EL PAPEL DE LAS ENTIDADES DE CERTIFICACIÓN Y LA SEGURIDAD DE LA INFORMACIÓN Y LOS DERECHOS PERSONALES EN EL COMERCIO ELECTRÓNICO[1]

Dr. MARCOS QUIROZ GUTIÉRREZ[2]

Fecha de recepción: 24 de abril de 2009 - Fecha de aceptación: 1º de julio de 2009

Resumen

Los adelantos tecnológicos han permitido el desarrollo a pasos agigantados del comercio electrónico. No obstante, la contratación por medios digitales se encuentra rodeada por un entorno desalentador: la inseguridad de la información personal. En efecto, hoy en día es común la recolección ilimitada de datos personales, los cuales son un activo empresarial de suma importancia que puede ser explotado de diversas maneras en la sociedad de la información.

Este artículo aborda primordialmente dos temas: por un lado, diversos aspectos relacionados con la firma digital, la firma electrónica y las entidades certificadoras; y por el otro, la inseguridad de la información de las personas que participan en el comercio electrónico. Además, es planteado un tercer tópico, el cual tiene que ver con la inaplicabilidad del concepto tradicional del abuso de información privilegiada producida por la sociedad de la información.

Palabras Clave: *Comercio electrónico, entidad de certificación, firma digital, firma electrónica, información personal.*

Abstract

Technological advances have allowed the fast development of electronic commerce. However, digital hiring is surrounded for a disappointing entorn: the insecurity of personal information. Nowadays, is common the unlimited colection of personal data, which are a vital business asset that can be exploited in different ways in the information society.

This article studies two issues: firstly, various aspects related to digital signature, electronic signature and certification authorities, secondly, the uncertainty of the information of people involved in electronic commerce. In addition, it has a third topic, which is the inapplicability of the traditional concept of abuse of privileged information produced by the information society.

Key Words: *Electronic commerce, certification authority, digital signature, electronic signature, personal information.*

INTRODUCCIÓN

[1] Ponencia ganadora del segundo lugar en el IX Concurso Internacional de Estudiantes de Derecho Nivel Pregrado en el marco del XXIX Congreso Colombiano de Derecho Procesal que tuvo lugar en Medellín (Colombia) los días 3, 4 y 5 de septiembre de 2008.

[2] Fueron también integrantes de este Grupo de Investigación los estudiantes: SUHAD MAY ABDALA MANOTAS, MAURICIO ANDRÉS MORALES HURTADO, LYANA ISABELLA DE LUCA RUIZ, PAULA DE GAMBOA, FABIO ANDRÉS RESTREPO BERNAL, ANDRÉS FELIPE ALONSO JIMÉNEZ, ORLANDO ENRIQUE SANTAMARÍA ECHEVERRÍA, CAROLINA ANDREA SIERRA CASTILLO.

Desde siempre la desconfianza ha sido un sentimiento persistente en la humanidad. Esta es la causa para que las personas implementen, experimenten y mejoren constantemente mecanismos y medios que doten de seguridad las relaciones jurídicas que establezcan. Tal objetivo ha sido logrado por antonomasia con el documento, el cual, con toda la evolución que ha sufrido, es una excelente forma para establecer y dejar constancia de las relaciones (negocios y contratos) sobre las que se hace referencia, convirtiéndose en un instrumento de comunicación y expresión de gran importancia para el tracto jurídico. Para ilustrar el asunto, piense el lector en una contratación llevada a cabo por dos personas ubicadas en territorios geográficos distintos, pero unidas por el intercambio de "mensajes de datos" enviados y recibidos por medio de internet.

El paso del tiempo también ha dejado sus marcas en la visión tradicional de firma. Al lado de la manuscrita y gracias a la introducción progresiva de la tecnología en la vida de las personas y a su reconocimiento en el mundo jurídico, aparecen las firmas electrónica y digital, de las que hoy se habla con soltura, sin extrañezas, y que, sin saberlo, ha sido utilizada por la mayoría. En efecto, hay una firma electrónica, como se verá más adelante, en un *e-mail* enviado y recibido por personas identificadas o identificables.

Pues bien, mensajes de datos y firmas electrónicas y digitales son elementos que mejoran el intercambio de información, la adquisición, oferta y promoción de bienes y servicios deseados para satisfacer las necesidades humanas. No obstante, la contratación telemática como realidad innegable y benéfica para las personas, se desarrolla alrededor de la incertidumbre y la inseguridad. En efecto, la implementación y el uso de las nuevas tecnologías han aumentado los riesgos para los derechos y la información de las personas, quienes con el pasar del tiempo van dejando una serie de datos que pueden ser recopilados y explotados sin ninguna limitación[3]. Sin duda, como dicen algunos, "la aldea global es esta desnudez de la intimidad"[4].

La defensa de estos valores en juego debe ser destinataria de todos los esfuerzos que puedan empeñarse en ello, porque el centro del tema se sitúa en la idea de que preservar los datos de las personas es lo mismo que salvaguardarlas a ellas, "o aún, proteger los datos es lo mismo que proteger a la persona, como proteger su casa: porque la casa y los datos son el **habitáculo del yo**"[5]. En otras palabras, la información de los humanos goza de una relevancia manifiesta porque es el contenido de su personalidad.

El problema radica en que la inseguridad y la desconfianza generalizadas no producen efectos aislados que resulten irrelevantes para la comunidad en general, al contrario, esa desazón percibida por quienes participan en el comercio telemático dificulta la aplicación real de los sustentos esenciales del *e-commerce* como son la equivalencia funcional y la eficacia probatoria de la firma y el documento electrónicos.

---

[3] Remolina Angarita, Nelson. "Data protection: panorama nacional e internacional". *Internet, Comercio Electrónico y Telecomunicaciones.* Primera Edición. Bogotá. Universidad de los Andes, Legis Editores. 2002. p. 100.

[4] Díaz, Francisco Eugenio . "La protección de la intimidad y el uso de internet", *Informática y Derecho*, Nos. 30-32 y 31, 1999, Mérida, Centro Regional de Extremadura, p. 152.

[5] Ibídem.

En la superación de estos escollos, las Entidades de Certificación[6] desempeñan un rol importante. Estas, en conjunto con otros elementos, promueven la seguridad jurídica del comercio electrónico, aseguran la autenticidad, integridad y no repudiación de los mensajes de datos, por lo que deben ser más asequibles para las personas del común.

Con el objetivo de abordar y sentar posición sobre estos temas, la presente ponencia se divide en tres partes: primero, se expondrá sobre la Infraestructura de Clave Pública –o PKI de acuerdo a su denominación en inglés– y acerca de todo lo relacionado con las firmas digitales de criptografía asimétrica y las firmas electrónicas, (primera parte); luego, se escudriñarán los riesgos y formas de protección de los derechos y la información de las personas involucradas de alguna manera en la contratación telemática (segunda parte); y, por último, se reflexionará en torno a los cambios profundos que ha traído la sociedad del comercio electrónico en la noción tradicional del abuso de información privilegiada (tercera parte).

Este esquema de 3 capítulos será aterrizado con algunas conclusiones en las que se señalarán algunas propuestas y se hará énfasis sobre temas relevantes.

Se procede, entonces, a desarrollar el plan por el que se ha optado.

1. LA INFRAESTRUCTURA DE CLAVE PÚBLICA (O PUBLIC KEY INFRASTRUCTURE) Y LAS ENTIDADES DE CERTIFICACIÓN

1.1 PKI

La Infraestructura de Clave Pública es un sistema complejo que brinda seguridad a la hora de intercambiar información en operaciones electrónicas. Concretamente, es un conjunto de métodos, tecnologías y técnicas que garantizan la seguridad en el mundo electrónico, con las Entidades de Certificación y las claves asimétricas como componentes esenciales[7].

La base de una PKI bien construida está determinada por la confidencialidad de la información, su integridad, disponibilidad, autenticación, autorización o control de acceso, y no repudiación de los mensajes de datos.

Las Autoridades de Certificación son el corazón del sistema PKI. Ellas hacen posible su aplicación y, por tanto, garantizan la seguridad y la autenticidad de la información enviada[8].

---

[6] A nivel internacional han sido conocidas con las voces sinónimas de Terceros de Confianza (TC), Trusted Third Party (TTP), Certification Authority (CA) o Autoridades de Certificación (AC).

[7] El sistema de criptografía asimétrica se basa en algoritmos, a través de dos claves que pertenecen a la misma persona, una pública y una privada. El remitente cifra el mensaje con la clave pública del destinatario, y este lo descifra con su clave privada. Este sistema facilita el intercambio de información ya que las partes no deben ponerse de acuerdo en una clave para cifrar y descifrar.

