Situación normativa de la Sociedad de la Información en Colombia

Juan Fernando Salazar[*]

Resumen

El presente artículo tiene como objetivo general describir la situación normativa de dos grandes temas de la Sociedad de la Información en Colombia: (i) el comercio electrónico, las firmas digitales y las entidades de certificación y (ii) los delitos informáticos y los delitos cometidos por computador. En tal sentido, proyecta la naturaleza extraterritorial inherente al fenómeno de la Sociedad de la Información, y compara las soluciones ya implementadas en el país con esfuerzos normativos realizados en otras regiones, así como los impulsados por organismos internacionales. El resultado de las consideraciones concluye que el desarrollo normativo de la Sociedad de la Información tiene que estar basado en la existencia de políticas públicas de largo plazo, que no rivalicen con el proceso globalizador.

Palabras claves

Sociedad de la Información, comercio electrónico, firmas digitales, entidades de certificación, delitos informáticos, TIC.

Abstract

This article aims to describe the laws that regulate two main Information Society issues in Colombia: (i) e-commerce, digital signatures and certification authorities, and (ii) electronic crimes and crimes committed by electronic means. In this sense, the Information Society is projected as a cross-border phenomenon, and legal solutions implemented in Colombia are compared with those of other regions, as well as those promoted by international organizations. This analysis leads to the conclusion that a legal framework for the Information Society has to be based on the existence of long-term public policies, which do not run counter to the process of globalization.

Keywords

Information Society, E-commerce, Digital signatures, Certification authorities, Electronic crimes, ICT.

---

[*] Abogado, Magister de la Erasmus Universiteit Rotterdam. Pofesor del Departamento de Ciencia Jurídica y Política de la Pontificia Universidad Javeriana Cali.

Recibido: 6 de mayo de 2009 Aprobado: 28 de mayo de 2009

1. Introducción

Las primeras conexiones a Internet en Colombia, y la consecuente delegación de números IP[1] para el país, ocurrieron en el primer lustro de la década de los noventa del siglo XX. Sin embargo, el desarrollo explosivo que Internet ha tenido a partir de la segunda mitad de la década ha estado marcado por el crecimiento de la World Wide Web[2]. Es también un periodo en el cual la cantidad de conectados en el país ha aumentado considerablemente, pero aún sigue manteniéndose en un número reducido de la población. De acuerdo al informe trimestral de conectividad, publicado por la Comisión de Regulación de Telecomunicaciones[3], los suscriptores del servicio de acceso a Internet superaron la barrera de los dos millones a diciembre de 2008. Siguiendo el riguroso método estadístico de la multiplicidad, el ente regulador colombiano estima que el total de usuarios del servicio de acceso a Internet en el país es de unos diecisiete millones de personas, cifra que, al ser comparada con la población colombiana —estimada en cuarenta y cuatro millones de habitantes—, representa una penetración de 38,6%. Aunque esto es algo mejor que el promedio de otros países en vías de desarrollo, es todavía muy inferior al ponderado de los países desarrollados. Sin embargo, Colombia se encuentra por encima del promedio mundial, estimado por Internet World Stats en 23,8%[4].

---

[1] Sigla del inglés *Internet Protocol*. Garrote Fernández-Díez (2003: 21-22) indica que una dirección IP permite reconocer un determinado computador en Internet, diferenciándolo de todas las demás máquinas. Este método de identificación es incómodo de utilizar y recordar para las personas, y por ello tiene su traducción en el llamado sistema de nombres de dominio.

[2] World Wide Web significa "telaraña mundial". Garrote Fernández-Díez (2003: 27-31), en una primera aproximación conceptual a la WWW, indica que esta se comporta como un soporte electrónico en el que se almacenan textos, sonidos e imágenes de una manera ordenada y fácilmente accesible para el usuario, incluso si éste no es muy versado en aplicaciones informáticas. El éxito de la WWW también se explica por el hecho de que su manejo es intuitivo; desde una mera observación de la interfaz gráfica de un navegador, cualquier persona puede acceder a la WWW con un grado de eficiencia y sencillez muy elevado.

