DEL DOCUMENTO FÍSICO AL DOCUMENTO ELECTRÓNICO

M.Sc. Raúl Guevara Villalobos

La revolución tecnológica ha planteado el giro de la sociedad industrial a la sociedad de la información[1], cuya fuerza motriz ha sido las computadoras y el Internet[2].

Los medios de comunicación se han enlazado con el día a día de todas las personas en la mayoría de las sociedades, a tal punto que han logrado interferir en patrones tiempo espaciales de organización, ayudando a la generación de nuevos espacios y ritmos de vida. La migración de la tecnología de la computación desde la industria y el laboratorio, hasta nuestras casas ha intensificado estos procesos[3]. Por ejemplo, el correo electrónico derriba barreras espaciales y temporales, al permitir enviar documentos de manera casi instantánea entre dos o más personas que pueden estar en continentes diferentes. Similar situación ocurre con los SMS, o los "realtime" chats y redes sociales.[4]

Las aplicaciones y las consecuencias de su uso tienen dimensiones insospechadas hace 10 años; los recientes disturbios y saqueos en Londres son ejemplo de ello[5].

Perry Sutcliffe- Keenan, un muchacho de 22 años de Latchford, Warrington, Inglaterra, usó su cuenta de Facebook para publicar una página denominada "*The Warrington Riots*". A la mañana siguiente de haberla creado, él removió la página y se disculpó argumentando que había sido una broma. Si bien su mensaje fue distribuido a 400 contactos en Facebook, no causó ningún efecto.

No obstante, una Corte de Chester Crown condenó al señor Sutcliffe a 4 años de cárcel por considerar que su mensaje había causado un verdadero pánico y obligó a la fuerza policial a organizarse para retener cualquier manifestación en Warrington. Por su parte, la Fiscalía solicitó la pena de prisión argumentando que el "post" había causado un pánico significativo en las comunidades de Warrington debido a los rumores de que la violencia se esparciría.[6]

1 LONG (Larry). Introducción a las computadoras y al procesamiento de la información. Segunda edición. Prince Hall. P2.
2 RAMONET (Ignacio). Internet, el mundo que llega: Los nuevos caminos a la comunicación. Editorial Alianza. 1998.
3 HACKETT (Edward) y otros. The Handbook of Science and Technology Studies. Tercera edición. MIT Press. London, 2008.
4 Las Ciencias Sociales discuten sobre tres asumpciones fundamentales: (i) Que la cultura, el día a día y los individuos son material y conceptualmente distintos de las tecnologías; (ii) que las tecnologías son socialmente moldeadas, pero la sociedad no está tecnológicamente moldeada; que las avitidad humana, en la forma de fuerza social, histórica y económica, es la única fuerza o agente que impacta la cultura. LISTER (Martin) y otros. New Media. A Critical Introduction. Segunda Edición. Routledge. New York, 2009. P. 238.
5 On line: www.guardian.co.uk/uk/2011/aug/16/facebook-riot-calls-men-jailed. Martes 16 de agosto del 2011.
6 CfrOnlinewww.telegraph.co.uk/news/uknews/law-and-order/8706712/England-riots-Facebook-riots-sentences-will-act-as-deterrent.html

El uso de las redes sociales durante manifestaciones en Egipto y recientemente en Londres, ha puesto en la palestra el rol que el Gobierno de Inglaterra piensa deben tener las redes sociales, e incluso se ha sugerido la posibilidad de desconectar lo sistemas de telecomunicaciones o al menos las redes sociales para prevenir el desorden civil[7]. Research in Motion se encuentra actualmente bajo presión ya que se la ha requerido explique sus acciones durante las manifestaciones en Londres, después de que un usuario de Blackberry usó la aplicación de Messenger de BB para difundir posibles objetivos de los disturbios y saqueos.

Los desarrollos tecnológicos han puesto en jaque las regulaciones de propiedad intelectual en varias ocasiones, especialmente en la segunda mitad del Siglo XX. Por ejemplo, el desarrollo de redes "peer to peer" como Napster y Kazaa, entre otras, permitieron la adquisición de música y videos de manera casi instantánea y mucho más económica que la música en algún soporte material, lo que llevó a transformar las leyes de propiedad intelectual, así como la distribución de datos.