[8] Zubite Uribe, Hermann. "Los Mensajes de Datos y las Entidades de Certificación". *Internet, Comercio Electrónico y Telecomunicaciones*. Primera Edición. Bogotá. Universidad de los Andes, Legis Editores S.A. 2002. p 64.

El éxito de la seguridad que brinda la tecnología PKI está en el manejo que se le dé a las claves, especialmente a la privada, por lo tanto el soporte que la contenga debe ser de avances tecnológicos que le permitan al usuario estar tranquilo y darle un manejo adecuado.

Ese manejo de claves se desarrolla parcialmente por medio de los repositorios, que son un depósito de la información relacionada con los certificados, como sucede con las listas de la revocatoria de estos.

1.2 Aspectos Generales de las Entidades de Certificación

De acuerdo con la Ley 527 de 1999 o de Comercio Electrónico, las Entidades de Certificación desempeñan un rol relevante en torno a la autenticidad e integridad de los documentos electrónicos, logrando la seguridad jurídica y, a su vez, la eficacia probatoria de este equivalente funcional del documento tangible. Son definidas como aquellas autorizadas para certificar firmas digitales, ofrecer o facilitar los servicios de registro y estampado cronológico de mensajes de datos, entre otras funciones relativas a las comunicaciones electrónicas[9].

El papel primordial de las TTP –quienes son el centro del sistema PKI– consiste en vincular una clave pública con la persona que ha firmado digitalmente un mensaje de datos, lo que logra aminorar los riesgos y contribuir en la producción de la confianza y seguridad deseadas dentro del comercio electrónico.

Pueden ser autorizados por la Superintendencia de Industria y Comercio para constituirse como EC los notarios, los cónsules, las Cámaras de Comercio y las personas jurídicas públicas o privadas, colombianas o extranjeras, que cuenten con la capacidad económica y financiera suficientes y los recursos técnicos necesarios para prestar eficientemente sus servicios[10].

En Colombia puede haberlas de dos tipos: Abiertas y Cerradas[11]. Las primeras ofrecen certificados que no se limitan al intercambio de mensajes

---

[9] Colombia, Congreso de la República, Ley 527 de 18 de agosto de 1999, artículo 2 Literal d: "Entidad de Certificación. Es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y 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".

[10] Colombia, Congreso de la República, Ley 527 de 18 de agosto de 1999, Artículo 29: CARACTERÍSTICAS Y REQUERIMIENTOS DE LAS ENTIDADES DE CERTIFICACIÓN. Podrán ser entidades de certificación, las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero y las cámaras de comercio, que previa solicitud sean autorizadas por la Superintendencia de Industria y Comercio y que cumplan con los requerimientos establecidos por el Gobierno Nacional, con base en las siguientes condiciones: "a) Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como entidad de certificación; "b) Contar con la capacidad y elementos técnicos necesarios para la generación de firmas digitales, la emisión de certificados sobre la autenticidad de las mismas y la conservación de mensajes de datos en los términos establecidos en esta ley". Parágrafo 1 del artículo1 de la Ley 588 de 2000: "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".

[11] En Colombia el **Instituto Colombiano de Codificación y Automatización Comercial, el Banco de la República, la UAE Dirección de Impuestos y Aduanas Nacionales – DIAN y**

entre la entidad y el suscriptor o, de haber esta limitación, cobran por la prestación de sus servicios, mientras que las segundas no perciben remuneración alguna y su actividad se restringe al intercambio de mensajes de datos con el usuario[12].

Como una forma de garantizar la confianza en sus actividades, están inhabilitados para ser representantes legales o administradores de estas entidades por el mismo tiempo que la ley penal o administrativa señale, aquellas personas condenadas a penas privativas de la libertad por delitos diferentes a los políticos o culposos o que hayan sido suspendidas o excluidas del ejercicio de su profesión por falta grave[13].

El primer inconveniente sorteado por las AC fue la acción de inconstitucionalidad en contra de la Ley de Comercio Electrónico, debido a que los demandantes consideraron que se había eliminado el monopolio de la fe pública que tienen los notarios[14]. Este problema jurídico fue resuelto con la exequibilidad de las normas cuestionadas de la Ley 527 de 1999 debido a que la Corte Constitucional consideró que la expedición de Certificados Digitales no puede enmarcarse dentro de la fe pública, ni es un servicio público que puedan prestar solamente los notarios. Esta decisión sentó la posición de que en la práctica las Entidades de Certificación (tanto abiertas como cerradas) no cumplen funciones notariales propiamente dichas, sino que en realidad sus actividades se aproximan más a las de los registradores públicos.

Por otro lado, las Entidades de Certificación tienen una posición de garante frente a la información que manejan y que no es publicada en los certificados. Por ello, deben garantizar su confidencialidad y seguridad en su manejo, máxime cuando podría haber casos en los que se considere como información privilegiada.

1.3 Certicámara S. A.: la única entidad de Certificación Abierta que existe en Colombia

Por medio de las resoluciones 1007 de 2002 y 9887 de 2007, la Superintendencia de Industria y Comercio autorizó a la **Sociedad Cameral de**

Ecopetrol S.A. son las Entidades de Certificación Cerradas autorizadas por la Superintendencia de Industria y Comercio. Como en su momento se señalará, Certicámara S.A. es la única abierta existente.

[12] Colombia, Presidencia de la República, Ministerio de Desarrollo Económico, Ministerio de Comunicaciones y Ministerio de Comercio Exterior, Decreto 1747 de 11 de septiembre de 2000, numerales 8 y 9 del artículo 1: "8. Entidad de certificación cerrada: entidad que ofrece servicios propios de las entidades de certificación sólo para el intercambio de mensajes entre la entidad y el suscriptor, sin exigir remuneración por ello. "9. Entidad de certificación abierta: la que ofrece servicios propios de las entidades de certificación, tales que: a) Su uso no se limita al intercambio de mensajes entre la entidad y el suscriptor, o b) Recibe remuneración por éstos".

[13] Colombia, Congreso de la República, Ley 527 de 18 de agosto de 1999, Literal c del artículo 29: "c) Los representantes legales y administradores no podrán ser personas que hayan sido condenadas a pena privativa de la libertad, excepto por delitos políticos o culposos; o que hayan sido suspendidas en el ejercicio de su profesión por falta grave contra la ética o hayan sido excluidas de aquélla. Esta inhabilidad estará vigente por el mismo período que la ley penal o administrativa señale para el efecto".

[14] Colombia, Corte Constitucional, Sala Plena, Sentencia de constitucionalidad C-662 de 2000. 8 de junio de 2000. Magistrado Ponente: Fabio Morón Díaz. Expediente D-2693

Certificación Digital, Certicámara S.A., como la primera y única Entidad de Certificación Abierta en Colombia.

Esta se atribuye como "propósito fundamental proporcionar las herramientas necesarias para que los empresarios y demás usuarios de Internet del país puedan realizar Negocios Electrónicos con Seguridad Jurídica"[15].

Certicámara ofrece los servicios de expedición de Certificados Digitales de firmas electrónicas con la tecnología de criptografía asimétrica, el archivo y estampado cronológico de mensajes de datos, el aseguramiento de sitios Web y de redes privadas virtuales, la implementación de correo electrónico seguro empresarial de mensajes de datos, entre otros.

Su actividad monopolística ha producido un elevado costo de los certificados digitales (algunos oscilan entre $540.000 y $1.500.000), debido a que la remuneración de sus servicios es fijada libremente por ella[16]. Esos elevados montos podrían ser disminuidos, según funcionarios de Certicámara, con la obligatoriedad de los certificados digitales en las transacciones del Comercio Electrónico. A lo mejor, la baja de estos precios podría lograrse con el surgimiento de otra TTP abierta, donde el valor lo determine el mercado.

1.4 Especial referencia al Banco de la República como Entidad de Certificación Cerrada

El Banco de la República de Colombia se destaca dentro de las TTP cerradas que han recibido el aval para realizar su función. Esta es una entidad de derecho público, de rango constitucional, domiciliada en Bogotá y encargada de ejercer las funciones de Banca Central. Como persona jurídica de derecho público y de origen nacional, fue autorizada por la Superintendencia de Industria y Comercio mediante la Resolución 6372 del 28 de febrero de 2000, por lo que ha adquirido y montado una infraestructura de llaves públicas (PKI).

El objeto de la infraestructura instalada por el Banco apunta exclusivamente a establecer la forma de incrementar los niveles de seguridad en los servicios electrónicos ofrecidos, de conformidad con la legislación vigente, como son la guarda y custodia de información de especial connotación confiada por los diferentes bancos del país.

Todo esto le permite a esta TTP cerrada estar a la vanguardia en el desarrollo de sus actividades, de donde surgen beneficios para entidades de gran calado en el desarrollo económico del país como las que conforman el sector financiero y bancario.