[3] Como organismo regulador del mercado de las telecomunicaciones en Colombia, la CRT cumple la misión de promover la competencia y la inversión, así como proteger los derechos de los usuarios. En su página web www.crt.gov.co están disponibles los informes de Internet, que periódicamente revelan los resultados de investigaciones estadísticas del número aproximado de usuarios de Internet en el país, a partir de la cantidad de accesos o suscripciones.

[4] *Internet World Stats,* Miniwatts Marketing Group. Consultada 20 de abril de 2009. <http://www.internetworldstats.com/stats.htm>

Aun con este porcentaje de penetración, que todavía no abarca la mitad de la población, e impulsado por desarrollos de otros países y por recomendaciones de organismos internacionales, el Estado colombiano ha emprendido una tarea de diseño de estrategias y regulaciones en relación con el uso de las tecnologías de información y comunicación (en adelante, TIC) y, por ende, las respectivas relaciones jurídicas propias de la Sociedad de la Información[5].

Infortunadamente, muchos de estos desarrollos estratégicos no se han hecho armónicamente ni han sido fundamentados en políticas públicas de largo alcance[6]. Este fenómeno sucede primordialmente porque el enfoque de la doctrina y las propuestas normativas para las TIC en Colombia se han centrado en el estudio de las tecnologías y las posibles implicaciones jurídicas que estas pueden tener, sin verdaderamente entrar a analizar algunas de las cuestiones fundamentales en este debate, como lo es el papel del derecho con respecto a las innovaciones tecnológicas, o si la Sociedad de la Información constituye un nuevo paradigma que requiera nuevas soluciones jurídicas. Refiriéndose a este punto, Aboso y Zapata (2006: 8) indican que la regulación de las TIC involucra "toda una visión sociocultural y política del desarrollo tecnológico, la que no puede soslayar que también gravitan intereses económicos sectoriales"; consecuentemente, habrá posturas "hiperlibertarias", autorregulatorias o regulatorias.

Colombia no se adscribe de lleno a ninguna de las posturas anteriores, denotando el largo camino por recorrer para consolidar una política de Estado que le permita al país insertarse en la Sociedad de la Información. Mientras tanto, de las deliberaciones han estado ausentes cuestionamientos relacionados

[5] En este sentido, vale destacar la Agenda de Conectividad, creada durante el gobierno de Andrés Pastrana para impulsar el uso y la masificación de las TIC en el país. El programa ha sufrido una serie de cambios y ajustes en los que la prioridad es articular el trabajo entre las entidades del gobierno, la comunidad, el sector productivo y la academia. Hoy se desarrolla bajo las políticas del Plan Nacional de Desarrollo que buscan integrar los temas de educación, salud, seguridad y lucha contra la corrupción.

[6] La concepción inicial de la Agenda de Conectividad, como programa del Ministerio de Comunicaciones encargado de impulsar el uso y masificación de las TIC como herramienta dinamizadora del desarrollo social y económico del país, ha sido gradualmente desplazada, por lo menos en protagonismo, por el Plan TIC. Este Plan busca lograr que "todos los colombianos estén informados y conectados" (*Colombia Plan TIC.* Ministerio de Comunicaciones. Consultada el 24 de abril de 2009. <http://www.colombiaplantic.org/>). A través de sus proyectos, busca mejorar el desempeño de Colombia en los ejes de educación, justicia, salud, competitividad, investigación, desarrollo y formación, mediante el uso de las TIC.

con la axiología de las normas que rigen fenómenos de la Sociedad de la Información, pues si los principios jurídicos de éstas fueran diferentes a los tradicionales, seguramente las formas de las instituciones jurídicas que de ellos se deriven también tendrían características nuevas.

El presente artículo no pretende responder estas importantísimas cuestiones, sino que tiene como objetivo general establecer la situación normativa de los grandes temas de la Sociedad de la Información en Colombia. Los temas contemplados son dos: (i) el comercio electrónico, las firmas digitales y las entidades de certificación y (ii) los delitos informáticos y los delitos cometidos por computador. En un futuro escrito, resultado de este mismo esfuerzo investigativo, se comentará lo pertinente a la protección de datos personales y el gobierno electrónico.