Esto son tan solo algunos ejemplos de cómo los avances en las comunicaciones y en la tecnología presentan retos para los operadores jurídicos.

Uno de los temas principales, ha sido la necesidad de adaptar las instituciones y conceptos del derecho a las nuevas realidades organizacionales, posibles gracias a las nuevas tecnologías y avances de la informática. El Internet es hoy uno de los medios más usados para la transferencia de datos y realización de actividades comerciales, que requiere combinar requisitos tecnológicos de seguridad en cuanto a la identidad del emisor y receptor de la comunicación, y que se asegure que la información va a ser fidedigna y confidencial.

A continuación repasaremos algunos retos que ha tenido que afrontar el Derecho para poder adaptarse a las nuevas situaciones que plantea el avance de la tecnología y la informática, especialmente en relación a la autenticidad de los documentos y de quienes los suscriben.

1. DOCUMENTO ELECTRÓNICO

La noción de documento ha venido evolucionando conforme la dinámica de las interacciones sociales[8] en diferentes sociedades. Actualmente, es posible considerar una página web, un Chat, un post en facebook, o un correo electrónico un documento?

Tradicionalmente el documento[9] cuenta con dos elementos objetivos: la información, y su soporte. En el caso del documento electrónico, este es:

7 Online www.zdnet.com/blog/btl/british-pm-considers-turning-off-social-networks-amid-further-riots/54711?tag_?=content;siu-container.

8 DE SANTO (Victor). El proceso civil. Buenos Aires. Editorial Universidad. 1983. Tomo III.

9 Es "la representación gráfica de un pensamiento, generalmente por escrito, con un contenido de finalidad preconstituida y de constatación de hechos o acontecimientos, acreditados, probatoriamente, frente a futuras contingencias, destinados al tráfico jurídico" Tribunal Supremo 6-10-75. Citado por TERAMOND (Carmen) y otro. Concepto, valor jurídico y regulación de la firma digital en Costa Rica. Universidad de Costa Rica. Facultad de Derecho. Tesis para optar por el grado de Licenciadas en Derecho. 2002

"una secuencia informática de bits (números binarios) que pueden representar cualquier tipo de información, cumple los requisitos del documento en soporte de papel, en el sentido de que contiene un mensaje (texto alfanumérico o diseño gráfico) en lenguaje convencional (el binario) sobre soporte (cinta, disco), destinado a durar en el tiempo"[10].

Desde el punto de vista jurídico, la importancia de un documento es servir de medio de prueba. El artículo 368 del Código Procesal Civil de Costa Rica indica que son documentos

"… los escritos, los impresos, los planos los dibujos, los cuadros, las fotografías, las fotocopias, las radiografías, las cintas cinematográficas, los discos, las grabaciones magnetofónicas, los discos, y en general, todo objeto mueble que tenga carácter representantivo o declarativo".

Si bien es cierto esta definición no incluye expresamente la de documento electrónico, la Ley de Certificados, Firmas Digitales y Documentos Electrónicos de Costa Rica, Ley N. 8454, (en adelante LCDFDDE), aplica el principio de equivalencia funcional:

"*Cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático, se tendrá jurídicamente equivalente a los documentos que se otorguen, residan o transmitan por medios físicos.*

En cualquier norma del ordenamiento jurídico en la que se haga referencia a un documento o comunicación, se entenderán de igual manera tanto los electrónicos como los físicos. …"

Por su parte, el artículo 4 de la Ley de comentario indica:

"Los documentos electrónicos se calificarán como públicos o privados, y se les reconocerá fuerza probatoria en las mismas condiciones que a los documentos físicos."

