SISTEMAS DE SEGURIDAD Y CRIPTOGRAFÍA

A. CONTEXTO GENERAL

El término criptografía proviene del griego *kriptos*, que significa ocultar, y de *gráphein* que significa escritura. En este sentido consiste en "esconder" un escrito de ma-nera que sólo pueda ser visto o percibido por el destinatario que se quiere reciba el mensaje (Juan de Jesús Angel. "Cripto-grafía para principiantes, en [www. lacasadejara.org]).

Podemos afirmar que criptografía o encriptamiento es la disciplina que estudia los sistemas de cifrado destinados a ocultar el contenido de un mensaje de datos enviado y recibido entre las partes inmersas en la generación, comunicación y almacenamiento de información entre las partes.

La criptografía reúne una serie de técnicas (teoría de la información, teoría de los números, desarrollo de algoritmos) que buscan proteger la información.

La criptografía, de manera contraria a lo que se puede pensar, no es algo nuevo o de reciente aparición, pues, como lo mencionaremos a continuación, el hombre a lo largo de su existencia ha deseado que la información por él generada no sea conocida por todos, sino sólo por aquellos individuos a quien va dirigida de manera específica.

En este contexto empecemos por aludir a métodos como el de la Csitala Espartana, desarrollado alrededor del año 400 a. C. por este pueblo guerrero fundado por Licurgo. Dicho método, consiste en dos varas idénticas: en una de ellas el remitente escribe sobre un pergamino enrollado a lo largo de la vara, mientras que el destinatario enrolla el pergamino en el mismo sentido en la otra vara y puede leer el mensaje inicialmente escrito.

También encontramos el sistema multicolumnar, mediante el cual se escribe de manera vertical siguiendo una secuencia de números, por medio de una clave que determina el número de columnas y a las que se puede acceder en un orden preestablecido de acuerdo a la permutación.

Otro sistema bastante interesante es el conocido como el algoritmo de Julio César; creado y desarrollado por el famoso emperador y general de la antigua Roma, se basa en un mecanismo simple de sustitución, donde cada letra se desplaza o corre a la tercera letra siguiente de la inicial. Por ejemplo, la letra a equivale a la letra d (la palabra año se represen-taría como dqr).

Durante la Segunda Guerra Mundial (1939-1945), y debido principalmente a las redes de espionaje y contraespionaje,

surgen una serie de sistemas de encriptamiento, cifrado y descifrado que se conocen como los sistemas clásicos.

Son ellos, por ejemplo, la máquina de encriptamiento desarrollada por la Alemania nazi conocida como el "Proyecto Enigma", que sirvió en los principios de la confrontación armada para ocultar y evitar que los aliados pudieran conocer las técnicas y estrategias que se planeaban y se comunicaban por escrito a través del telégrafo (clave Morse).

Estos sistemas de cifrado le dieron una ventaja enorme al Tercer Reich frente a sus enemigos, pero los aliados encontraron finalmente la manera de descifrar el sistema a través del sistema conocido como "Proyecto Ultra", lo cual trajo como consecuencia que la balanza se inclinara en su favor, pues al interceptar los mensajes conocían de antemano los movimientos de los alemanes.

En un comienzo, entonces, la criptografía fue de gran utilidad para fines militares; sin embargo, tal y como la conocemos hoy tuvo su aparición a mediados de los años 70, con la invención del sistema conocido como DES (Data Encrytion Standard) en 1977, y posteriormente en 1978 con el sistema RSA (Rivest, Shamir, Adleman). También debemos mencionar los métodos conocidos como Gamal y Rabin (Angel. "Criptografía para principiantes, cit.).

Los sistemas de criptografía pueden clasificarse en razón de su correspondencia, y con base en ello se conocen los siguientes:

> *Criptografía simétrica*: las técnicas de encriptamiento son simétricas cuando "se requiere la misma clave para desencriptar el documento que para encriptarlo" (Andrés Hall. *El rol del encriptado de datos en la despapelización*). Es decir que la simetría hace referencia a que las partes tienen la misma llave para realizar las operaciones de cifrar y descifrar la información contenida en un mensaje de datos. Esta técnica es conocida como criptografía de clave privada o de llave privada, pues para que esta operación tenga éxito se requiere de la cautela con que las partes guarden la llave privada, pues de hacerse pública cualquier persona podría tener acceso a la información.
>
> *Criptografía asimétrica*: se refiere a "aquella que utiliza dos claves diferentes para cada usuario: una para cifrar, que se llama clave pública, y otra para descifrar, que se llama clave privada" (Angel. "Criptografía para principiantes", cit.). La diferencia con la simétrica radica en la existencia de dos claves diferentes, lo que significa que un documento encriptado con una clave privada puede únicamente ser descifrado con la respectiva clave pública, e igualmente, un documento cifrado con la clave pública solamente puede ser desencriptado con la correspondiente clave privada. En términos más simples podríamos decir que se tiene en la mano derecha una "llave" para encriptar o cifrar el documento, y en la mano izquierda otra que cumple la tarea de desencriptarlo o descifrarlo. Este método es conocido como criptografía de clave pública.

En términos generales, los problemas llamados a solucionar con la criptografía son básicamente cuatro:

> – La confidencialidad de la información transmitida, es decir, que los datos enviados sólo puedan ser leídos por los destinatarios autorizados.

– La integridad de la información transmitida, estos es, que no pueda ser alterada en el transcurso de ser enviada y ser recibida.
– La autenticidad de los titulares y de los establecimientos de comercio, en el sentido que se pueda confirmar que el mensaje recibido haya sido enviado por quien dice haberlo hecho o que el mensaje ha sido recibido por quien se esperaba lo recibiera.
– El no repudio o no rechazo de las operaciones realizadas, esto es, no se puede negar la autoría de un mensaje recibido o enviado.

En este sentido, es preciso entrar a definir el concepto de protocolo de seguridad: como "la parte visible de una aplicación, es el conjunto de programas y actividades programadas que cumplen con un objetivo específico y que usan esquemas de seguridad criptográfica" ("Protocolos de seguridad", en [http://members.es.tripod.de/cursoredes/cripto/proto.htm]). Dentro de estos encontramos principalmente el protocolo SSL (Secure Socket Layer) y el protocolo SET (Secure Electronic Transactions).

Veamos a continuación en qué consiste cada uno de ellos:

SSL (Secure Socket Layer)

Es un protocolo de seguridad desarrollado en 1994 por Netscape Inc., y tiene como principal particularidad el hecho de permitir que se establezcan sesiones de comunicación encriptada entre emisor y receptor. Como ejemplo encontramos las salas privadas en los *chats*. El sistema opera a través de la verificación de la información generada por el receptor.