Para abordar los temas pretendidos, es crucial comprender que la naturaleza extraterritorial, inherente al fenómeno de la Sociedad de la Información, requiere soluciones coordinadas e integradas[7]. Esto puede realizarse al comparar las soluciones ya implementadas con esfuerzos normativos realizados en otras regiones, así como con esfuerzos impulsados por organismos internacionales[8].

Como lo advierte Camacho Clavijo (2005: 31-32), la Sociedad de la Información hace referencia a un conjunto de actividades comerciales, comportamientos sociales, actitudes individuales y formas de organización política y administrativa que comparten el mismo medio de transmisión de la información: las redes de comunicación. Requiere, entonces, una adecuación del derecho y por tanto de las normas legales pertinentes para dicho ámbito social. Es en este marco que Colombia ha estado desarrollando regulaciones en torno a diversos temas de la Sociedad de la Información[9], siendo las normas relacionadas con el comercio electrónico y con las firmas digitales las primeras

---

[7] Con ocasión de la contratación comercial electrónica, Zapata (2002: 215) plantea preguntas tan interesantes como esta: "¿ha creado el comerciante un establecimiento en la jurisdicción del comprador para hacer ventas o, es el comprador quien ha viajado virtualmente a la jurisdicción del vendedor para hacer una compra?" La necesidad de coordinación internacional, producto de la extraterritorialidad de los fenómenos de la Sociedad de la Información, es evidente.

[8] Pertinentemente, Zapata (2002:215) destaca el trabajo ad hoc de la Cámara de Comercio Internacional, que plantea con meridiana precisión el tema de la extraterritorialidad de las relaciones jurídicas.

[9] En el mismo sentido, Davara Rodríguez (2006: 24-25), realiza interesantes consideraciones en torno a la necesidad de regular los novedosos temas que ha impuesto la Sociedad de la Información.

en haber hecho su aparición. Fueron seguidas, más recientemente, por aquellas que penalizan conductas que atentan contra la información, como bien jurídico tutelado por el derecho penal, y por las que velan por la protección de datos personales, en desarrollo de los derechos fundamentales consagrados en el artículo 15 de la Constitución Política.

Es importante señalar que muchas experiencias normativas han generado resultados ineficaces, por lo que, en este segmento del conocimiento jurídico, la investigación encuentra un bastión para indagar sobre las buenas prácticas que deben caracterizar las relaciones de la Sociedad de la Información (Iriarte Ahon, 2005).

También es importante decir que las normas, por sí solas, no generan un aumento en el uso de las TIC, ni tampoco las TIC por sí solas generan desarrollo social sostenible. Se requiere el diseño y desarrollo de políticas públicas de largo plazo, que enmarquen la expedición de las normas que regulan las novedosas relaciones jurídicas de la Sociedad de la Información. Esta es, pues, la idea central del artículo: el desarrollo normativo de la Sociedad de la Información tiene que estar basado en la existencia de políticas públicas de largo plazo, que no rivalicen con el proceso globalizador.

2. El comercio electrónico, las firmas digitales y las entidades de certificación

De las normas jurídicas relacionadas con temas de la Sociedad de la Información, la referida al comercio electrónico, firmas digitales y entidades de certificación es la más desarrollada, legal, jurisprudencial y doctrinalmente. La Ley 527 de 1999, conocida popularmente como Ley de Comercio Electrónico, es en realidad una ley que avala la aptitud probatoria de los mensajes de datos, reconoce las firmas digitales y crea las entidades de certificación, más que tratarse de una norma de contratación electrónica per se.

Entre los insumos básicos para el desarrollo de dicha norma, se encuentran la Ley de Firma Digital de Utah de 1996 y la Ley Modelo de Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional[10] de 1996. Colombia fue el primer país de América Latina en expedir una norma de tal naturaleza[11].

[10] Esta comisión permanente de las Naciones Unidas tiene por objetivo fomentar la armonización y unificación progresivas del derecho mercantil internacional. Entre sus frentes de trabajo más destacados está el de comercio electrónico, que, aparte de la ley modelo de comercio electrónico, ha trabajo en temas como el valor jurídico de la

La Ley de Comercio Electrónico colombiana exige la utilización de una Infraestructura de Clave Pública[12] (PKI) con un organismo regulador supracertificador, sistema que algunos (Richards, 1999: 873-907) han denominado el modelo Utah, en oposición al modelo de operación abierta que configura la equivalencia funcional a partir de los usos y costumbres del mercado. Otros países del ámbito regional que comparten el modelo adoptado por Colombia son Argentina, Brasil y Venezuela, mientras que otros, como los caribeños Bermuda, Belice e Islas Caimán, han optado por el modelo abierto. La Directiva Europea de Firma Electrónica optó por un modelo intermedio, que pretende ser tecnológicamente neutro y que puede tener o no un ente regulador o certificador.