Esta distinción es de gran relevancia ya que según sea el documento electrónico público o privado, deberá por un lado ser certificado (primer caso), y por otro lado se le aplican las consideraciones del artículo 369 y 370 del Código Procesal Civil. A manera de ejemplo, un archivo electrónico de una resolución de una institución de la Administración Pública no puede ser considerado documento electrónico público. Para ello, además de ser emitido por la Administración pública, requiere

"*tener garantía de identidad e integridad de la información, mientras que en el segundo, no existe tal seguridad, al no estar debidamente acreditada una firma electrónica que así lo garantice. Es entonces, la seguridad jurídica uno de los fundamentos distintivos del documento público electrónico, frente a otras manifestaciones de la conducta administrativa hechas mediante mecanismos informáticos. Esa seguridad jurídica se evidencia en las condiciones de inalterabilidad, accesibilidad y atribución. … Es así como la firma digital certificada busca garantizar las indicadas condiciones a la hora de emitir un documento público electrónico y por consiguiente,*

10 TERAMOND (Carmen) y otro. Concepto, valor jurídico y regulación de la firma digital en Costa Rica. Universidad de Costa Rica. Facultad de Derecho. Tesis para optar por el grado de Licenciadas en Derecho. 2002. P. 61.

de no contarse con dicho requisito legal, no podríamos estar en presencia de un documento con tal carácter, con todas las consecuencias jurídicas que ello conlleva. Hechas las anteriores consideraciones, procederemos a resolver sobre el fondo del caso sometido a nuestro conocimiento."[11].

2. LA FIRMA DIGITAL

La firma es una de las partes esenciales de todo documento, ya que identifica al autor de un documento quien asume la responsabilidad por su contenido[12].

La comunicación mediante medios electrónicos plantea el problema de cómo identificar al autor de un documento. Debido a ello surge el concepto de Firma Digital.

La doctrina diferencia la firma digital de la firma electrónica, diferencia que es importante desde el punto de vista práctico por el valor probatorio que se le da a cada una. La firma digital se basa en criptografía, por lo que se presume válida salvo que se demuestre lo contrario, pues hay de por medio mecanismos de verificación, normalmente, por parte de una entidad certificadora autorizada por el Estado. Firma electrónica es un concepto amplio que comprende cualquier carácter electrónico usado por alguien con el fin de autenticar un registro, por lo que abarca cualquier método de identificación. Es por ello que corresponde a quien introduce el documento como prueba demostrar su validez.

La legislación costarricense al igual que la de Brasil, no diferencia entre una y otra, aunque el contenido de las regulaciones es propio de la firma digital.

a. Característica de la firma digital

La firma digital tiene la misma finalidad que la firma manuscrita ya que expresa la identidad del autor y la autenticidad. Es el resultado de aplicar algoritmos de encriptación[13] a un conjunto de datos, que permite que un documento se traduzca a una serie numérica única mediante la utilización de un Algoritmo llamado Hash[14], y que solo son reconocibles por el destinatario quien podrá comprobar la identidad del remitente, la integridad del documento, autoría y autentificación.

11 Tribunal Contencioso Administrativo Sección Sexta, Segundo Circuito Judicial de San José. Sentencia N. 61- 2011- VI, de las 9:00 del 9 de marzo del 2011. En esta resolución, no se considera documento electrónico público un archivo pdf de una institución pública, localizado en un servidor para descarga del público en una página web, por no contar con firma digital certificada.

12 Cuervo Álvarez (José). La Firma digital y Entidades de Certificación. Informática y Derecho. Revista Iberoamericana de Derecho Informático: Contratación Electrónica, Privacidad e Internet, Mérida. En VEGA (Hannia) Los nuevos medios de comunicación: Su impacto jurídico sobre el concepto de documento y el Concepto de firma y su valor probatorio. Tesis para optar por el grado de Licenciada en Derecho. Facultad de Derecho de la Universidad de Costa Rica. 2003.

13 La criptografía es entendida como "la rama de las matemáticas aplicadas que se ocupa de transformar mensajes en formas aparentemente inteligibles y devolverlas a su forma original." DEVOTO (Mauricio). Comercio Electrónico y Firma Digital. La Ley, 2001

14 Es una construcción criptográfica usada para verificar la integridad y autenticidad de una firma digital. Su función es obtener una huella de un archivo, mensaje o datos, que permite su autenticación. Existe la llamada función hash unidireccional que permite generar un código a partir de un mensaje y así se genera un valor secreto único libre de colisiones. STALLING (William). Fundamentos de seguridad en redes. Aplicaciones y Estándares. Segunda Edición. Pearson Educación S.A. Madrid, 2004. P. 61.