1.5 Los Certificados de Firmas Digitales

El certificado digital es un documento electrónico firmado digitalmente y expedido por una entidad de certificación una vez ha confirmado la identidad

---

[15] Cfr. http://www.certicamara.com

[16] Colombia, Congreso de la República, Ley 527 de 18 de agosto de 1999, artículo 31: "REMUNERACIÓN POR LA PRESTACIÓN DE SERVICIOS. La remuneración por los servicios de las entidades de certificación serán establecidos libremente por éstas".

del titular de las claves pública y privada, con el fin de asegurar la autenticidad, confidencialidad y no repudio de otro mensaje de datos.

Los certificados tienen un término de vigencia que puede ser conocido a través de los repositorios en los que se publican. Esa vigencia se encuentra determinada por el grado de seguridad ofrecido por el par de claves, teniendo en la cuenta la fecha de su creación y la probabilidad de que los recursos tecnológicos existentes permitan derivar la llave privada a través de la pública, caso en el que, de acuerdo al artículo 16 del Decreto 1747 de 2000, la firma deja de ser única[17].

Una vez se venza o sea revocado el certificado, esto se hará conocer a través de los repositorios[18]. La importancia del punto radica en que las firmas realizadas antes de la revocatoria[19] por pérdida de la clave privada o del vencimiento siguen siendo válidas, siempre que se acredite el momento en que fue adherida a un mensaje de datos[20].

El certificado emitido por una entidad abierta logra que la firma digital que respalda sea equivalente a la manuscrita cuando se verifiquen estos supuestos: (I) Permite la verificación de que se empleó la clave pública; y (II) La firma fue realizada durante el tiempo de validez del certificado y según los términos de la Declaración de Prácticas de Certificación[21]. Empero, aquellos

---

[17] Zubieta Uribe, Hermann. "Los Mensajes de Datos y las Entidades de Certificación". *Internet, Comercio Electrónico y Telecomunicaciones.* Primera Edición. Bogotá. Universidad de los Andes, Legis Editores S.A. 2002, p. 61. Este autor hace una detenida explicación de la probabilidad para determinar las claves.

[18] Henao Restrepo, Dario. "Ley de Comercio Electrónico en Colombia". *Nuevos Retos del Derecho Comercial*. Primera Edición. Bogotá. Bibiliteca Jurídica Diké. 2000, p. 173.

[19] Colombia, Congreso de la República, Ley 527 de 18 de agosto de 1999, artículo 37: "REVOCACIÓN DE CERTIFICADOS. El suscriptor de una firma digital certificada, podrá solicitar a la entidad de certificación que expidió un certificado, la revocación del mismo. En todo caso, estará obligado a solicitar la revocación en los siguientes eventos: "1. Por pérdida de la clave privada. "2. La clave privada ha sido expuesta o corre peligro de que se le dé un uso indebido. "Si el suscriptor no solicita la revocación del certificado en el evento de presentarse las anteriores situaciones, será responsable por las pérdidas o perjuicios en los cuales incurran terceros de buena fe exenta de culpa que confiaron en el contenido del certificado. "Una entidad de certificación revocará un certificado emitido por las siguientes razones: "1. A petición del suscriptor o un tercero en su nombre y representación. "2. Por muerte del suscriptor. "3. Por liquidación del suscriptor en el caso de las personas jurídicas. "4. Por la confirmación de que alguna información o hecho contenido en el certificado es falso. "5. La clave privada de la entidad de certificación o su sistema de seguridad ha sido comprometido de manera material que afecte la confiabilidad del certificado. "6. Por el cese de actividades de la entidad de certificación, y "7. Por orden judicial o de entidad administrativa competente".

[20] Hermann Zubieta Uribe. "El tiempo en los mensajes de datos". *El Contrato por Medios Electrónicos*, Primera edición, Bogotá, Universidad Externado de Colombia, 2003, p. 140.

[21] Colombia, Presidencia de la República, Ministerio de Desarrollo Económico, Ministerio de Comunicaciones y Ministerio de Comercio Exterior, Decreto 1747 de 11 de septiembre de 2000, artículo 15: "USO DEL CERTIFICADO DIGITAL. Cuando quiera que un suscriptor firme digitalmente un mensaje de datos con su clave privada, y la respalde mediante un certificado digital, se darán por satisfechos los atributos exigidos para una firma digital en el parágrafo del artículo 28 de la Ley 527 de 1999, sí: "1. El certificado fue emitido por una entidad de certificación abierta autorizada para ello por la Superintendencia de Industria y Comercio. "2. Dicha firma se puede verificar con la clave pública que se encuentra en el certificado con relación a firmas digitales, emitido por la entidad de certificación. "3. La firma fue emitida dentro del tiempo de validez del certificado, sin que éste haya sido revocado. "4. El mensaje de datos

que emiten las TTP cerradas deben contener la advertencia expresa de que no puede verificarse la firma con la clave pública del suscritor y que la firma no fue realizada en el tiempo de validez del certificado, lo que no solamente es falso y equivocado sino que ha dejado en el ambiente la idea de que únicamente los certificados de Certicámara dotan de valor probatorio a las firmas digitales que avalan[22].

Sin dudas, una expresión como la anterior no puede ser prohijada bajo ninguna circunstancia, debido a que desconoce que todas las Autoridades de Certificación (tanto las abiertas como las cerradas) emplean la misma tecnología para producir una firma digital, esto es, la infraestructura de clave pública o PKI. Por ello, se impone la necesidad de sostener que todas las firmas digitales acreditadas por cualquier EC cerrada dotan de autenticidad a los documentos electrónicos en los que se encuentran, y por lo tanto, son totalmente equivalentes a las firmas manuscritas en lo que tiene que ver con los efectos jurídicos señalados por la ley.

1.6 Firma digital vs. Firma Electrónica

Infortunadamente, la preeminencia que las normas colombianas le dan a la firma digital parece dar cabida a especulaciones que niegan la validez y eficacia probatoria que tendría la firma electrónica[23].

Para despejar este equívoco es necesario hacer claridad sobre los conceptos. Firma electrónica es el género y se define como un "método adecuado" que permite identificar al iniciador de un mensaje de datos, de acuerdo con las condiciones particulares de éste. Por el contrario, la firma digital es la especie y consiste en un conjunto de datos incluidos en un mensaje de datos y obtenidos por conducto de la criptografía asimétrica, esto es, únicamente a través de las entidades de certificación[24]. Es decir, hay dos posibilidades para lograr la autenticidad de un documento electrónico. La primera, consiste en suscribirse a una entidad de certificación y firmarlo digitalmente; la otra será utilizar un "método adecuado" por medio del que se pueda identificar a quien ha enviado un mensaje de datos.

Entre estas opciones, la "neutralidad tecnológica" y el enfoque de los "equivalentes funcionales"[25] son nociones que deben presidir la adopción de las

---

firmado se encuentra dentro de los usos aceptados en la DPC, de acuerdo al tipo de certificado".

[22] Colombia, Presidencia de la República, Ministerio de Desarrollo Económico, Ministerio de Comunicaciones y Ministerio de Comercio Exterior, Decreto 1747 de 11 de septiembre de 2000, artículo 4: "Información en certificados. Los certificados emitidos por las entidades de certificación cerradas deberán indicar expresamente que sólo podrán ser usados entre la entidad emisora y el suscriptor. Las entidades deberán informar al suscriptor de manera clara y expresa, previa expedición de los certificados, que éstos no cumplen los requisitos del artículo 15 del presente decreto".

[23] Pérez Useche, Marco. "El Tratamiento de la Firma Electrónica en Colombia y en el Derecho Uniforme". *Derecho del Comercio Electrónico*. Primera Edición. Bogotá. 2002. Biblioteca Jurídica Diké, p. 94.

[24] Recalde Castelles, Andrés. "Comercio y Contratación Electrónica". *Informática y Derecho.* Nos. 30-32 y 31. 1999. Mérida. Centro Regional de Extremadura, p. 75.

[25] Zubieta Uribe, Herman. "Los Mensajes de Datos y las Entidades de Certificación". Ob.Cit., p. 50.

nuevas tecnologías en el mundo jurídico. En consecuencia, la aplicación judicial en los diferentes países debe ser "imparcial" entre las diversas posibilidades tecnológicas a implementar y no negarle valor a la documentación electrónica ni a las diferentes formas que sirven para conseguir autenticidad de un documento electrónico, las cuales tendrán los mismos efectos que sus símiles tradicionales. Dicho de otra manera, no debe haber preferencias –en cuanto a los efectos otorgados– entre un método de firma, sea este en su modalidad digital o electrónica, como se explicó.