La norma en cuestión se ha desarrollado desde la perspectiva de la validación del documento electrónico a través de las equivalencias funcionales de escrito, firma y original, siendo entonces la regulación de la firma digital una consecuencia. Los casos del Perú, Brasil y Argentina han planteado la regulación desde la firma misma como instrumento para la manifestación de la voluntad.

Los diferentes modelos y aproximaciones por los que han optado los diferentes países generan dificultades reales a la integración normativa sobre este particular. Al respecto, el caso colombiano no reúne de forma integral los diferentes temas que se pueden deducir del análisis comparado, como la regulación de las firmas electrónicas de género, la manifestación de la voluntad por medios electrónicos o la contratación electrónica. Este es un problema del que adolece la Ley 527 de 1999, sin olvidar que, a la luz del

---

documentación electrónica, la Ley Modelo de la CNUDMI sobre firmas electrónicas (2002), la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (2007) y el Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firmas electrónicas (2009).

[11] Actualmente, todos los países latinoamericanos gozan de normatividad en torno a este tema, naturalmente, con antecedentes legislativos diferentes, por lo que el propósito de unificación y armonización en este sentido no está del todo satisfecho.

[12] Al respecto, Rincón Cárdenas (2006b: 220) explica que este sistema implica la existencia de dos llaves o claves para ser utilizadas; una llamada clave pública, que, como su nombre lo indica, puede ser conocida y es accesible por toda persona, y otra segunda clave denominada privada, la cual se encuentra sólo en conocimiento de su tenedor. De esta manera, un mensaje es cifrado al momento de su envío con la llave pública y luego, al ser recibido, es descifrado con la llave privada o secreta, que solamente conoce el destinatario del mensaje.

principio de flexibilidad, la norma no pretende regular los pormenores del comercio electrónico. Sin embargo, la vigencia de la regla debe monitorearse, merced a la constante innovación tecnológica, que puede poner en el mercado mejores alternativas para resolver, con mayor eficiencia, las intenciones del legislador de 1999.

Hay que analizar también el hecho de que la expedición de la Ley 527 de 1999 se vio impulsada desde la perspectiva comercial (tanto en temas de comercio electrónico, como en el negocio mismo de la certificación digital), por lo cual muchas de sus disposiciones están pensadas desde la perspectiva de cómo acreditar a los actores en los procesos de comercio electrónico, sin que se haya pensado en la firma como un instrumento de expresión humana[13], sino únicamente desde la perspectiva contractual.

Lo anterior es parte de un movimiento global que pretende institucionalizar el reconocimiento y validez de las firmas digitales como herramienta primordial para el desarrollo del comercio electrónico. Al respecto, Peña Valenzuela (2003: 209) afirma que Colombia es un país líder en la regulación de la firma digital, aunque reconoce que falta un mayor acceso de los ciudadanos a la red y más capital de riesgo para incentivar la naciente industria de Internet.

En el caso de las entidades de certificación, la Ley de Comercio Electrónico encuentra su decreto reglamentario en el 1747 de 2000, el cual determina el funcionamiento de dichas entidades y establece el contenido de los certificados que emitan. El contenido del certificado digital está, a su vez, tomado de las recomendaciones dadas por normas mínimas internacionales.

Con relación a la posibilidad de utilizar un certificado emitido fuera del país, ello es posible en virtud a las certificaciones recíprocas del artículo 43 de la ley, las cuales son válidas en la medida que una entidad de certificación nacional avale, conforme a las normas colombianas, el certificado emitido en el exterior.