La encriptación[15] por parte del emisor se realiza mediante su llave privada o secreta[16], mediante la cual el emisor firma el documento. Esta clave privada tiene asociada una clave pública que es la que permite al receptor desencriptar el mensaje y leerlo. Su seguridad radica en que la clave privada es absolutamente secreta y propia del autor del documento electrónico, así como en la certificación de la clave pública por la autoridad certificadora.

Esta característica es precisamente una de las diferencias entre la firma digital y manuscrita, ya que en la primera para cada documento electrónico se genera una firma digital única e irrepetible, mientras que en segunda, la firma tiene que ser el mismo rasgo identificador de la persona para todo documento que se firme[17].

La legislación costarricense define la firma digital como:

" *… cualquier conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico*". (artículo 8 de la LCFDDE[18])

"Una firma digital se considerará certificada cuando sea emitida al amparo de un certificado digital vigente, expedido por un certificador registrado."

La definición dada en el artículo 8 de la LCDFDDE es acorde con la necesidad de garantizar:

(i) La integridad del mensaje, es decir, que no se ha modificado el mensaje.

(ii) La autenticidad, es decir, la identificación del autor.

(iii) No repudio de tal manera que no se puede negar la autoría de un mensaje.

(iv) La neutralidad tecnológica, ya que no se excluye ninguna tecnología mediante la cual se pueda lograr cumplir con los anteriores características que debe reunir la Firma Digital.

El valor probatorio de la firma digital se encuentra en el artículo 9 y 18 de la LCDFDDE. Al respecto el artículo 18 de la LCDFDDE establece:

"Los documentos y las comunicaciones suscritos mediante firma digital, tendrán el mismo valor y la eficacia probatoria de su equivalente firmado en manuscrito. En cualquier norma jurídica que se exija la presencia de una firma, se reconocerá de igual manera tanto la digital como la manuscrita.

15 Actualmente se utiliza la criptografía de clave pública o encriptación asimétrica, en la que se generan dos llaves relacionadas matemáticamente entre sí: la privada y la pública.

16 Cfr. Revista de Ciencias Jurídicas 97: Vacíos legales en Costa Rica por el uso de la red: El "e-practice". Prof. Bernal Arias Ramírez. Universidad de Costa Rica y Colegio d Abogados de Costa Rica. Enero- Abril 2002.

17 Sobre el particular Diego Cruz explica el uso indebido de "firma" en la firma digital: CRUZ (Rivero). Definición y Naturaleza Jurídica de la Firma Electrónica. Marcial Ponds. Madrid, 2006.

18 En similar sentido se expresa el artículo 6 bis de la Ley Orgánica del Poder Judicial que regula los documentos electrónicos en la tramitación judicial, actos y resoluciones judiciales.

Los documentos públicos electrónicos deberán llevar la firma digital certificada."

Como se desprende de lo anterior, los documentos electrónicos privados con firma digital no certificada son válidos, sin embargo, corresponderá a las Partes comprobar que se cumple con los requisitos de la firma digital y que el mecanismo tecnológico utilizado es apto para ello.[19]. No obstante, si el documento electrónico privado cuenta con firma digital certificada, constituirá plena prueba, según así lo establece el artículo 18 de la LCDFDDE:

"Sin perjuicio de lo dispuesto en los artículos 3º, 9º y 19 de esta Ley, los certificados digitales expedidos por certificadores registrados ante la Dirección de Certificadores de Firma Digital, solo tendrán pleno efecto legal frente a terceros, así como respecto del Estado y sus instituciones."

Es importante indicar que en Costa Rica, la Administración Pública y alguna jurisprudencia ha utilizado indebidamente el término firma digital, para referirse a la firma manuscrita captada por un instrumento tecnológico, y guardada en algún formato de imagen que permite su reproducción en algún documento público, como la cédula de identidad o el pasaporte[20].

b. Certificados digitales

Los certificados digitales son documentos que prueban la vinculación entre una clave pública y una clave privada, y que buscan evitar el uso de la clave pública por parte de otras personas. El certificado es firmado digitalmente con la clave privada del emisor y normalmente contienen la clave pública asociada a esa clave privada, la identificación del signatario por su nombre o seudónimo, fecha de expiración, el nombre de la autoridad certificante que lo emite, la firma digital de la autoridad certificadora, lo datos de verificación de la firma del emisor (clave pública), límites de uso y de valor, entre otra información[21]. Su formato está definido por un estándar internacional denominado X.509 UIT-T que es utilizado por infraestructuras de claves públicas (PKI).