Su fin primordial es el de permitir la confidencialidad y la autenticación a través de la red. Es un protocolo ampliamente utilizado por los navegadores con el fin de brindar confidencialidad, autenticación del servidor e integridad de la información que circula en la red. Cuando la página *web* se identifica con https (HTTPS Hiper Text Transfer Protocol Secure) se entiende que automáticamente se está en presencia de este protocolo (Dianelos Georgoudis. "Encriptación fuerte en Internet: realidad y mito", en [www.aui.es]).

Cuando se quiere establecer una comunicación segura a través del protocolo SSL se necesitan seguir una serie de pasos. "Primero se necesita hacer una solicitud de seguridad. Luego, y después de haber obtenido esto, se deben establecer los parámetros que se utilizarán para SSL. Esta parte se conoce como SSL handshake. Una vez se haya establecido una comunicación segura, se deben hacer las verificaciones periódicas para garantizar que la comunicación sigue siendo segura a medida que se transmiten los datos" (Fernando Ramos. "Aspectos a tener en cuenta para implantar una solución de comercio electrónico segura y efectiva", en [www.legalia.com]).

El proceso mencionado en detalle puede ser descrito de la siguiente manera.

La solicitud la hace el cliente a un servidor que soporte SSL. Cuando SSL acepta la solicitud del cliente se empieza a negociar la conexión SSL, que como ya lo mencionamos se denomina SSL *handshake*. Durante esta etapa se presentan diferentes situaciones: *client hello* (en donde el cliente informa al servidor qué algoritmos de criptografía puede utilizar y solicita una verificación de la identidad del servidor); *server hello* (cuando el servidor responde

identificándose digitalmente a través de su llave pública); aprobación del cliente (cuando éste verifica la validez del certificado digital que el servidor le envía), y por último la verificación (en donde el cliente y el servidor se envían las anteriores transacciones encriptadas con la llave secreta). Si las dos partes confirman la validez de las transacciones, el proceso del *handshake* se consolida.

Por lo general cuando el cliente abandona una sesión SSL se presenta un mensaje que manifiesta que la comunicación ya no es segura.

SET (Secure Electronic Transaction)

Es un protocolo de seguridad desarrollado por Visa y Mastercard con el apoyo y la plataforma tecnológica de la International Business Machine (IBM), Microsoft y Netscape. En él participan un grupo de actores para darle seguridad a las transacciones (banco emisor de la tarjeta de crédito, tarjetahabiente, Comerciante que dispone del sitio *web*, cámara de compensación o *Gateway* que procesa el pago y autoridad certificadora); sin embargo exige una serie de pasos que requieren el registro de los usuarios para efectos de adquirir un código de seguridad.

El SET es un protocolo de seguridad diseñado especialmente con el propósito de asegurar las transacciones que se realizan en cualquier tipo de red en línea por medio de tarjetas de crédito.

Dentro de este protocolo intervienen diferentes partes en la transacción:

> Titular o *cardholder*: es la persona a la cual se le ha emitido una tarjeta; en este sentido sería el comprador de determinado producto.
>
> Emisor: es la entidad financiera emisora de la tarjeta de crédito o débito.
>
> Establecimiento o *merchant*: es quien está ofreciendo en la red bienes o servicios a cambio de un pago.
>
> Adquirente: es una entidad financiera que establece una cuenta bancaria con el establecimiento y procesa las autorizaciones de pago por tarjeta de crédito y los propios pagos realizados por este establecimiento.
>
> Pasarela de pagos: es el mecanismo por medio del cual se procesan y autorizan las transacciones del *merchant*. (Vicente Estévez. "Comunicación segura a través de redes abiertas de información II", en [www.marketingycomercio.com]).

La virtud del protocolo SET consiste en que se produce un tratamiento independiente de la información, en el sentido que, en primer lugar, el número de la tarjeta de crédito nunca llega a manos del vendedor, por lo que no hay un conocimiento por parte de éste acerca de la información financiera del comprador, y en segundo lugar, la entidad financiera tampoco tiene acceso al contenido de la compra, solo de la cantidad o importe que le toca pagar.

El procedimiento de SET es el siguiente:

"El cliente inicializa la compra: consiste en que el cliente usa el *browser* para seleccionar los productos a comprar y llena la forma de orden correspondiente. SET comienza cuando el cliente hace clic en 'pagar' y se envía un mensaje de iniciar SET.

"El cliente, usando SET, envía la orden y la información de pago al comerciante: el *software* SET del cliente crea dos men-

sajes, uno conteniendo la información de la orden de compra, el total de la compra y el número de orden. El segundo mensaje contiene la información de pago, es decir, el número de la tarjeta de crédito del cliente y la información del banco emisor de la tarjeta. El primer mensaje es cifrado usando un sistema simétrico y es empaquetado en un sobre digital que se cifra usando la clave pública del comerciante. El segundo mensaje también es cifrado pero usando la clave pública del banco (esto previene que el comerciante tenga acceso a los números de tarjetas de los clientes). Finalmente el cliente firma ambos mensajes.

"El comerciante pasa la información de pago al banco: el *software* SET del comerciante genera un requerimiento de autorización, éste es comprimido (con un algoritmo *hash*) y firmado por el comerciante para probar su identidad al banco del comerciante, además de ser cifrado con un sistema simétrico y guardado en un sobre digital que es cifrado con la clave pública del banco.

"El banco verifica la validez del requerimiento: el banco descifra el sobre digital y verifica la identidad del comerciante; en el caso de aceptarla descifra la información de pago del cliente y verifica su identidad. En tal caso genera un requerimiento de autorización, lo firma y envía al banco que generó la tarjeta del cliente.

"El emisor de la tarjeta autoriza la transacción: el banco del cliente (emisor de la tarjeta) confirma la identidad del cliente, descifra la información recibida y verifica la cuenta del cliente en caso de que no haya problemas, aprueba el requerimiento de autorización, lo firma y lo regresa al banco del comerciante.

"El banco del comerciante autoriza la transacción: una vez recibida la autorización del banco emisor, el banco del comerciante autoriza la transacción, la firma y la envía al servidor del comerciante.

"El servidor del comerciante complementa la transacción: el servidor del comerciante da a conocer que la transacción de la tarjeta fue aprobada y muestra al cliente la conformidad de pago, y procesa la orden que pide el cliente terminando la compra cuando le son enviados los bienes que compró el cliente.

"El comerciante captura la transacción: en la fase final de SET el comerciante envía un mensaje de 'captura' a su banco, lo que confirma la compra y genera el cargo a la cuenta del cliente, así como acreditar, el monto a la cuenta del comerciante.