El gobierno nacional ha encomendado la labor de inspección y vigilancia de la Infraestructura de Clave Pública a la Superintendencia de Industria y

[13] La necesidad de adaptar los medios probatorios a la Sociedad de la Información es imperiosa, en la medida en que la digitalización de muchos contenidos y obras y la realización de transacciones internacionales sobre intangibles, así como la publicación creciente de datos en Internet, generan conflictos que deben resolverse por tribunales o árbitros en los cuales las pruebas son generalmente presentadas en formato electrónico.

Comercio, que a priori concede licencia a las personas autorizadas por ley para conformarse como entidades de certificación. En ese orden de ideas, una entidad de certificación en Colombia podrá obtener licencia de funcionamiento si se atempera a los consensos tecnológicos (como los basados en normas ISO o estándares ITU) reconocidos por el ente gubernamental.

El derecho colombiano se adecua a las tendencias internacionales en seguridad de la información, no tomándolas como un dogma, sino entendiendo que no se puede intentar cambiar algo que está definido desde la técnica, es decir, a diferencia de otras temáticas donde la costumbre social genera diferencias sobre un mismo tema, no es factible entender de diferentes maneras un fenómeno tecnológico, como el de la Infraestructura de Clave Pública. La existencia de figuras divergentes impediría una acción adecuada en procesos sociales que traspasan fronteras.

Es claro, sin embargo, que Colombia se adhiere a un modelo técnico estandarizado, de los varios que han sido acogidos por las diferentes legislaciones del orbe. Por lo tanto, urgen iniciativas eficaces de armonización que deriven en esquemas de integración internacional, por ejemplo, para el intercambio de información por medios digitales con certificación cruzada.

Estos esfuerzos legislativos, que están encaminados a generar confianza en los usuarios de las redes electrónicas, no tienen aún un eco en la sociedad de consumo en Colombia. Al respecto, Rincón Cárdenas (2006a: 117-118) observa que la mayoría de las transacciones realizadas a través de Internet en el país son transacciones no monetarias, como consultas de saldos y extractos, las que representan más de la mitad de las hechas a través de la red. Porcentualmente, siguen siendo muy superiores al total de las transacciones monetarias realizadas por el mismo medio, sobre todo en la banca personal. Utilizando datos de la Asociación Bancaria de Colombia, Rincón Cárdenas concluye que puede pronosticarse que las operaciones bancarias a través de Internet habrán de aumentar paulatinamente, así como lo hará la gama de servicios que en ellas se ofrecen.

La inversión que las compañías realicen a efectos de proveer servicios por canales electrónicos solo será posible cuando el marco regulatorio de la Sociedad de la Información sea estable. La estabilidad jurídica en ese sentido es dada por la coordinación de posturas entre las diferentes ramas del poder público y los intereses privados. Lo anterior estaría jalonado por políticas públicas de largo plazo, que en términos institucionales permitan incluir a Colombia en la Sociedad de la Información.

Un ejemplo paradigmático en torno a estas políticas públicas es el impulsado por la Unión Europea. "eEurope" es una iniciativa política dirigida a asegurar que las generaciones venideras de europeos obtengan el máximo provecho de los cambios que está produciendo la Sociedad de la Información[14]. Estos cambios —que, según Devoto (2001: 30), son los más significativos desde la Revolución Industrial— son de enorme trascendencia y son de alcance mundial.

De la misma manera como aquí se concibe para Colombia, Devoto concluye que la buena gestión de esta transformación representa el principal desafío económico y social para la Unión Europea. Por tanto, las repercusiones en el empleo, el crecimiento económico y la productividad a escala internacional penden de la coherencia de un macroproyecto para la Sociedad de la Información.

3. Los delitos informáticos y los delitos cometidos por computador

Con el advenimiento de la Sociedad de la Información, el derecho ha tenido que amoldar sus disposiciones de *ultima ratio*, a efectos de crear sanciones a quienes atenten contra los medios informáticos, o cuando se valen de estos para la comisión de delitos ya descritos en la ley penal[15].

Tímidamente, el legislador colombiano de 2000 introdujo al código penal un tipo que denominó acceso no autorizado a un sistema informático, el cual confería al infractor una multa como sanción. La norma estuvo vigente durante 9 años, sin que hubiese sido estrenada en la práctica judicial, denotando su rampante ineficacia, al no haber contemplado una sanción más drástica para el transgresor. Veremos cómo la denominada Ley de Delitos Informáticos derogó la disposición anti-*hackers*[16], remplazándola por una que incluye pena privativa de la libertad.