El artículo 11 de la LCDFDDE define certificado digital como:

"… el mecanismo electrónico o digital mediante el que se pueda garantizar, confirmar o validar técnicamente:

a) La vinculación jurídica entre un documento, una firma digital y una persona.

b) La integridad, autenticidad y no alteración en general del documento, así como la firma digital asociada.

19 Sobre este tema, la legislación española es muy clara en reconocer valor probatorio únicamente a los documentos con firma digital certificada, o como se le llama en el Ley 59/2003 Ley de Firma Electrónica, Firma Electrónica Reconocida.

20 Cfr. Sala Constitucional de la Corte Suprema de Justicia. Recurso de Habeas Corpus Voto N. 2005- 8862 de las 17:18 del 5 de julio del 2005; y Voto N. 2005- 0562, del 29 de abril del 2005. Sobre el tema, ver aclaración que hace la Sala Tercera de la Corte Suprema de Justicia, resolución N. 2009- 1296, del 14 de octubre del 2009.

21 MUÑOZ (Ramiro). Un Proyecto Español de Firma Electrónica. En Firma Digital y Administraciones Públicas. I Edición. Lerko Print S.A. Madrid, 2002. P. 109

c) La autenticación o certificación del documento y la firma digital asociada, únicamente en el supuesto del ejercicio de potestades públicas certificadoras. (…)".

Para ello es necesario la intervención de una tercera persona en la comunicación: la Autoridad Certificadora.

Debido a que este es un tercero de confianza en cuyas manos se deja la seguridad del sistema (la autenticidad del mensaje y la identificación de su autor, aunado al momento en que se entiende que la comunicación electrónica se ha efectuado), los diferentes ordenamientos jurídicos han establecido estrictas normas para garantizar la probidad de los prestatarios de estos servicios[22].

Entre los requisitos que establece la LCDFDDE están:

(i) Rendir garantía de fidelidad.

(ii) Contar con la tecnología y sistemas de seguridad.

(iii) Estar debidamente inscritos en la Dirección de Certificadores de Firma Digital del Ministerio de Ciencias y Tecnología.

(iv) Cumplir los requisitos técnicos fijados por la Entidad de Acreditación Nacional.

3. VALOR JURÍDICO DEL DOCUMENTO ELECTRÓNICO

En Costa Rica, el uso de documento electrónico es válido para todo acto jurídico, a menos que exista una disposición que indique lo contrario. El artículo 5 de la LCDFDDE le ha reconocido al documento electrónico pleno valor en los siguientes casos, sin la lista taxativa:

a. La formación, formalización y ejecución de los contratos.

Los mecanismos de seguridad asociados a la firma digital y los certificados digitales, fueron desarrollados originariamente para dar seguridad al intercambio de datos que se da en el comercio electrónico.

El internet ha permitido un aumento en la oferta de bienes y servicios, lo que se ha traducido en muchos casos, en variedad de bienes y servicios a costos menores de los ofrecidos en las tiendas físicas, debido a costos menores de intermediación, entre otros. Este fenómeno ha alcanzado las relaciones entre comerciante y consumidor, empresas entre sí, consumidores entre sí, y las relaciones de la Administración Pública con sus usuarios y proveedores.

Ejemplo de esto ultimo es la puesta en marcha en varios países de plataformas tecnológicas seguras que le permiten a los usuarios hacer trámites en línea, así como a proveedores de servicios contratar con el Estado.

22 RINCÓN (Erica). Manual de derecho comercial y de Internet. Centro Editorial Universidad del Rosario, Bogotá. 2006. P.233.