"El generador de la tarjeta envía el aviso de crédito al cliente: el cargo de SET aparece en el estado de cuenta del cliente que se le envía mensualmente" (Angel. "Criptografía para principiantes", cit.).

Electronic Data Interchange (EDI) - (X.400, X.500, X.509)

Está constituido por la interacción de una serie de herramientas que permite que socios comerciales, tales como las partes inmersas en un contrato de suministro, intercambien órdenes de compra, cotizaciones, ofertas, notificaciones de embarque y transferencias de fondos. Este fue el primer instrumento utilizado por los comerciantes para realizar *e-commerce* utilizando las redes de valor agregado y telemático.

Existen dos estándares de Electronic Data Interchange (EDI), un primero denominado EDI ASC X12 y un segundo conocido como EDIFACT.

El primero (EDI ASC X12) es utilizado en Norteamérica, principalmente en Estados Unidos, donde el Instituto de Codificación de Estándares Americano se encarga de implementarlo.

El segundo (EDIFACT) es acogido por el Sistema de la Organización de Naciones Unidas (ONU) y por la Unión Europea (UE). En Colombia este es el sistema más difundido a través del Instituto Colombiano de Codificación y Automatización (IAC), el cual opera bajo los parámetros establecidos por el INCONTEC, bajo la supervigilancia de la Superintendencia de Industria y Comercio, Delegatura para la Protección al Consumidor.

Para el caso colombiano, de conformidad con lo establecido en la Ley 527 de 1999, el Decreto Reglamentario 1747 de 2000 y la Resolución 26930 de 2000 se adoptaron los estándares de certificación reconocidos internacionalmente, desarrollados por organizaciones de reconocida trayectoria como el PKIX (*working group* del Internet Engineering Task Force-IETF); el National Institute of Standars and Technologies (NIST); el Common Criteria Proyect Sponsoring Organization (CCPSO) y el International Organization for Standardization (ISO).

En el artículo 18 de la Resolución 26930 del 26 de octubre de 2000 expedida por la Superintendencia de Industria y Comercio se establecieron como estándares aplicables los algoritmos definidos en el Draft Representation of Public Key and Digital Signature en Internet (X.509 versión 2 y 3) Public Key Infraestructure Certificates, desarrollado por el PKIX y el IETF, incluyendo el denominado MD2.

B. ANÁLISIS SOCIOECONÓMICO: SEGURIDAD EN LOS MEDIOS TELEMÁTICOS

Al hablar de seguridades, debemos afirmar que la seguridad es uno de los puntos de mayor trascendencia que debe tener en cuenta cualquier actividad que base sus negocios en sistemas computarizados, considerando la tendencia actual de avanzar cada vez más hacia el uso de redes de computadores a todos los niveles de producción y comercialización de bienes y servicios.

En este entendido, es menester precisar qué se entiende por "seguridad": tomando la definición de Luis Ventura Ruiz en su artículo "Cortafuegos", podemos tomar la "seguridad" en redes telemáticas la protección frente a ataques e intrusiones en recursos corporativos por parte de sujetos a los que no se permite el acceso a dichos recursos (en *Boletín de Criptomición,* n.º 35). Es decir, podemos hablar de lugar seguro, informáticamente hablando, cuando el sitio al cual estoy protegiendo mediante los diferentes sistemas de protección existentes brinda un alto grado de certeza de que la información que pretendo proteger no puede ser accesada por un tercero sin autorización para ello.

No obstante lo anterior, afirma el mismo autor que "en los ámbitos de seguridad en redes el ordenador realmente seguro es aquel que está físicamente desconectado de todas las redes internas o externas (sin ninguna tarjeta de red), tampoco tendrá disquetera (y en su caso unidad de almacenamiento externo, como grabadores y lectores de cintas, discos extraíbles, etc.) o acceso a impresoras y se encontrará en una habitación acorazada

con un guardia jurado insobornable, y si este operador está apagado, mejor que mejor". Esta descripción, un poco exagerada por cierto, refleja la realidad del mundo de los sistemas en el cual, sin la menor duda, es claro que no existe un sistema computarizado cien por ciento seguro, toda vez que existe toda clase de formas diferentes con las que se puede romper la seguridad de estos sistemas.

En términos sencillos podríamos afirmar que un sistema telemático no es seguro cuando es vulnerable. En este sentido, podríamos definir vulnerabilidad como "cualquier deficiencia de un sistema operativo o aplicación, la cual puede ser utilizada por usuarios no autorizados para fines no genuinos (usualmente para ocasionar daño)" ("Un estudio sobre la seguridad informática en México", SekureIT, Consultores en Seguridad Informática, wn [http://www.sekureit.com/]).

En virtud de lo anteriormente expuesto, es aconsejable diseñar una estrategia de seguridad teniendo en consideración la actividad empresarial que se esté desarrollando; sin embargo, siguiendo a José de Jesús Angel Angel, se podrían suponer tres pasos fundamentales: una política global de seguridad; realizar un análisis de riesgos, y por último tomar las medidas correspondientes:

"Política global de seguridad: se debe establecer el *status* de la información para la empresa o la organización; debe contener un objetivo general, la importancia de la tecnología de la información para la empresa, el periodo de tiempo de validez de la política, los recursos con que se cuenta, los objetivos específicos de la empresa.

"Debe establecerse la calidad de la información que se maneja según su objetivo; la calidad que debe tener la información quiere decir cuándo o para quién la información debe ser confidencial, cuándo debe verificarse su integridad y cuándo debe verificarse su autenticidad, tanto de la información como de los usuarios.

"Análisis de riesgos: consiste en enumerar todo tipo de riesgos a los cuales está expuesta la información y cuáles son las consecuencias, los posibles atacantes entre personas empresas y dependencias de inteligencia, las posibles amenazas, etc., enumerar todo tipo de posible pérdida, desde pérdidas directas, como dinero, clientes, tiempo, etc., hasta indirectas: créditos, pérdidas de imagen, implicación en un litigio, pérdida de confianza, etc.

"Medidas de seguridad: esta parte la podemos plantear como la terminación de toda la estructura de la seguridad de la información. Una vez planteada una política de seguridad, decir cuánto vale la información, un análisis de riesgo, decir cuánto pierdo si le ocurre algo a mi información o qué tanto se gana si se protege; debemos establecer las medidas para que cumpliendo con la política de seguridad las pérdidas sean las menores posibles y que esto se transforme en ganancias, ya sea materiales o de imagen".