---

[14] La iniciativa eEurope se propone acelerar los cambios positivos en la Unión Europea y garantizar que la transformación hacia la Sociedad de la Información adopte la forma de la cohesión, y no de la división, de la sociedad. Trata de integrar, no de fragmentar, por tanto es una oportunidad, no una amenaza. Básicamente, la iniciativa eEurope se propone poner al alcance de todos los europeos los beneficios de la Sociedad de la Información.

[15] Davara Rodríguez (2006: 358-359) define el delito informático como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software".

[16] Al respecto, Davara Rodríguez (2006: 364-365) comenta que el acceso, malintencionado o no, de una persona no autorizada, a los datos que se encuentran en

La conducta de los *hackers* constituye un delito que, según el autor chileno Huerta (2000), consiste en acceder de manera indebida, sin autorización o contra derecho, a un sistema de tratamiento de la información, con el fin de obtener una satisfacción de carácter intelectual —por el desciframiento de los códigos de acceso o *passwords*, no causando daños inmediatos y tangibles en la víctima—, o bien por la mera voluntad de curiosear o divertirse de su autor.

Otros autores, como Reyna (1999), lo han incluido dentro del concepto de intrusismo informático, definiéndolo como el comportamiento consistente en la introducción a sistemas de información o computadoras, infringiendo medidas de seguridad destinadas a proteger los datos contenidos en ella.

Por otro lado, a través de la expedición de la Ley 679 de 2001, el legislador introdujo una nueva modalidad de delito cometido por computador, al disponer que, si los actos sexuales con personas menores de catorce años eran cometidos por medios virtuales, utilizando redes globales de información, el agente incurriría en las penas correspondientes, disminuidas en una tercera parte. Esta disposición ha sido derogada por la Ley 1236 de 2008, la cual, de forma genérica, es decir, sin importar el medio a través de cual se cometa el delito, castiga los actos sexuales con menor de catorce años, aplicando penas privativas de la libertad que van de nueve a trece años.

No es hasta 2009 que el legislador colombiano finalmente hace una adición al catálogo delictual, a través de la expedición de la Ley 1273, conocida como Ley de Delitos Informáticos. Al crear un nuevo bien jurídico tutelado, denominado la información y los datos, la norma consagra una decena de tipos que condenan el actuar de la criminalidad informática.

Interesantemente, la expedición de la norma se dio gracias al impulso académico del juez Alexander Díaz García y del profesor Harvey Rincón Ríos, quienes, fundamentados en el convenio de Budapest de 2001, redactaron el proyecto de ley que se convirtió en la mencionada Ley de Delitos Informáticos.

---

soportes informáticos, se está produciendo, motivado cada vez más por la falta de seguridad de los sistemas y de formación de las personas que en ellos operan, facilitado más, si cabe, por las posibilidades que ofrecen las modernas técnicas de comunicación que permiten el conocimiento, manejo y transferencia de información entre sistemas, con máximas garantías y mínimo riesgo.

Los nuevos tipos introducidos por la norma son el acceso abusivo a un sistema informático[17], la obstaculización ilegítima de sistema informático o red de telecomunicación, la interceptación de datos informáticos, el daño informático[18], el uso de software malicioso[19], la violación de datos personales[20], y la suplantación de sitios web para capturar datos personales. Estos tipos penales fueron creados como delitos que atentan contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

Las conductas anteriores concluyen en agravación punitiva cuando:

1. Recaen sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Son cometidas por servidor público en ejercicio de sus funciones.
3. Se realizan aprovechando la confianza depositada por el poseedor de la información, o por quien tuviere un vínculo contractual con este.
4. Revelan el contenido de la información en perjuicio de otro.
5. Se obtiene provecho para sí o para un tercero.

---

[17] El castigo que ofrece esta norma, que va desde los 48 hasta los 96 meses de prisión, adicionado con multa, está dado para el acceso doloso, como por ejemplo, obteniendo una lista de clientes o de resultados de un competidor, o conociendo la información que un tercero procesa o envía por correo electrónico, o la información que simplemente almacena, mediante el acceso a sus computadores o archivos, ya sea a distancia, ya sea por medio de la introducción de programas en el equipo del afectado, que realicen una copia de otros programas, o de resultados de procesos o de investigación.