Ahondando sobre el tema, es relevante recordar que la Ley Modelo de Firmas Electrónicas de la CNUDMI, la cual fue incorporada al ordenamiento jurídico colombiano, adopta la neutralidad tecnológica como centro de las normas que propone, al consagrar que ninguna disposición podrá privar, restringir o excluir de efectos jurídicos a cualquier método para crear firmas electrónicas que sea fiable y apropiado de acuerdo al entorno del mensaje de datos[26]. Por lo anterior, el articulado de la ley de Comercio Electrónico colombiana y su decreto reglamentario son imparciales entre las opciones tecnológicas, por tal motivo ordenan que la validez jurídica sea predicada respecto de cualquier método adecuado que permita identificar al autor de un documento electrónico o al iniciador de un mensaje de datos, como lo permitiría, por ejemplo, un *e-mail* enviado desde una cuenta de correo electrónico personal de una persona identificada o identificable.

La conclusión no podría ser otra: Toda forma apropiada para identificar al iniciador de un mensaje de datos es una firma electrónica y, por ende, equivalente a la firma manuscrita, como sucede también con las firmas digitales[27].

1.7 La Responsabilidad Civil de la Entidades de Certificación

Con el fin de despejar equívocos, hay que señalar que las actividades desarrolladas por las Entidades de Certificación son de estricto índole mercantil y no corresponden a la prestación de un servicio o actividad públicos, lo que elimina de plano la posibilidad de que se alegue responsabilidad de la Nación por daño antijurídico, de acuerdo al artículo 90 de la Constitución Política[28].

Teniendo claro lo anterior, el punto de partida se ubica en el artículo 2341[29] del Código Civil, donde se consagra el principio general de que todo aquel que produce un daño debe resarcirlo. Esta regla amplia es aterrizada y reiterada por el artículo 18 del Decreto 1747 de 2000 que ordena a las Entidades de

---

[26] Comisión de las Naciones Unida para el derecho mercantil internacional. Ley Modelo de la CNUDMI sobre Firmas Electrónicas de 5 de julio de 2001, artículos 3 y 6.

[27] Cfr. Colombia, Congreso de la República, Ley 527 de 18 de agosto de 1999, artículo 7. Cfr. también Peña Valenzuela, Daniel. "El Contrato Electrónico y los Medios Probatorios". *El Contrato por Medios Electrónicos.* Primera Edición. Bogotá. Universidad Externado de Colombia. 2003, pp. 194-198.

[28] Colombia. Corte Constitucional. Sentencia C-662 de 8 de junio de 2000. Magistrado Ponente: Fabio Morón Díaz. Expediente D-2693.

[29] Colombia, Congreso de la República, Código Civil sancionado el 26 de mayo de 1873, artículo 2341: "El que ha cometido un delito o culpa, que ha inferido daño a otro, es obligado a la indemnización, sin perjuicio de la pena principal que la ley imponga por la culpa o el delito cometido".

Certificación responder por todos los perjuicios que llegaren a causarle a los suscriptores y a quienes confíen en sus certificados.

Como puede observarse, son dos la relaciones jurídicas en las que participa la TTP como eventual productora de un perjuicio. En efecto, con el suscriptor la ata un contrato, mientras que frente a un tercero su relación es únicamente extracontractual, distinción que determina el régimen aplicable al resarcimiento, así: en la responsabilidad contractual la norma aplicable es el artículo 1604[30] del Código Civil que consagra en su segundo inciso el régimen de culpa presunta, empero, para la responsabilidad extracontractual será deber del litigante demostrar la culpa en la que incurrió la Entidad Certificadora. En otras palabras, si es deseo de la EC relevarse de responsabilidad contractual deberá demostrar que ejerció la diligencia y el cuidado debidos o la existencia de una causa extraña –como caso fortuito o fuerza mayor– mientras que en la responsabilidad aquiliana le corresponderá a su contraparte probar la culpa, negligencia o impericia[31].

Por otro lado, aunque se ha ventilado mucho la discusión acerca de la peligrosidad de las actividades realizadas por las TTP, es válido afirmar que en abstracto éstas no son riesgosas y por ende no hay, en principio, responsabilidad objetiva de su parte. No obstante, de llegar a optarse por la vía contraria, la entidad será irresponsable ante el daño sólo cuando logre romper el nexo de causalidad al demostrar la existencia de un hecho imprevisible, irresistible y jurídicamente ajeno a su actividad[32].

Vale señalar que las premisas generales de responsabilidad contractual pueden ser alteradas por las partes en las estipulaciones que convengan.

En lo que tiene que ver con Certicámara, la Declaración de Prácticas de Certificación publicada en su página *web* contiene cláusulas limitativas y exonerativas de responsabilidad. En efecto, allí se señala que las obligaciones de la entidad son de medio y no de resultado, que no le asiste deber alguno de resarcir daños producidos más allá del año siguiente a la pérdida de vigencia o la revocatoria del certificado, que además responderá hasta por la culpa leve y fija en US $ 50.000 la suma máxima para indemnizar los daños que el uso de sus certificados produjera, sin importar algún otro aspecto adicional[33].

Estas cláusulas exonerativas y limitativas del resarcimiento serán inoponibles siempre que en el caso concreto haya responsabilidad por parte de

---

[30] Colombia, Congreso de la República, Código Civil sancionado el 26 de mayo de 1873, artículo 1604: " ... El deudor no es responsable del caso fortuito, a menos que se haya constituido en mora (siendo el caso fortuito de aquellos que no hubieran dañado a la cosa debida, si hubiese sido entregado al acreedor), o que el caso fortuito haya sobrevenido por su culpa.

"La prueba de la diligencia o cuidado incumbe al que ha debido emplearlo; la prueba del caso fortuito al que lo alega.

"Todo lo cual, sin embargo, se entiende sin perjuicio de las disposiciones especiales de las leyes, y de las estipulaciones expresas de las partes".

[31] Cuéllar Gutiérrez, Humberto. *Responsabilidad Civil Extracontractual*. Primera Edición. Bogotá. Librería Jurídicas Wilches. 1983, pp. 29-31.

[32] Peña Valenzuela, Daniel. *La Responsabilidad Civil en la Era Digital*. Primera Edición. Bogotá. Universidad Externado de Colombia. 2007, pp. 71-91.

[33] Cfr. http://www.certicamara.com

Certicámara a título de culpa grave o dolo o llegara a establecerse que el monto de los US $50.000 es irrisorio para la indemnización de las lesiones, debido al número de perjudicados o a la calidad de aquéllas[34].

2. LA SEGURIDAD DE LA INFORMACIÓN Y LOS DERECHOS PERSONALES EN EL COMERCIO ELECTRÓNICO

2.1 Inseguridad y Desconfianza en la Red

Internet, la red de comunicación por antonomasia, ha sido el motor del Comercio Electrónico, facilitando el desarrollo empresarial y al mismo tiempo la satisfacción de intereses de los consumidores. No obstante, la producción de estos beneficios se encuentra rodeada por una realidad preocupante: la inseguridad. En efecto, la *web* no fue diseñada teniendo en mente la protección de los derechos y la información de sus usuarios[35].

Este panorama eleva su grado de alarma cuando se comprende que la total implementación de los supuestos requeridos por la Contratación Telemática (como la equivalencia funcional y la eficacia probatoria del documento y la firma electrónicos) sólo es posible si los usuarios confían en el sistema, lo cual se producirá únicamente cuando se atenúe la agresividad de las nuevas tecnologías hacia los derechos personales.

2.2 Riesgos para los Datos Personales

Toda la información que las personas van dejando dispersa a lo largo de sus vidas puede ser fácilmente recogida, confrontada, analizada, transferida, utilizada, accedida sin autorización, etc.[36]. Hoy en día, "al abrir la ventana de nuestro ordenador a la calle de la red global de ordenadores entre sí conectados, nos exponemos a la indiscreta observación de los demás usuarios de esa urdimbre de máquinas, programas e información digitalizada que, sin nuestro consentimiento y sin siquiera nuestro conocimiento, pueden ir anotando las huellas electrónicas personales que vamos dejando en nuestra ruta de *internautas*"[37].

En suma, el aumento de las formas de vulneración del derecho a la intimidad y a la autodeterminación informativa que ofrecen los desarrollos tecnológicos ha ocasionado hoy una preocupación mayor a todas las conocidas a lo largo de nuestra era[38].

2.3 La Indebida Manipulación de Información Personal en la Historia

---

[34] Peña Valenzuela, Daniel. *La Responsabilidad Civil en la Era Digital.* Ob.Cit.