Con el desarrollo de este tema resulta inevitable abordar el relativo a los sistemas de vigilancia virtual. Luego de los lamentables y trágicos hechos acaecidos el 11 de septiembre de 2001 en las ciudades norteamericanas de Nueva York y Washington, y en Pensilvania, se evidenció cómo muchos de los sistemas de seguridad, por confiables, seguros y diversos que ellos sean, pueden en determinado momento ser fácilmente vulnerados.

A raíz de estos hechos, las agencias de seguridad de Estados Unidos, el Federal

Bureau of Investigation-FBI y la National Security Agency-NSA, han incrementado la acción de sus sistemas de seguridad y monitoreo, particularmente en la red mundial de información, Internet, y en las comunicaciones vía telefónica y fax.

Para ello estas agencias han desplegado aplicaciones y *software* de detección en línea, tales como el sistema Carnívoro (DCS100) del FBI y el sistema Echelon de la NSA.

En 1997 el FBI empezó a operar un sistema de vigilancia de tráfico virtual, particularmente de proveedores de servicios de Internet (ISP), denominado en ese momento como Omnívoro.

Omnívoro fue utilizado hasta finales de 1999, cuando hizo su incursión el sistema Dragonware Suite (DWS) el cual permitiría la reconstrucción de correos electrónicos, archivos electrónicos e inclusive *web sites* borrados.

Uno de los principales componentes del DWS, es precisamente el sistema Carnívoro, el cual es una herramienta desarrollada bajo el sistema operativo Windows NT/2000 y que se encarga de analizar y revisar la red y detectar comunicaciones sospechosas.

Los datos capturados por Carnívoro aparecen generalmente desconfigurados y sin orden. Por lo tanto es necesario compactarlos a través del uso de una herramienta denominada Packeteer, la cual les da un orden coherente.

Por último, un dispositivo denominado Coolminer se encarga de medir el grado de amenaza que reporten estos datos. De igual modo el sistema crea una base de datos, que se retroalimenta de datos previamente almacenados.

Así vemos cómo el desarrollo de los sistemas de seguridad no sólo depende de una iniciativa intelectual, sino también de las circunstancias socioeconómicas que cada país afronta, motivo por el cual los actores institucionales y privados deben rescatar su papel protagónico en estos temas, en pro de que los avances tecnológicos redunden en mayores niveles de seguridad y calidad de vida de nuestras sociedades.

C. PERSPECTIVA JURÍDICA

1. NATURALEZA JURÍDICA DE LOS SISTEMAS DE VIGILANCIA DIGITAL

La puesta en marcha del sistema de vigilancia digital representa, en opinión de muchos, una intromisión en la privacidad de los usuarios de la red mundial de información; no obstante, el FBI afirma que para su uso es necesario que medie orden de una corte judicial, de conformidad con las leyes vigentes en ese país. Es decir, a pesar de existir consenso frente a la necesidad de combatir a los criminales y terroristas del mundo, existe paralelamente una creciente preocupación de los defensores de los derechos civiles en cuanto éstos pueden ser seriamente limitados y hasta suspendidos.

En efecto, podría pensarse en una inminente violación al derecho de la privacidad de las comunicaciones personales, garantizadas actualmente para el caso colombiano por el artículo 15 de la Constitución Política. Dicho derecho fundamental constituye un derecho individual derivado del *status* de libertad protegido por la norma superior.

Ahora bien, en el ámbito de la legis-lación codificada es necesario detenernos en el estudio que el nuevo régimen penal colombiano le otorga al tema (Ley 599 de 2000).

En primer lugar, el artículo 192 del Código Penal consagra el delito de violación ilícita de comunicaciones con el siguiente tenor: "el que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida una comunicación privada dirigida a otra persona, o se entere indebidamente de su contenido, incurrirá en prisión de uno (1) a tres (3) años, siempre que la conducta no constituya un delito sancionado con pena mayor".

Por su parte, el artículo 301 del nuevo Código de Procedimiento Penal (Ley 600 de 2000) consagra lo relacionado con la interceptación de comunicaciones. Dicho artículo reza: "El funcionario judicial podrá ordenar, con el único objeto de buscar pruebas judiciales, que se intercepte mediante la grabación magnetofónica de las comunicaciones telefónicas, radiotelefónicas y similares que utilicen el espectro electromagnético, que se hagan o se reciban y que se agreguen al expediente las grabaciones que tengan interés para los fines del proceso. En este sentido, las entidades encargadas de la operación técnica de la respectiva interceptación, tienen la obligación de realizar la misma dentro de las cuarenta y ocho horas siguientes a la notificación de la orden.

"Cuando se trate de interceptación durante la etapa de la investigación la decisión debe ser remitida dentro de las veinticuatro (24) horas siguientes a la Dirección Nacional de Fiscalías. En todo caso, deberá fundamentarse por escrito. Las personas que participen en estas diligencias se obligan a guardar la debida reserva. Por ningún motivo se podrán interceptar las comunicaciones del defensor.

"El funcionario dispondrá la práctica de las pruebas necesarias para identificar a las personas entre quienes se hubiere realizado la comunicación telefónica llevada al proceso en grabación. Tales grabaciones se anexarán al expediente, por medio escrito certificado por el respectivo funcionario".

De la lectura de la anterior disposición legal se desprende una fuerte tendencia proteccionista de nuestra legislación del derecho a la intimidad de las personas, y significa que aun al interior de una investigación penal se deben observar una serie de requisitos para proceder a la interceptación de las comunicaciones de los particulares.

La Corte Constitucional tuvo la oportunidad de pronunciarse en relación con este tema y dijo al respecto: "de acuerdo con lo señalado con el artículo15, inciso 3.º de la Carta Política, para que las comunicaciones privadas puedan ser interceptadas y registradas deben cumplirse tres condiciones: que haya orden judicial, que exista una ley en la que se contemplen los casos en los cuales procede tal medida y que se cumplan las formalidades exigidas en la ley". Agregamos al concepto de la Corte que la orden judicial de interceptación de comunicaciones debe contemplar serios límites materiales, en el sentido que la información que se anexe al expediente debe guardar rigurosa relación con los hechos que se investigan en el proceso penal.

Por otra parte, y en complemento del anterior fallo, en providencia reciente el mismo tribunal constitucional determinó el alcance de los mensajes de datos consagrados en la Ley 527 de 1999.

En efecto, la Corte en una interpretación sistemática del ordenamiento

jurídico colombiano determinó que el artículo 6.º de dicha ley estaba acorde con los mandatos constitucionales y, por tanto, no reñía en especial con el artículo 28 de la Carta Política.

Dijo la Corte en providencia C-831 de 2001, con ponencia de Alvaro Tafur Galvis:

"La Ley 527 de 1999 no se limita al tema del comercio electrónico, aun cuando sus orígenes y su inspiración internacional conciernen fundamentalmente al ámbito mercantil.