[18] De la redacción de esta norma vale la pena destacar dos aspectos: (i) de una parte, la influencia del principio de la neutralidad tecnológica, propio del derecho del comercio electrónico, al incluir cualquier soporte informático (hardware) y cualquier modalidad lógica (software) como objetos de la conducta punible, y (ii), de otra parte, la referencia clara al dato informático, dándole el protagonismo que se merece, como noticia cierta sobre un hecho que puede incluir un alto contenido económico y patrimonial.

[19] Este es el caso de los conocidos virus informáticos, que, según Davara Rodríguez (2006: 365-366), "consisten en rutinas, instrucciones o partes de programas que se introducen a través de un soporte físico que los contiene, o través de la red de comunicaciones, actuando en el momento, o con efecto retardado, y destruyendo datos, información o programas y, en ocasiones, toda la información contenida en el ordenador."

[20] La intimidad y su entorno, así como la defensa de la honra y el buen nombre, se encuentran protegidas constitucionalmente por el artículo 15 superior y representan una referencia directa concreta y concreta a la informática. En el caso de la violación de datos personales, se pretende proteger, por normas de *ultima ratio*, la intimidad como derecho fundamental.

6. Tiene fines terroristas o que generen riesgos para la seguridad o defensa nacional.
7. Utilicen como instrumento a un tercero de buena fe.

Finalmente, al mejor estilo de la película *Hackers* (Softley, 1995), la norma dispone, para el responsable de la administración, manejo o control de dicha información, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales, hasta por 3 años.

Respecto de los delitos cometidos por computador, considerados por la ley como atentados informáticos, quedaron estipulados el hurto por medios informáticos y semejantes y la transferencia no consentida de activos. Resta conocer cuál va a ser la eficacia de la norma, teniendo en cuenta que en la práctica judicial colombiana todavía no se permean, ni se sienten culturalmente como una verdadera felonía, las conductas delictivas propias de la Sociedad de la Información.

En consecuencia, por su novedad la llamada Ley de Delitos Informáticos será susceptible de múltiples interpretaciones y de diversas opiniones. Sin embargo, lo que nadie pone en duda es la implicación que la informática, y las TIC en general, tienen en la realización de muchas conductas criminales. No es posible ignorar las múltiples conductas dolosas o imprudentes, con graves perjuicios para terceros, que se están constantemente realizando por medios electrónicos y que, bajo ninguna circunstancia, pueden quedar exentas de sanción penal.

4. A manera de conclusión

En Colombia existen diversos niveles de regulación, interdependientes e interrelacionados, con relación a la Sociedad de la Información. Un primer nivel es el de la regulación técnica, fijado por estándares internacionales. Un segundo nivel es el de la regulación jurídica, que asume y da fuerza vinculante a dichos estándares técnicos. Respecto de los fenómenos derivados del comercio electrónico, la Ley 527 de 1999, y sus decretos reglamentarios, han regulado la existencia en Colombia de una presunción legal de validez sobre las firmas digitales, cuando están avaladas por certificados expedidos por entidades de certificación digital, que, a juicio de la Superintendencia de Industria y Comercio, cumplan con los parámetros técnicos indicados en las normas.

Colombia asume, entonces, un esquema donde la intervención del Estado se hace presente para garantizar la confianza de quienes realizan transacciones por medios electrónicos. Sin embargo, la eficacia de las disposiciones normativas es cuestionada, toda vez que no existe el convencimiento cultural de la eficiencia que la implementación de TIC trae a las actividades comerciales, o al menos las personas no están generalmente dispuestas a asumir los riesgos propios de las operaciones electrónicas.

La expedición de la Ley 1273 de 2009, conocida como Ley de Delitos Informáticos, se proyecta como una norma disuasoria contra la criminalidad electrónica, redundando en mayor confianza del público en el uso de los medios electrónicos. Solo con la cabal aplicación de las penas consagradas en la norma se sentarán precedentes que no permitan que Colombia se convierta en un paraíso de la delincuencia informática, como lo ha sido respecto de otras formas de criminalidad.