[35] Cfr. e-books: Albanese, Jason, Sonnenreich, Wes. *Network Security Ilustrated*. Primera Edición. Nueva York. McGraw-Hill. 2004. p. 147; Cole, Eric, Krutz, Ronald, Conley, James W., *Network Security Bible*, Primera edición, Indianapolis, Wiley Publishing, 2005; Becker, Eberhard, Buhse, Willms, Günnewig, Dirk y Rump, Niels, *Digital Rights Management, technological, economic, legal and political aspects*, Primera edición, Alemania, Springer, 1998.

[36] Davara, Miguel Ángel, *Manual de Derecho Informático*, Primera edición, Navarra, Aranzadi, 2000, p. 43.

[37] Cfr. Díaz, Francisco Eugenio, *La protección de la Intimidad y el Uso de Internet*. Ob. Cit., p. 150.

[38] Cfr. Remolina Angarita, Nelson, *Data protección: Panorama nacional e internacional*. Ob. Cit., p. 100.

La historia recuerda con amargura los malos manejos de los datos personales.

En 1941, el presidente de los Estados Unidos, Franklin D. Roosevelt, ordenó la confección de un listado con nombres y direcciones de todos los descendientes de japoneses que estuvieran residiendo en su país. El listado fue realizado en menos de una semana con base en los censos de 1930 y 1940. Luego del nefasto ataque a Pearl Harbor, quienes hacían parte de él fueron reubicados y sometidos a toda clase de abusos contra su integridad[39].

En la Francia de 1978, se concibió un proyecto denominado Safari (siglas de "Systéme Automatisé pour les Fichiers Administratifs et le Répertoire des Individus"). La idea pretendía asignar a cada francés un número de identificación y unificar la información contenida en los ficheros públicos. El deseo tuvo una férrea oposición que lo hizo naufragar porque nada impedía que se repitiera lo sucedido durante la ocupación nazi, donde con el decidido apoyo del coloso tecnológico IBM la simple verificación de dígitos contenidos en numeraciones de identidad o la consulta de tarjetas perforadas permitía conocer la raza, la religión o el sexo de las personas[40].

Hace un tiempo, los documentos desclasificados de la Agencia de Seguridad Nacional de los Estados Unidos (NSA) permitieron confirmar la existencia de la red de espionaje y tratamiento de información por medios electrónicos más grande del mundo. Creada principalmente por los Estados Unidos, Australia y Gran Bretaña, Echelon se encarga de interceptar y analizar comunicaciones con el objetivo inicial de perseguir el terrorismo. Sus sedes en todo el mundo no están sujetas a ningún control, lo que ha motivado la protesta del Parlamento Europeo y de otras instancias internacionales para impedir que se produzca algún factor de riesgo en perjuicio de los derechos de los *internautas*[41].

Antes de enrolarse en la lucha revolucionaria con la guerrilla de las FARC y de ser extraditado a los Estados Unidos, el vallenato Ricardo Palmera, alias Simón Trinidad, se desempeñaba como gerente de un Banco en la capital del departamento del Cesar. Una vez alzado en armas, Palmera secuestró y extorsionó a varios hacendados cesarenses gracias a haber llevado consigo toda la información a la que tuvo acceso por su cargo[42].

En 2003, la conocida y controvertida empresa Choice Point –que circula como ave de rapiña sobre la información personal en México, Nicaragua, Guatemala, Venezuela, Costa Rica, entre otros– adquirió una completa y valiosa base de datos con la fecha y lugar de nacimiento, el número de identificación y de pasaporte, la descripción familiar y de los rasgos físicos de 31 millones de colombianos, el nombre de todas las empresas registradas en el

---

[39] Ibídem, p. 116.
[40] Cfr. Díaz, Francisco Eugenio, *La Protección de la Intimidad y el Uso de Internet*. Ob. Cit., p. 150.
[41] Cfr. De Alzaga, Pedro, "Echelon sale a la luz", *Diario del navegante,* 27 de enero de 2000, http://www.elmundo.es/navegante/2000/01/27/echelon.html.
[42] Remolina Angarita, Nelson, "Censos, Estadísticas y Datos Personales en la Era del Gobierno Electrónico", *Revista de Derecho, Comunicaciones y Nuevas tecnologías del GECTI*, No. 1, abril de 2005, Bogotá, pp. 207-246.

país, su NIT, identidad de los dueños, descripción del negocio en dos idiomas, fax, e-mail, teléfono e información financiera, además del número de identificación, tipo de artefacto y propietario de todas las aeronaves de Colombia. El negocio fue tan completo que el emporio informático ofrece como valor agregado actualizaciones semestrales para sus compradores, lo que le ha permitido recaudar en sólo un año la cifra de US $11.000.000. Entre los clientes conocidos de la compañía figuran agencias de seguridad de los Estados Unidos como el Servicio de Naturalización e Inmigración (que ya aceptó haber hecho varios operativos exitosos gracias a su adquisición), el FBI y la CIA[43].

2.4 La Información como Insumo Empresarial

Uno de los principales usos de la recolección y tratamiento exhaustivos de la información que circula en la red es el mercadeo. De manera sencilla y con una buena base de datos adquirida de cualquier forma, las empresas pueden conocer el mercado al que se enfrentan, crear perfiles de sus potenciales clientes o llegar de manera directa y simplificada al público.

Hay dos opciones para recoger la información a explotar: (I) Usar medios lícitos y leales; (II) Recurrir a la vía más expedita. No habrá que esforzarse para saber cuál es la alternativa más empleada, porque la tecnología brinda muchas opciones para recabar información personal de manera discreta, por no decir ilegal. Los recursos más conocidos, para mencionar sólo algunos, son las famosas *Cookies* y los S*pywares*[44]*.*

Otra forma de recabar información valiosa empleando la segunda opción está en las Cámaras de Comercio del país. Sus sedes en Cartagena, Bogotá, Santa Marta o Medellín ofrecen bases de datos empresariales generalmente con la identificación, la ubicación, el tipo de empresa, la actividad económica, sucursales, situación jurídica, financiera e información de constitución[45].

Apenas se haya recogido la información inicia el *e-marketing* a través de lo que en el argot informático se conoce como O*pt-in o Spam.* Estos consisten en el envío masivo de mensajes propagandísticos de acuerdo con los perfiles y hábitos de los destinatarios[46].

---

[43] Cfr. Remolina Angarita, Nelson, "Protección de Datos Personales ¿Política Integral de Estado?" *Sistemas,* No. 1, enero-marzo 2006, Bogotá, Asociación Colombiana de Ingenieros de Sistemas. http://www.acis.org.co/index.php?id=733; Calle D´Aleman, Sol Beatríz, "Protección de Datos de Carácter Personal en el Comercio Electrónico". *Sociedad de la Información Digital: Perspectivas y Alcances.* Primera edición. Bogotá. Universidad Externado de Colombia, p. 233.

[44] Las Cookies son archivos de texto almacenados por el servidor de una página web en el disco duro de un navegante que le permitirá conocer lo realizado en los enlaces visitados. Los spywares vienen escondidos generalmente en programas de uso libre (free software) y recogen información del usuario aún sin que esté conectado a la red. Una vez se produzca la conexión se enviarán todos los datos almacenados sin que el titular lo sepa.

[45] Cfr. Las direcciones las respectivas páginas web: Cámara de Comercio de Bogotá http://camara.ccb.org.co/contenido/categoria.aspx?catID=84,
Cartagena http://www.cccartagena.org.co/economica/basedatos.htm,
Medellín http://www.camaramed.org.co/servicioquees.asp, y
Santa Marta http://www.ccsm.org.co/serv_cam/bde/sc_bde_index.php

[46] En el Spam no hay autorización del receptor mientras que en el Opt-in sí la hay.

Con todo, ambos son mecanismos atractivos que garantizan una promoción efectiva de bienes y servicios, asegurando a los comerciantes la posibilidad de ubicar, atraer y conservar clientes con el envío de mensajes publicitarios cada vez más personalizados, lo que supera notablemente a los mecanismos tradicionales de *marketing* en la producción de resultados de la ecuación costo-beneficio[47], lo que explica porqué suele ser atractivo para el mundo de los negocios usar y abusar de los datos personales. Aquí impera la máxima (antes frase de cajón) de que "la información es poder".

2.5 Protección de los Datos Personales

Infortunadamente el mercadeo no es el único destino que tienen los datos personales, estos son aprovechados diariamente por sectores oscuros de la sociedad que saben mucho acerca de nosotros para llevar a cabo sus actividades *non sanctas*.

El asunto no es de poca monta ni es un tema del futuro, es una realidad de hoy lo quiera o no el Derecho. Por ello la conclusión preliminar a la que se llega es que los participantes del Comercio Electrónico se encuentran totalmente desprotegidos ante el abuso del contenido mismo de su personalidad: su información.

2.5.1 Intentos de Regulación

En los años posteriores a la Constitución de 1991 ha habido varios intentos de regulación. Basta recordar los proyectos 12 de 1993, 71 y 75 de 2002, 64 de 2003 o 142 de 2004. Todos corrieron la misma suerte al no ser aprobados.