"Al respecto recuerda el señor Procurador en su intervención que del análisis del respectivo expediente legislativo se comprueba que, si bien el proyecto inicial restringía el contenido de la norma al campo exclusivamente comercial, éste se fue ampliando para hacer finalmente referencia en forma genérica al acceso y uso de los mensajes de datos. En este sentido en el texto definitivo se eliminó la alusión al 'comercio electrónico en general' contenida en el título del capítulo I de la parte primera de la ley, para hacer simplemente referencia a 'las disposiciones generales'.

"En consecuencia, contrariamente a lo señalado por los intervinientes representantes de los ministerios de Justicia y de Desarrollo, ha de entenderse que la Ley 527 de 1999 no se restringe a las operaciones comerciales sino que hace referencia en forma genérica al acceso y uso de los mensajes de datos, lo que obliga a una comprensión sistemática de sus disposiciones con el conjunto de normas que se refieren a este tema dentro de nuestro ordenamiento jurídico y en particular con las disposiciones que como el artículo 95 de la Ley Estatutaria de Administración de Justicia se han ocupado de esta materia Dicha disposición señaló en efecto que los juzgados, tribunales y corporaciones judiciales podrán utilizar cualesquiera medios técnicos, electrónicos, informáticos y telemáticos para el cumplimiento de sus funciones, y que los documentos emitidos por los citados medios, cualquiera que sea su soporte, gozarán de la validez y eficacia de un documento original siempre que quede garantizada su autenticidad, integridad y el cumplimiento de los requisitos exigidos por las leyes procesales. Es decir que bajo el presupuesto del cumplimiento de los requisitos aludidos un mensaje de datos goza de validez y eficacia".

Lo anterior significa que la Corte Constitucional fijó jurisprudencia en cuanto al alcance jurídico de los mensajes de datos, en el sentido que no debe ser limitado dicho concepto al tema meramente mercantil o comercial, pues esa no fue la intención del legislador y la ley no lo limita en tal sentido. Bajo este entendido, los mensajes de datos gozan perfectamente de la protección de las normas citadas anteriormente.

En el caso particular de los programas "Echelon" y "Dragon Ware Suite", nos encontramos frente a un inconveniente adicional. Por la naturaleza de Internet, esto es, por ser una red mundial de información, pueden caer en observación y por tanto ser retenidos por las agencias de inteligencia mensajes o comunicaciones provenientes de cualquier lugar del planeta, presentándose sin lugar a dudas problemas tan serios como conflictos de leyes y jurisdicciones, siendo más grave aún en el tema que se estudia en este aparte, es decir, la posible confrontación de jurisdicciones y leyes penales.

En efecto, según información tomada del artículo de prensa arriba citado, en la

actualidad se están presentando investigaciones en el seno de la Unión Europea dirigidas a averiguar los registros de enormes movimientos no autorizados sobre sus plataformas tecnológicas (edición digital del diario *El Tiempo*, lunes 24 de septiembre de 2001, [www.eltiempo.com]).

En resumen, tenemos que, si bien la implementación de sistemas digitales de espionaje en Internet y demás medios telemáticos, a través de los cuales puede ser interceptada una gran variedad de información circulante en la red mundial de información, que puede verse traducida en avances significativos en las investigaciones de hechos criminales y terroristas, es también una realidad (y creciente preocupación en todos los estamentos de la sociedad), su uso indiscriminado va en detrimento de las libertades civiles y de los derechos individuales fundamen-tales de los particulares, siendo por tanto necesario un control multisectorial en esta clase de prácticas.

Para terminar, vale pena reflexionar si Colombia, entendiendo tanto el sector privado como el sector público, se encuentra preparada para afrontar una guerra contra los terroristas y piratas virtuales, habida consideración que, en concordancia con la tendencia mundial, cada vez se trasladan o ubican más actividades en el mundo virtual, lo cual se ve reforzado por lo dicho en el artículo publicado en *El Tiempo*, el 8 de octubre de 2001, respecto de la necesidad de tomar precauciones en este sentido, "sobre todo ahora que la publicación en línea, y dentro de poco la posibilidad de realizar transacciones a través de Internet, son algunas de las actividades de las entidades gubernamentales, según lo dispuesto por la Agenda de Conectividad del Gobierno" (edición digital del diario *El Tiempo*, lunes 8 de octubre de 2001, [www.eltiempo.com]).

2. NATURALEZA JURÍDICA DE LA FIRMA DIGITAL Y SU CLASIFICACIÓN

El abordaje jurídico de los sistemas de vigilancia digital impone la necesidad de introducirnos en el tema de las firmas digitales, razón por la cual para nuestro estudio definiremos firma digital como un conjunto de caracteres que se anexan a un documento (mensaje de datos), por medio de la cual se acredita quién es su autor (iniciador) y que no ha existido mutación o alteración alguna de los datos que se transmiten, desde la iniciación hasta la recepción del mensaje de datos (integridad).

En otras palabras, cuando un documento está revestido por una firma digital se puede obtener certeza sobre la persona de quien proviene el mensaje de datos y que la información contenida en el mismo no ha sido alterada ni vulnerada en su tránsito por la red.

El artículo 7.º de la Ley Modelo sobre Comercio Electrónico dictada por la Comisión de Naciones Unidad para el Derecho Mercantil Internacional- CNUDMI establece la posibilidad que la exigencia de la existencia de una firma manuscrita en un documento, sea satisfecha por medio electrónicos (firma electrónica) respecto de los mensajes de datos. En otras palabras, la firma electrónica se constituye como un equivalente funcional de la firma manuscrita o quirografaria.

Por su parte, el artículo 2.º de la Directiva Europea 93 del 13 de diciembre de 1999, por la cual se establece un marco comunitario para la firma electrónica, define lo que se entiende por firma

electrónica propiamente dicha y firma electrónica avanzada cuando dispone:

"Firma electrónica: los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medios de autenticación;

"Firma electrónica avanzada: la firma electrónica que cumple los requisitos siguientes: a. Estar vinculada al firmante de manera única; b. Permitir la identificación del firmante; c. Haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control; d. Estar vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable".

Por su parte, el tratadista español Pedro Alberto de Miguel Asensio afirma: "La firma digital es creada por medio de la clave privada del firmante (que genera una serie ininteligible de números y letras que representan la firma y que es diferente para cada documento que se firma) y es susceptible de ser verificada con la correspondiente clave pública, de modo que puede llegar a garantizar (típicamente con intervención –en particular para la autenticación– de un tercero que presta servicios de certificación) la autenticación e integridad del mensaje, así como su no repudio de origen" (*Derecho privado de Internet*, Civitas, 2001, p. 363).