A través de la planeación a largo plazo de sus diferentes frentes de gestión, el Estado debe entender el uso de las TIC como pilar fundamental de los medios de producción, respaldado en normas que no vayan al vaivén de las recomendaciones de turno de organismos internacionales, sin que por ello se pueda entender a Colombia como un país ajeno al proceso globalizador.

Las leyes 527 de 1999 y 1273 de 2009 constituyen los dos cuerpos normativos más importantes de temas de la Sociedad de la Información en Colombia. Se espera que la investigación de la cual surgió este artículo arroje uno nuevo en torno a otros dos fenómenos cruciales de esta temática: (i) la protección de los datos personales y (ii) el gobierno electrónico.

Bibliografía

Aboso, Gustavo Eduardo y María Florencia Zapata. *Cibercriminalidad y derecho penal.* Montevideo: Editorial B de F (2006).

Camacho Clavijo, Sandra. *Partes intervinientes, formación y prueba del contrato electrónico.* Madrid: Editorial Reus (2005).

Carbajo Cascón, Fernando. *Publicaciones electrónicas y propiedad intelectual.* Madrid: Editorial Colex (2002).

CNUDMI Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. *Ley modelo de la CNUDMI de comercio electrónico con la guía para su incorporación al derecho interno, versión 1998.* Nueva York: Naciones Unidas (1999).

CNUDMI Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. *Ley modelo de la CNUDMI de firmas electrónicas con la guía para su incorporación al derecho interno 2001.* Nueva York: Naciones Unidas (2002).

CNUDMI Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. *Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales.* Nueva York: Naciones Unidas (2007).

CNUDMI Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firmas electrónicas.* Viena: Naciones Unidas (2009).

Couto Calviño, Roberto. *Servicios de certificación de firma electrónica y libre competencia.* Granada: Editorial Comares (2008).

Cubillos Velandia, Ramiro y Erick Rincón Cárdenas. *Introducción al comercio electrónico.* Bogotá: Ediciones Jurídicas Gustavo Ibáñez (2002).

Davara Rodríguez, Miguel Ángel. *Manual de derecho informático.* Madrid: Editorial Aranzadi (2006).

Devoto, Mauricio. *Comercio electrónico y firma digital.* Buenos Aires: La Ley (2001).

Flores Doña, María de la Sierra. *Impacto del comercio electrónico en el derecho de la contratación.* Madrid: Editoriales de Derecho Reunidas (2002).

Garrote Fernández-Díez, Ignacio. *El derecho de autor en internet.* Granada: Editorial Comares (2003).

Huerta Miranda, Marcelo. "Figuras delictivo-informáticos tipificadas en Chile." *Revista de Derecho Informático*. Alfa-Redi (2000).

Iriarte Ahon, Erick. *Estado situacional y perspectivas del derecho informático en América Latina y el Caribe.* Santiago de Chile: Naciones Unidas (2005).

Peña Valenzuela, Daniel. "El contrato electrónico y los medios probatorios." En: *El contrato por medios electrónicos.* Bogotá: Universidad Externado de Colombia (2003).

Reyna Alfaro, Luis Miguel. "Fundamentos para la protección penal de la información (almacenada, tratada y transmitida mediante los sistemas de procesamiento de datos) como valor económico de empresa." *Revista de Derecho Informático*. Alfa-Redi (1999).

Richards, Jason R. "The Utah Digital Signature Act as 'Model' Legislation: A Critical Analysis." *The John Marshall Journal of Computer & Information Law*: *An International Law Journal on Information Technology* 17.3 (1999), pp. 873-907.

Rincón Cárdenas, Erick. *Contratación electrónica.* Bogotá: Centro Editorial Universidad del Rosario (2006a).

Rincón Cárdenas, Erick. *Manual de derecho de comercio electrónico y de Internet.* Bogotá: Centro Editorial Universidad del Rosario (2006b).

Softley, Iain (director). *Hackers* (Producción cinematográfica estadounidense). Metro-Goldwyn-Mayer (1995).

Zapata Arbeláez, Adriana. "Ley aplicable y jurisdicción competente en conflictos surgidos en la contratación comercial electrónica." En: *Derecho del comercio electrónico.* Bogotá: Dike (2002).