Con la sentencia C-1011 de 2008, la Corte Constitucional impartió su aprobación al último proyecto de Ley Estatutaria sobre el tema (Senado 027 de 2006, Cámara 221 de 2007), el cual se convirtió en la Ley 1266 de 2008, que pretende regular el uso y abuso de la información personal. Lamentablemente, este no es el sistema de protección necesario por los siguientes motivos, entre otros: (I) Se limita al manejo de las bases de datos financieros, crediticios y comerciales, catalogando esta actividad como de interés público, la cual en realidad tiene fines netamente comerciales interesantes sólo para un sector de la economía; (II) Clasifica sin ningún criterio razonable a los datos en públicos, semi-privados –entre los que se encuentra el dato financiero y crediticio de la actividad comercial– y privados; (III) No exige la autorización del titular para la administración de información financiera, crediticia, comercial o proveniente del exterior; (IV) La información negativa permanecerá 4 años en los reportes electrónicos luego de que la obligación sea cancelada voluntariamente.

Con esta normatividad, Colombia sigue estando en mora de ofrecerle a sus residentes una solución que aminore la incertidumbre respecto de sus datos y sus derechos personales.

2.5.2 Principios

[47] Peña Valenzuela, Daniel. "Reflexiones en torno al Concepto de Empresa Virtual". *Contexto.* No. 22 segundo cuatrimestre. 2007. Bogotá, Universidad Externado de Colombia, p. 118.

Ante la ausencia de una normatividad fuerte, este trabajo propone como eje central de cualquier regulación sobre el tema un esquema de protección de datos personales orientado por principios, el cual recae sobre actividades en las que se verifiquen dos supuestos: (I) El manejo de información personal, y; (II) Que ésta se encuentre contenida o sea manipulada por medio de archivos o bases de datos[48].

Los principios cobijan a todas las etapas del tratamiento de información personal, como la recolección, el almacenamiento, la circulación, la publicación, la transferencia, el uso, etc., consultando el equilibrio entre el desarrollo de la sociedad del Comercio Electrónico y los derechos de los consumidores[49].

Es imperativo aclarar que el centro del sistema de protección no está determinado únicamente por el Derecho a la Intimidad, sino que también lo integra el Derecho al Correcto Tratamiento de la Información Personal o a la Autodeterminación Informativa o Hábeas Data. Si no fuera así, la preeminencia exclusiva de los datos privados sería el límite único del tratamiento de la información personal, dejando desamparados otros bienes jurídicos también relevantes[50].

Los principios formulados se nutren de la filosofía de la regulación de los Derechos Fundamentales en la Constitución Nacional, sus intentos de regulación por el Congreso de la República, los criterios expuestos por la doctrina nacional y foránea, y las decisiones producidas por la Corte Constitucional colombiana, sin que ello impida dejar a un lado lo que no se considere pertinente.

Antes de entrar a analizarlos, hay que aclarar que en este escrito se toma partido por la respuesta a ciertos interrogantes que la doctrina mundial se ha planteado en torno a cualquier sistema de protección de la información personal. En efecto, no cabe duda que la salida más afortunada a la desprotección de la información de las personas está en una regulación genérica y amplia, que no incentive medidas coyunturales de acuerdo al sector a proteger, como se presenta actualmente con la Ley Estatutaria de Hábeas Data colombiana, que sólo regula lo concerniente a los datos financieros y crediticios.

Además, siguiendo el pensamiento de la doctrina constitucional, no es propicio distinguir entre bases de datos privadas y públicas, porque esto es insuficiente, superficial y peligroso, pues el hecho de que cierta información se encuentre en una base de datos pública no implica que mediante la circulación puedan menoscabarse derechos de la misma forma como podría llegar a suceder con un fichero privado.

Hay que reconocer que no hay ningún impedimento para considerar que las personas jurídicas pueden también ser titulares del Derecho al Correcto Tratamiento de la Información y a la Intimidad, porque el manejo inadecuado de

---

[48] Upegui Mejía, Juan Carlos. “Diez Ideas para un Régimen de Datos Personales en Clave Latinoamericana” D*erecho Comparado de la Información*, No. 10, julio-diciembre de 2007, México, Universidad Nacional Autónoma de México.
[49] Calle D’Aleman, Sol Beatríz. “Protección de Datos...”. Ob. Cit., pp. 232 y 234.
[50] Upegui Mejía, Juan Carlos. “Diez Ideas para un ...”, Ob. Cit.

los datos relacionados con la actividad mercantil de los entes empresariales también es relevante para el derecho, toda vez que las estructuras sociales y comunicativas también se proyectan sobre estos[51].

Inicia el análisis de los principios que orientan el esquema de protección de la información personal.

2.5.2.1 Principio de Titularidad[52]

Este principio parte de la base de que cuando se protegen los datos personales, también se resguarda a la persona, quien es la única titular legítima de su información[53]. La titularidad de la que aquí se habla no tiene nada que ver con el clásico concepto del Derecho de Propiedad. Efectivamente, impide que otros accedan a esa esfera del individuo comprendida por todo aquello que lo define como tal.

La autorización de la recolección y el tratamiento de los datos no produce su adquisición por terceros, ni da lugar a que puedan ser cedidos, enajenados, embargados o susceptibles de prescripción.

El tiempo no es un obstáculo para que el titular solicite según su deseo la eliminación de las bases de datos que sobre él existan.

2.5.2.2 Principio de Consentimiento Informado[54]

El Consentimiento Informado es una garantía que permite el tratamiento de información personal solamente con la autorización expresa, escrita y revocable del titular, a quien se le debe informar completamente de todos los aspectos concernientes a la recolección, finalidad, uso, etc.

En cada caso, deberá delimitarse la forma como la información será obtenida, dónde se almacenará, qué actos comprenderá su tratamiento, término de vigencia, cuál es la finalidad perseguida con la manipulación y cualquiera otra referencia que pueda influir en el titular al otorgar el consentimiento. La variación posterior de cualquiera de estos aspectos no será posible sin la anuencia del titular.

2.5.2.3 Principio de Pertinencia[55]

---

[51] Colombia, Presidencia de la República, Ministerio de Desarrollo Económico, Ministerio de Comunicaciones y Ministerio de Comercio Exterior. Decreto 1747 de 11 de septiembre de 2000, artículo 18 del Decreto 1747 de 2000: “Responsabilidad. Las entidades de certificación responderán por todos los perjuicios que se causen en ejercicio de sus funciones (…).

[52] Cfr. Colombia, Corte Constitucional, Sala Primera de revisión. Sentencia de tutela T-414 de 16 de junio 1992, Magistrado Ponente: Ciro Angarita Barón, Expediente T-534.

[53] Miguel Ángel Davara, *Manual de Derecho* I*nformático*, Ob. Cit., p. 48.

[54] Cfr. Colombia. Corte Constitucional. Sala Tercera de Revisión. Sentencia de tutela T-307 de 5 de mayo 1999 Magistrado Ponente: Eduardo Cifuentes Muñoz, Expedientes T-187958; T-729 de 5 de septiembre 2002. Sala Séptima de Revisión. Magistrado Ponente: Eduardo Montealegre Lynett, Expedientes T-467467; T-592 de 17 de julio de 2003 Magistrado Ponente: Álvaro Tafur Gálvis; C-993 de 12 de octubre de 2004. Sala Plena. Magistrado Ponente: Jaime Araújo Rentería, Expedientes D-5134; T-526 de 27 de mayo de 2004. Sala Octava de Revisión. Magistrado Ponente: Álvaro Tafur Gálvis, Expediente T-850.657.

[55] Cfr. Colombia. Corte Constitucional. Sentencia C-185 de 4 de marzo de 2003, Sala Plena. Magistrado Ponente: Eduardo Montealegre Lynett, Expediente D-4220.

La adecuación entre los datos personales obtenidos y su utilización asegura el fortalecimiento de la protección de información personal y evita que se excedan los límites permitidos.

En otros términos, la licitud del tratamiento está determinada por el grado de conexidad que haya entre la finalidad, la recolección, el uso y la calidad de la información. Esto ocasiona que sólo puedan recabarse datos pertinentes según el objetivo perseguido con su manipulación.

De importancia manifiesta resulta para este principio la demarcación conceptual de los llamados "Datos Sensibles" pues "la experiencia de estos últimos años sobre la aplicación de leyes de protección de datos ha puesto de relieve, de un lado, la dificultad de establecer un catálogo exhaustivo de los datos real o potencialmente sensibles, y de otro, la evidencia de que cualquier información, en principio neutra o irrelevante, puede convertirse en sensible a tenor del uso que se haga de la misma"[56].