El tambíen tratadista español Omar Castellá Muñoz, en su condición de *network solutions manager*, en un artículo sobre firma electrónica, presenta una serie de posibilidades de cara a una regulación de la firma electrónica partiendo para ello de lo establecido en la legislación española consignada en el Real Decreto Ley sobre Firma Electrónica (RDLFE) n.º 14 del 17 de septiembre de 1999 (cfr. [www.emprendedoras.com/articles/article26.htm]).

El artículo 3.º del RDLFE dispone los efectos jurídicos de la firma electrónica distinguiendo entre:

"Firma electrónica avanzada. Basada en certificado reconocido y que está producida por dispositivo seguro de creación de firma. Los efectos jurídicos de la firma electrónica avanzada son dos: tiene el mismo valor jurídico que la firma manuscrita y es admisible como prueba en juicio. Se establece una presunción legal: la firma electrónica avanzada tendrá los efectos jurídicos antedichos si el certificado reconocido en que se basa es expedido por un proveedor de servicios de certificación acreditado (persona física o jurídica que expide certificados reconocidos, pudiendo prestar otros servicios con relación a la firma electrónica) y el dispositivo de creación de firma está certificado según lo dispuesto en el artículo 12 del RDLFE.

"Firma electrónica (que no es avanzada). Graduación de su valor jurídico y será, en principio, admisible como prueba en juicio".

Propone el citado autor, con base en el artículo 3.º del RDLFE, la siguiente clasificación:

– *Firma electrónica alegal*. La firma electrónica, en su forma más básica, constituye un mecanismo de seguridad mínima, a la par que respeta la economía de la transacción.

– *Firma electrónica legal básica y avanzada*. En su forma básica o avanzada, la firma electrónica legal, como veremos, constituye uno o varios mecanismos de seguridad jurídica básica y, por lo tanto, con impacto en el costo por transacción.

– *Firma electrónica legal cualificada.* Representada técnicamente por formas más complejas de firma, combinada con otros elementos, como requisitos de operación de dispositivos seguros, evaluaciones de conformidad, etc., los cuales constituyen mecanismos de elevada seguridad jurídica, aunque suponen mayores costos por transacción.

– *Firma electrónica legal y legitimada.* Finalmente, las firmas y los requisitos de los documentos, puestos en combinación con determinados procedimientos y actuación de determinados profesionales, suponen mecanismos de muy elevada seguridad jurídica, pero la interacción de estos grupos de requisitos (requisitos, firmas y procedimientos) suponen un costo que únicamente se justifica a la luz de la realización de transacciones de costo ciertamente elevado.

Así las cosas, la conclusión lógica de todo lo anterior apunta a establecer que el uso de la firma electrónica y el reconocimiento de la eficacia jurídica de la firma electrónica básica, avanzada, cualificada y otras, como la legitimada, se soportan en los certificados electrónicos como elementos esenciales para la validez de la firma electrónica luego de ser comprobada por éste.

Ahora bien, para el caso colombiano, el artículo 2.º literal c de la Ley 527 de agosto de 1999 define la firma digital como:

"Firma digital. Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación".

Así mismo el artículo 7.º del referido texto legal expresa:

"Firma. Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:

"a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación.

"b) Que el método sea tanto confiable como apropiado para el propósito el cual el mensaje fue generado o comunicado.

"Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que no exista una firma".

Para firmar digitalmente un documento electrónico el autor utiliza su clave privada (num. 4 art. 1.º Dcto. 1747 de 2000), para que por medio de la clave pública sea confirmada posteriormente la autenticidad del mensaje.

El artículo 28 de la Ley 527 de 1999 contempla las características de autenticidad y de no repudio antes vistas, en el siguiente sentido: "cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo".

Igualmente, el artículo citado trae lo que la doctrina conoce como *equivalentes funcionales*, mencionados en este estudio, es decir, que la ley le otorga a la firma digital, y por ende al documento firmado

de esta forma, la misma validez, fuerza y alcance probatorio que a la firma manuscrita y al documento contenido en soporte material. Así, la tradicional firma manuscrita o quirografaria, que implica la aceptación de la autoría de determinada declaración de voluntad por parte de quien suscribe el documento, es reemplazada por una firma digital.

En este orden de ideas, la firma digital consiste "en encriptar un texto con la clave privada del firmante" (Ernesto Rengifo. "Comercio electrónico, documento electrónico y seguridad jurídica", en *Memorias Comercio Electrónico*, Universidad Externado de Colombia, noviembre de 2000).

En este sentido, la Corte Constitucional de Colombia, en sentencia C-662 del 8 de junio de 2000, M. P.: Fabio Morón Díaz, frente al tema de las firmas digitales manifestó lo siguiente:

"A través de la firma digital se pretende garantizar que un mensaje de datos determinado proceda de una persona determinada; que ese mensaje no hubiera sido modificado desde su creación y que el receptor no pudiera modificar el mensaje recibido.

"Una de las formas para dar seguridad en la creación y verificación de una firma digital es la criptografía, la cual es una de las ramas de las matemáticas aplicadas que se ocupa de transformar, mediante un procedimiento sencillo, mensajes en forma aparentemente inteligibles y devolverlas a su forma original.

"Mediante el uso de un equipo físico especial, los operadores crean un par de códigos matemáticos, a saber: una clave secreta o privada, conocida únicamente por su autor, y una clave pública, conocida como del público. La firma digital es el resultado de la combinación de un código matemático creado por el iniciador para garantizar la singularidad de un mensaje en particular, que separa el mensaje de la firma digital y la integridad del mismo con la identidad de su autor.

"La firma digital debe cumplir idénticas funciones que una firma en las comunicaciones consignadas en papel. En tal virtud, se toman en consideración las siguientes funciones de ésta:

> "Identificar a una persona como el autor;
> "Dar certeza de la participación exclusiva de esa persona en el acto de firmar;
> "Asociar a esa persona con el contenido de documento.

"Concluyendo, es evidente que la transposición mecánica de una firma autógrafa sobre papel y replicada por el ordenador en un documento informático no es suficiente para garantizar los resultados tradicionalmente garantizados por la firma autógrafa, por lo que se crea la necesidad de que existan establecimientos que certifiquen la validez de estas firmas".

Al anterior análisis es necesario agregar la frecuencia con que expresiones tales como firma digital, firma digitalizada, firma quirografaria o manuscrita y firma mecánica se tienden a confundir, en su alcance y contenido real; por ello es preciso hacer una distinción entre unas y otras, para concluir que es sólo la firma digital la que presenta una trascendencia real para el comercio electrónico, habida cuenta que es la que permite dotar a un documento electrónico del mismo alcance, efecto y validez probatorio de un documento material (equivalente funcional).

Firma digitalizada: es aquella que se obtiene de reproducir una firma quirografaria o manuscrita a través de medios

mecánicos, como el escáner, y llevarla a medio magnético para permitir su posterior reproducción. Pensemos por ejemplo en las firmas que muchas personas plasman en las entidades financieras al momento de abrir una cuenta u obtener un determinado producto.

Firma quirografaria o manuscrita: es la que se utiliza de manera ordinaria por las personas para manifestar su consentimiento en todo tipo de documentos materiales; es también denominada firma autógrafa.

Firma mecánica: es la que se utiliza para ser estampada en una serie de documentos producidos en serie y donde por medio de un acto administrativo previo se permite su utilización con total validez. Pensemos por ejemplo en la firma utilizada en los certificados de cámara de comercio expedidos para acreditar la existencia y representación legal de las sociedades comerciales. En este sentido, es de singular importancia lo establecido en el Decreto 2150 de 1995 sobre eliminación de tramites, al permitir la utilización de esta clase de firmas.

3. ENTIDADES DE CERTIFICACIÓN: CONCEPTO, CLASES Y CERTIFICADOS DIGITALES

Cubierto el tema de las firmas digitales, es preciso desarrollar para su complementariedad el tema de las entidades de certificación y su aplicación en los sistemas de vigilancia digital. Así, éstas constituyen una "tercera parte confiable" en la relación contractual, cuya función es la de acreditar o "certificar" el vínculo existente entre una determinada clave y su propietario real, lo cual realiza a través de la expedición de un certificado digital.

Según el artículo 29 de la Ley 527 de 1999 pueden ser entidades de certificación las personas jurídicas, públicas o privadas, nacionales o extranjeras, y las cámaras de comercio que obtengan autorización de la Superintendencia de Industria y Comercio (SIC).

Igualmente el parágrafo primero del artículo 1.º de la Ley 588 de 2000, cuyo articulado regula lo relacionado con la función notarial, expresamente autoriza a los notarios y cónsules para actuar como entidad de certificación, previa la autorización respectiva por la SIC.

Las entidades de certificación deben cumplir con una serie de requisitos para ser autorizadas como tales por la Superintendencia de Industria y Comercio, entidad esta que a su turno actuará como entidad de certificación de las certificadoras.

Estos requisitos se pueden resumir en tres grandes grupos:

– Requisitos de orden técnico y de infraestructura.
– Requisitos presupuestales, de capital y de constitución de garantías.
– Requisitos y calidades personales de sus administradores.

El *modus operandi* de estas entidades se puede asimilar a una especie de notario electrónico, teniendo en cuenta sin embargo que la entidad de certificación distinta a una notaría o a un consulado no ejerce la función notarial ni es depositaria de la fe pública; simplemente es un tercero imparcial distinto a las partes involucradas en la relación contractual: la entidad de certificación emite una declaración en el sentido de verificar

ciertos datos, expidiendo un certificado de claves, el cual está firmado por su propia clave, para que de este modo se garantice la autenticidad de la información, su integridad y la identidad de las partes que se proporciona.

El Decreto 1747 de 2000 trae una división de las entidades de certificación, clasificándolas en cerradas y abiertas.

Las entidades de certificación cerradas son aquellas que se encargan de desarrollar actividades referidas al "intercambio de mensajes entre la entidad y el suscriptor, sin exigir remuneración por ello" (art. 1.º num. 8 Dcto. 1747 de 2000). Sobre este punto cfr. [www.certinet.com] (hoy Latin Trust Andina S. A.).

Las autoridades de certificación abiertas por su lado, se encargan de ofrecer servicios propios de toda entidad de certificación, bajo condiciones tales como: a) su uso no se limita al intercambio de mensajes entre la entidad y el suscriptor, y b) recibe remuneración por éstos. Muy pronto entrará en funcionamiento Certicamaras como una de las primeras entidades de certificación abiertas (cfr. [www.certicamaras.com.co]).

La Ley 527 de 1999 define en su artículo 32 los deberes de las entidades de certificación, estableciendo entre otros los siguientes:

> a) Emitir certificados conforme a lo solicitado o acordado con el suscriptor;
> b) Implementar los sistemas de seguridad para garantizar la emisión y creación de firmas digitales, la conservación y archivo de certificados y documentos en soporte de mensaje de datos;
> c) Garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor;
> d) Garantizar la prestación permanente del servicio de entidad de certificación;
> e) Atender oportunamente las solicitudes y reclamaciones hechas por los suscriptores;
> f) Efectuar los avisos y publicaciones conforme a lo dispuesto en la ley;
> g) Suministrar la información que le requieran las entidades administrativas competentes o judiciales en relación con las firmas digitales y certificados emitidos y en general sobre cualquier mensaje de datos que se encuentre bajo su custodia y administración;
> h) Permitir y facilitar la realización de las auditorías por parte de la Superintendencia de Industria y Comercio;
> i) Elaborar los reglamentos que definen las relaciones con el suscriptor y la forma de prestación del servicio;
> j) Llevar un registro de los certificados.

Estos deberes se relacionan con las necesidades que tienen los usuarios del comercio electrónico, tales como la protección de la disponibilidad, confidencialidad e integridad de los sistemas.

> – La disponibilidad es la propiedad técnica por la cual los datos, la información y los sistemas de información son accesibles y funcionan puntualmente.
> – La confidencialidad es la propiedad técnica a través de la cual los datos y la información no se hacen disponibles, ni se dan a conocer a personas, entidades y procesos no autorizados.
> – La integridad es la característica por la que los datos y la información son precisos y completos, e implica que los datos o la información no han sido modificados o alterados (Emilio José Archila Peñalosa. *Entidades de certificación*, Superintendencia de Industria y Comercio, septiembre de 1999).

Bajo este entendido, los deberes de estas entidades deben ser vistos desde tres ópticas distintas: la relación de las entidades certificación con el usuario, con la administración y con el público en general.

"En relación con el suscriptor, el deber principal de la entidad de certificación es cumplir oportuna y eficientemente con sus compromisos contractuales –emitir certificados, generar y certificar firmas, conservar la información en debida forma y subsanar cualquier falla u omisión del servicio– y, en todo caso, proteger la información que se le ha confiado.

"Frente a la administración y al público, debe atender las obligaciones de confianza y publicidad, dirigidas, en primer lugar, a garantizar la transparencia y libre competencia en el mercado y, en segundo lugar, a permitir que se ejerzan por parte de la Superintendencia de Industria y Comercio las labores de control y vigilancia" (ibíd.).