Precisamente por esa dificultad en la configuración del concepto, la Corte Constitucional colombiana ha analizado varios caminos para la definición de dato sensible, aunque no ha ofrecido un pronunciamiento unívoco.

La primera sentencia al respecto es la T-307 de 1999, donde la primera definición surge del principio de igualdad y no discriminación. En esta oportunidad define el concepto mediante una regla de prohibición: "… al amparo de la Carta de 1991 no puede menos que sostenerse que todo dato debe recolectarse para una finalidad constitucionalmente legítima. Lo anterior significa, entre otras cosas, que no puede recolectarse información sobre datos sensibles como, por ejemplo, la orientación sexual de las personas, su filiación política o su credo religioso, cuando ello, directa o indirectamente, pueda conducir a una política de discriminación o marginación"[57].

En una segunda oportunidad, en la sentencia T-729 de 2002 la información personal es "dato sensible" en la medida en que se encuentre relacionada con los derechos fundamentales de su titular, como la intimidad, la libertad y el derecho a la honra. Así mismo, hace la precisión de que el concepto de dato sensible sólo se entiende referido a su manejo a través de ficheros, es decir, que si el uso se lleva a cabo de otra manera el asunto no se encuentra comprendido por el Derecho a la Libre Autodeterminación Informativa.

En la sentencia T-310 de 2003, la Corte recorre un nuevo e ininteligible camino en la definición de información sensible, en la medida en que, a diferencia de las anteriores dos posturas, los datos sensibles implican la obligación de que la información circule oportunamente, como sería el caso de las órdenes de captura.

Con base en lo anterior y teniendo en mente la importancia de la integridad personal y el enorme peligro que engendra la indebida manipulación de cierta

---

[56] Pérez Luño, Antonio Enrique, Guerrero Mateus, María Fernanda. *Libertad Informática y Leyes de Protección de Datos Personales*. Primera edición. Madrid. Centro de Estudios Constitucionales. 1989. p. 153.

[57] Colombia. Corte Constitucional. Sentencia de tutela T-307 de 5 de mayo de 1999. Sala Tercera de Revisión. Magistrado Ponente: Eduardo Cifuentes Muñoz, Expediente T-187958.

información, este principio obliga a sentar como concepto de datos sensibles[58], aquellos que se encuentran relacionados con el origen racial y étnico, la vida sexual, las opiniones filosóficas, políticas, las convicciones morales o religiosas o la salud, inclusive la información financiera o crediticia de las personas, y, en ese sentido, sostener que su tratamiento a través de bases o ficheros se encuentra proscrito, toda vez que no se puede olvidar lo doloroso que fue en el pasado el uso y abuso de esta información.

Además, ningún grado de licitud puede haber en el tratamiento de este tipo de información debido a que no incorpora ni podrá incorporar ninguna finalidad benévola o benéfica para las personas.

2.5.2.4 Principio de Libre Acceso, Veracidad y Deber de Rectificación[59]

Como manifestación de la titularidad, toda persona tiene Derecho a saber que sus datos están siendo archivados, a conocer su contenido, a constatar la licitud y veracidad de la información recabada.

Si no es veraz la información que se manipula, el titular puede solicitar de plano su rectificación. En palabras de la Corte Constitucional, "[l]os datos tienen por su naturaleza misma una vigencia limitada en el tiempo, la cual impone a los responsables o administradores de bancos de datos la obligación ineludible de una permanente actualización a fin de no poner en circulación perfiles de "personas virtuales" que afecten negativamente a sus titulares, es decir las personas reales".

2.5.2.5 Principio de Seguridad y Confidencialidad[60]

Basta decir que toda persona natural o jurídica o cualquier institución pública o privada que realice tratamiento de datos personales con la autorización de su titular debe garantizar que su manejo no producirá ninguna afectación a los derechos de las personas ni a su entorno. Como la información sobre las

---

[58] Cfr. Colombia. Corte Constitucional. Sentencia de unificación de tutela SU-528 de 11 de noviembre de 1993. Sala Plena. Magistrado Ponente: José Gregorio Hernández, Expediente acumulados T-14518, T-14892 y T-15628; Sentencia de unificación de tutela Sentencia de unificación de tutela SU-089 de 1 de marzo de 1995. Sala Plena. Magistrado Ponente: Jorge Arango Mejía, Expediente T-41500.

[59] Cfr. Colombia. Corte Constitucional. Sentencias T-110 de 18 de marzo de 1993, Magistrado Ponente: José Gregorio Hernández; T-303 de 18 de junio de 1998, Magistrado Ponente: José Gregorio Hernández; T-321 de 21 de marzo 2000, Magistrado Ponente: José Gregorio Hernández; T-309 de 6 de mayo de 1999, Magistrado Ponente: Alfredo Beltrán Sierra; T-615 de 12 de diciembre de 1995, Magistrado Ponente: Fabio Morón Díaz; T-176 de 24 de abril de 1995, Magistrado Ponente: Eduardo Cifuentes Muñoz; T-443 de 12 de octubre de 1994, Magistrado Ponente: Eduardo Cifuente Muñoz; T-094 de 2 de marzo de 1995, Magistrado Ponente: José Gregorio Hernández; T-094 de 2 de marzo de 1995, Magistrado Ponente: José Gregorio Hernández; SU-089 de 1 de marzo de 1995, Magistrado Ponente: Jorge Arango Mejía; T-552 de 30 de octubre de 1997, Magistrado Ponente: Vladimiro Naranjo Mesa; T-096a de 2 de marzo de 1995, Magistrado Ponente: Vladimiro Naranjo Mesa; T-086 de 1 de marzo de 1996, Magistrado Ponente: Vladimiro Naranjo Mesa; T-097 de 3 de marzo de 1995, Magistrado Ponente: José Gregorio Hernández; T-414 de 16 de junio de 1992, Magistrado Ponente: Ciro Angarita Barón; T-060 de 30 de enero de 2003, Magistrado Ponente: Eduardo Montealegre Lynett.

[60] Colombia. Corte Constitucional. Sentencia T-227 de 17 de marzo de 2003. Sala Séptima de Revisión. Magistrado Ponente: Eduardo Montealegre Lynett, Expediente T-669050.

personas no es importante para el Derecho únicamente en proporción a su grado de conocimiento por el público, los datos recogidos –sean privados o no– no pueden ser divulgados.

Por ello, es obligación de quienes administren los ficheros autorizados para el tratamiento de información garantizar que sus empleados no la usarán de forma excesiva.

Los archivos donde reposa la información deben ser administrados con todo el cuidado posible para que no se produzca su pérdida, alteración, acceso no autorizado o sustracción, los cuales de suceder podrán ser fuente de Responsabilidad Civil y de Acción de Tutela.

3. LA DESUETUD DEL CONCEPTO TRADICIONAL DE INFORMACIÓN PRIVILEGIADA

Actualmente, la circulación constante de información como elemento fundamental del comercio ha generado toda una serie de cambios estructurales.

Los adelantos saltan a la vista: La mayoría de los "arduos y dispendiosos procesos de manejo de información contable, financiera y de recursos humanos, por ejemplo", cuentan "con el apoyo de los computadores"[61]; Las entidades públicas adquieren bienes o servicios de características uniformes y común uso por medio de subastas electrónicas[62]; "Las comunicaciones de la empresa entre sus empleados y directivos también han venido cambiando por la utilización de medios electrónicos. En tal sentido el correo electrónico y las intranets se han constituido en una imperativa forma de agilizar el flujo de información"[63].

Frente a esta realidad, la reacción de "la ciencia de la administración y las tecnologías de la información" ha sido de total amoldamiento al cambio. "El derecho por el contrario aparece rezagado frente a los avances tecnológicos y debe acudir a una deficiente herramienta como es la interpretación analógica de figuras y categorías nuevas"[64].

Ese rezago puede constatarse en el manejo que le da al abuso de información privilegiada. En efecto, incurre en esta conducta quien divulga datos que no son de dominio público, y que ha conocido de forma legítima en razón de su cargo o sus funciones.

Como puede observarse, el acceso legítimo a los datos divulgados está en el centro de la noción y es el punto distintivo con cualquier otro tema. Esto resulta insuficiente para el mundo de hoy, donde asistimos a la ruptura de concepciones tradicionales.

---

[61] Peña Valenzuela, Daniel. "*Reflexiones en torno al Concepto de Empresa Virtual"*, Op. Cit.
[62] Colombia. Congreso de la República. Numeral 2 del artículo 2 de la Ley 1150 de 16 de julio de 2007; Colombia. Presidente de la República, Ministro del Interior y Justicia, Ministro de Hacienda y Crédito Público, Ministro de Transporte, Directora del Departamento Nacional de Planeación. Artículos 18 a 28 del Decreto 66 de enero 16 de 2008.
[63] Peña Valenzuela, Daniel. "Reflexiones en torno al Concepto de Empresa Virtual", Op. Cit.
[64] Ibídem.