El máximo tribunal constitucional de nuestro país, en la sentencia ya citada, también se ocupó del tema de las entidades de certificación, cuyos apartes más importantes se transcriben a continuación:

"Uno de los aspectos importantes de este proyecto es la posibilidad de que un ente público o privado con poderes para certificar proporcione la seguridad jurídica a las transacciones por vía informática. Estos entes son las entidades de certificación, que una vez autorizadas están facultadas para: emitir certificados en relación con claves criptográficas de todas las personas, ofrecer o facilitar los servicios de registro estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales".

En relación con la naturaleza jurídica de dichas entidades, la sentencia afirma: "La naturaleza de la función de las entidades de certificación se considera como la prestación de un servicio público".

Por último, vale la pena recalcar la afirmación hecha por la Corte en relación con la función que éstas prestan:

"En consecuencia, las entidades de certificación son las encargadas, entre otras cosas, de facilitar y garantizar las transacciones comerciales por medios electrónicos o medios diferentes a los estipulados en papel, e implican un alto grado de confiabilidad, lo que las hace importantes y merecedoras de un control ejercido por un ente público, control que redunda en beneficio de la seguridad jurídica del comercio electrónico".

Frente a la posibilidad que los notarios se constituyan en entidades de certificación, el artículo 1.° de la Ley 588 de 2000 dispuso:

> *Notariado y competencias adicionales*. El notariado es un servicio público que se presta por los notarios e implica el ejercicio de la fe pública o notarial.
>
> Parágrafo 1.° Las notarías y consulados podrán ser autorizados por la Superintendencia de Industria y Comercio como entidades de certificación, de conformidad con la Ley 527 de 1999.
>
> Parágrafo 2.° Las notarías y consulados podrán transmitir como mensajes de datos, por los medios electrónicos, ópticos y similares a los que se refiere el literal a del artículo 2.° de la Ley 527 de 1999, a otros notarios o cónsules, copias, certificados, constancias de los documentos que tengan en sus archivos, así

> como de los documentos privados que los particulares quieran transmitir con destino a otros notarios y cónsules o personas naturales o jurídicas. Dichos documentos serán auténticos cuando reúnan los requisitos técnicos de seguridad para transmisión de mensajes de datos que establece la Ley 527 de 1999.

En resumen, bajo el amparo de la anterior disposición se autoriza expresamente a los notarios y cónsules para que presten los servicios certificadores en dichos términos, lo que a la postre puede resultar beneficioso en el procedimiento de conformación de estas entidades.

En cuanto a la naturaleza jurídica de los certificados digitales que las entidades de certificación emiten, a nivel de la investigación se concluye que son registros electrónicos que acreditan que una clave privada pertenece a determinado individuo o entidad. "La idea es que una tercera entidad intervenga en la administración de las claves privada y pública y asegure que las claves públicas tengan asociado un usuario claramente identificado" (Angel. "Criptografía para principiantes", cit.).

En este orden de ideas, "los certificados digitales tienen una similitud con las licencias de conducir: las primeras permiten viajar por las carreteras, los certificados digitales permiten navegar por la red Internet; la principal característica es que da identidad al usuario y puede navegar con seguridad" (ibíd.).

Por otro lado, el Decreto 1747 de 2000 define los certificados en su artículo 1.º numeral 6 como un "mensaje de datos firmado por la entidad que dé certificación que identifica tanto a la entidad de certificación que lo expide como al suscriptor y contiene la clave pública de este".

Muchos de los certificados digitales actualmente existentes consisten en tarjetas inteligentes o en tokens que poseen en su estructura un microchip que les permite almacenar una gran cantidad de información.

Una vez el usuario tiene un certificado electrónico en su poder, está en capacidad de identificarse en la red en forma de bits, logrando entrar en el mundo del comercio electrónico de forma segura, e intercambiar la información de forma protegida y confidencial.

Los certificados digitales tienen como función primordial brindar un registro electrónico donde constan ciertos elementos y hechos que garantizan todo tipo de transacción en la red.

El tratadista español, Pedro Alberto de Miguel Asensio, en su obra ya reseñada menciona la importancia de los certificados digitales cuando:

"Habida cuenta de que la plenitud de los efectos jurídicos de la firma electrónica se subordina a que esté basada en un 'certificado reconocido' y que haya sido producida por 'un dispositivo seguro de creación de firma', presumiéndose que concurren estas circunstancias si el certificado ha sido expedido por un 'prestador de servicios de certificación acreditado' y el dispositivo de creación se encuentra 'certificado'".

Ordinariamente los certificados digitales son expedidos por una entidad de certificación, que tiene una cobertura territorial específica, enmarcada ordinariamente por la autoridad que la acredita para ejercer tal función.

Para el caso colombiano, es la Superintendencia de Industria y Comercio la entidad que autoriza el funcionamiento de las entidades de certificación en nuestro

territorio, previo el cumplimiento de los requisitos ya mencionados. A su turno, la Superintendencia funge como certificadora de certificadoras.

Con base en lo anterior se tiene que los certificados digitales emitidos por las entidades de certificación cuya autorización de funcionamiento se da por parte de la Superintendencia de Industria y Comercio tienen una cobertura eminente-mente local a nivel nacional y acreditan a sus suscriptores dentro del territorio nacional.

Las entidades de certificación extranjeras, que emiten certificados y crean firmas digitales, de ordinario también tienen una cobertura restringida territorialmente hablando.

Puede suceder que exista una normatividad uniforme o de integración comunitaria, como por ejemplo la que existe en la Unión Europea (EU), y que podría, por qué no, existir a nivel de la Comunidad Andina de Naciones (CAN), que permita extender su espectro de influencia a las entidades de certificación y por ende a sus certificados legítimamente emitidos.

Otra alternativa es que existan convenios internacionales bilaterales o multilaterales que establezcan tal situación de validez de certificados expedidos por entidades sometidas al régimen de un país miembro.

Una alternativa que ha sido acogida por muchas legislaciones nacionales, siguiendo para ello lo establecido en las normas tipo que sobre comercio electrónico ha expedido la Comisión de Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI-UNCITRAL), es la de extender la validez de certificados emitidos por certificadoras extranjeras en su territorio, obviamente bajo ciertas circunstancias y situaciones.

Surge así el tema de las certificaciones recíprocas, a través de las cuales una entidad de certificación con asiento en un territorio determinado avala o legitima los certificados emitidos válidamente en su país de origen y en el que se pretende hacerlos valer, por una entidad extranjera, para que tengan plenos efectos en el territorio de la primera.