Con todo, es necesario que el manejo indebido de la información privilegiada comprenda también el rastreo, interceptación y toda forma de acceso ilegítimo de las comunicaciones, debido a que actualmente se sanciona exclusivamente el acceso autorizado de los datos privilegiados.

Este no es un simple tema conceptual sino que implica que no sigan sin consecuencias jurídicas aquellas conductas nocivas que el ordenamiento debe rechazar.

CONCLUSIONES

1. El papel desempeñado por las entidades de certificación de firmas digitales, es fundamental para promover la seguridad y la confianza en todas las aristas del comercio electrónico. El uso adecuado de la tecnología de Infraestructura de Clave Pública o PKI es un método muy seguro para la emisión, recepción y conservación de mensajes, asegurando su autenticidad e integridad.

2. La seguridad ofrecida por el sistema PKI y la firma digital, no puede servir de excusa para restarle valor a la firma electrónica propiamente dicha. Ambas formas de dotar de autenticidad a los documentos electrónicos gozan de validez jurídica y eficacia probatoria, como lo impone la “neutralidad tecnológica” y el “enfoque de los equivalentes funcionales”.

3. Aunque Certicámara S.A. está realizando de forma correcta sus funciones, se hace necesario que surja otra Entidad de Certificación abierta para que en una sana competencia pueda lograrse mejorías en el servicio de certificación digital, como por ejemplo, la disminución de los costos de los certificados digitales, los cual contribuiría enormemente a reducir la llamada brecha digital.

4. El Congreso de la República está en mora de expedir una ley estatutaria integral que defienda los derechos a la intimidad y al correcto tratamiento de la información personal de las personas involucradas en el comercio electrónico. Esta normativa debe ir por un camino totalmente contrario a la que hoy se encuentra vigente, toda vez que se ocupa únicamente permitir el uso indiscriminado de los datos financieros y crediticios.

5. La información financiera y creditica, la relacionada con las inclinaciones sexuales, las convicciones políticas y morales de las personas son datos sensibles que no puede ser objeto de tratamiento bajo ninguna circunstancia, debido al grave peligro que engendra para su titular el uso indebido de los mismos, no se puede echar por la borda toda la experiencia que la historia ha provisto respecto de la indebida manipulación de la información personal.

6. Se insiste, de acuerdo al principio de consentimiento informado, en la necesidad de que sólo cuando medie la autorización expresa del titular de los datos estos pueden ser tratados de acuerdo a los demás parámetros señalados. El cumplimiento de cada uno de los principios explicados debe ser *conditio sine qua non* para el uso de la información personal.

7. Más allá de cualquier discusión conceptual, el abuso de información privilegiada debe cobijar el acceso ilegítimo de las comunicaciones y no

únicamente el conocimiento autorizado de datos que no son de dominio público.

BIBLIOGRAFÍA

Archila Peñalosa, Emilio. "Principios de Regulación Tomados por la Superintendencia de Industria y Comercio como Base en la Reglamentación de las Entidades de Certificación", *Memorias Comercio Electrónico*, primera edición, Bogotá, Universidad Externado de Colombia, 2000.

Albanes, Jason, Sonnenreich, Wes. *Network Security Ilustrated*, primera edición, Nueva York, McGraw-Hill, 2004.

Becker, Eberhard et al. *Digital Rights Management, technological, economic, legal and political aspects*, primera edición, Alemania, Springer, 1998.

Calle D'Aleman, Sol Beatríz. "Protección de Datos de Carácter Personal en el Comercio Electrónico", *Sociedad de la Información Digital: Perspectivas y Alcances*, Bogotá, Universidad Externado de Colombia, 2007.

Cano, Jeymi. "Evidencia Digital: Conceptos y Retos", *Internet, Comercio Electrónico y Telecomunicaciones*, primera edición, Bogotá, Universidad de los Andes y Legis Editores, 2002.

Cole, Krutz et al. *Network Security Bible*, primera edición, Indianapolis, Wiley Publishing, 2005.

Díaz, Francisco Eugenio. "La protección de la intimidad y el uso de internet", *Informática y Derecho*, Nos. 30-32 y 31, 1999, Mérida, Centro Regional de Extremadura.

Henao Restrepo, Darío. "Ley de Comercio Electrónico en Colombia", *Nuevos Retos del Derecho Comercial*, primera edición, Medellín, Biblioteca Jurídica Diké, 2000.

Jijena Leiva, Renato. "Naturaleza Jurídica y Valor Probatorio del Documento Electrónico. El Caso de la Declaración de Importación Electrónica o Mensaje CUSDEC", *Informática y Derecho*, Nos. 30-32 y 31, 1999, Mérida, Centro Regional Extremadura.

Davara, Miguel Ángel. *Manual de Derecho Informático*, tercera edición, Navarra, Aranzadi, 2000.

Nuñez Jiménez, José. "Valor probatorio del Documento Electrónico. Su Autenticidad a través de la Criptografía", *Informática y Derecho*, Nos. 30-32 y 31, 1999, Mérida, Centro Regional Extremadura.

Peña Valenzuela, Daniel. "Reflexiones en torno al Concepto de Empresa Virtual", *Contexto*, No. 22 segundo cuatrimestre, 2007, Bogotá, Universidad Externado de Colombia.

Peña Valenzuela, Daniel. "El Contrato Electrónico y los medios probatorios", *El Contrato por Medios Electrónicos*, primera edición, Bogotá, Universidad Externado de Colombia, 2003.

Peña Valenzuela, Daniel, *La Responsabilidad Civil en la Era Digital*, Primera Edición, Bogotá, Universidad Externado de Colombia, 2007.

Pérez Luño. *Libertad Informática y Leyes de Protección de Datos Personales,* primera edición, Madrid, Centro de Estudios Constitucionales, 1989.

Pérez Useche, Marco. "El Tratamiento de la Firma Electrónica en Colombia y en el Derecho Uniforme", *Derecho del Comercio Electrónico*, primera edición, Medellín, Biblioteca Jurídica Diké, 2002.

Prieto Gutiérrez, Jesús. "Problemática y Expectativas en Torno al Documento Electrónico: Valor Probatorio", *Informática y Derecho*, Nos. 30-32 y 31, 1999, Mérida.

Recalde Castelles, Andrés. "Comercio y Contratación Electrónica", *Informática y Derecho*, Nos. 30-32 y 31, 1999, Mérida.

Remolina Angarita, Nelson. "Censos, Estadísticas y Datos Personales en la Era del Gobierno Electrónico", *Revista de Derecho, Comunicaciones y Nuevas tecnologías del GECTI*, No. 1, abril de 2005, Bogotá, Universidad de los Andes.

Remolina Angarita, Nelson. "Data protection: panorama nacional e internacional", *Internet, Comercio Electrónico y Telecomunicaciones*, primera edición, Bogotá, Universidad de los Andes y Legis Editores, 2002.

Remolina Angarita, Nelson. "Protección de Datos Personales ¿Política Integral de Estado?", *Sistemas,* No. 1, enero-marzo 2006, Bogotá, Asociación Colombiana de Ingenieros de Sistemas. http://www.acis.org.co/index.php?id=733.

Rengifo García, Ernesto. "Comercio Electrónico, Documento Electrónico y Seguridad Jurídica", *Memorias Comercio Electrónico*, primera edición, Bogotá, Universidad Externado de Colombia, 2000.

Upegui Mejía, Juan Carlos. "Diez Ideas para un Régimen de Datos Personales en Clave Latinoamericana", *Derecho Comparado de la Información*, No. 10, julio-diciembre de 2007, Ciudad de México, Universidad Nacional Autónoma de México.

Zubieta Uribe, Hermann. "El tiempo en los Mensajes de Datos", *El Contrato por Medios Electrónicos*, primera edición, Bogotá, Universidad Externado de Colombia, 2003.

Zubieta Uribe, Hermann. "Los Mensajes de Datos y las Entidades de Certificación", *Internet, Comercio Electrónico y Telecomunicaciones*, tercera edición, Bogotá, Universidad de los Andes y Legis Editores S.A., 2002.

LIBRERÍA EDICIONES DEL PROFESIONAL LTDA.

Calle 12, No. 5-24, Tel. 2433482, Bogotá,D.C., Colombia,
Dirección Postal
Instituto Colombiano de Derecho Procesal
Calle 67, No. 4A-09, Tel. 3104406 - Fax.3104489
Bogotá, D.C., Colombia,

Hecho el depósito que exige la ley.
Impreso en EDITORIAL ABC.
ISSN 0123-2479