En Costa Rica, uno de los principales temas de seguridad en comercio electrónico se dio con los servicios bancarios por internet. Varias entidades bancarias han sido condenadas a pagar por sustracciones de dinero no autorizadas por los clientes, utilizando los servicios de "*ebanking*". De relevancia para el tema en estudio es la obligación que tienen las entidades bancarias de utilizar los mecanismos de seguridad más seguros para las transacciones bancarias por Internet, como lo sería la firma digital:

"Esto se extrae del testimonio del señor Sebiani, quien indicó que la Institución se encontraba trabajando en la implementación de sistemas de identificación basados en la firma digital, el cual fue postergado debido a la iniciativa que desarrolla otra institución gubernamental, y que en su lugar, se implementó la "clave dinámica", la cual constituye un factor adicional para verificar la identificación del cliente. De igual forma, la prueba evacuada tampoco permite acreditar que en el caso concreto se de la concurrencia de alguna causa eximente de responsabilidad de la cual se extraiga la ajenidad del demandado respecto del daño … El Tribunal fundamentó su fallo en la existencia de un riesgo con base en el cual imputa el daño al Banco, lo cual resulta acorde con lo manifestado, en su conjunto, por el testigo perito en cuanto a la seguridad informática. Por otro lado, en cuanto a las eximentes, el recurrente expone dos argumentaciones que se complementan. Por un lado, afirma, se debió aplicar la figura de la presunción o indicio, y concluir que la causa del daño fue ajena; y por el otro, que este se derivó de una acción u omisión, consciente o inconsciente de la víctima. Como ya se adelantó, no existen elementos que permitan desvirtuar la presunción de que la señora Arroyo Vargas es demandante de buena fe. En virtud de lo expuesto, a pesar de que se desprende del testimonio del señor Sebiani que la plataforma interna del Banco no fue vulnerada y que los sistemas de seguridad son adecuados para garantizar la integridad de las bases de datos, considera esta Sala que no hay casación útil, toda vez que no se acreditó ninguna causa eximente de responsabilidad"[23].

A partir de ese momento, muchos bancos han incluido diferentes tecnologías para garantizar la seguridad de las transacciones, incluso algunas basadas en firma digital como el "*token*".

De igual manera, la sentencia de comentario analizó las obligaciones de los usuarios del servicio de banca electrónica:

"*Así, no cabe duda que es su responsabilidad el garantizar el manejo adecuado de la clave de acceso, así como seguir las recomendaciones dadas por las entidades financieras en materia de seguridad. La decisión de ser beneficiario de estos servicios lleva aparejado un deber de diligencia que, en caso de ser incumplido, podría liberar de responsabilidad al prestatario. No resulta admisible, de acuerdo a los principios de razonabilidad y proporcionalidad, relevar al cliente de sus deberes de prudencia en aquellos aspectos que forman parte de su ámbito personal de control, como lo es el lugar donde realiza la conexión, así como utilizar equipos de cómputo adecuados y con los programas informáticos adecuados para garantizar la seguridad de la información*"

23 SALA PRIMERA DE LA CORTE SUPREMA DE JUSTICIA. Sentencia N. 300-F-S1-2009. San José, a las once horas veinticinco minutos del veintiséis de marzo de dos mil nueve. Cfr SALA PRIMERA DE LA CORTE SUPREMA DE JUSTICIA. Sentencia 827-S1-F-2009. San José, a las ocho horas del siete de agosto de dos mil nueve.

b. Comunicación judicial, conservación de expedientes judiciales y administrativos; recepción, práctica y evacuación de prueba

Previo a la publicación de la LCDFDDE, ya el artículo 6 bis de la Ley Orgánica del Poder Judicial establecía la posibilidad de utilizar documentos electrónicos en las comunicaciones judiciales.

En similar sentido, la Ley de Notificaciones Judiciales, Ley N. 8687, establece la posibilidad de fijar de manera permanente, un domicilio electrónico para efectos de recibir notificaciones:

"Las personas físicas y jurídicas interesadas podrán señalar al Poder Judicial, una dirección única de correo electrónico para recibir el emplazamiento y cualquier otra resolución, en cualquier asunto judicial en que deban intervenir. Esta fijación podrá ser modificada o revocada en cualquier tiempo, por la persona interesada."

Para la notificación por correo electrónico existen una serie de procedimientos regulados en esta misma Ley y en el Manual de Procedimientos de Comunicaciones por Medios Electrónicos de las Oficinas Judiciales.

Por su parte, el artículo 12 de esta Ley indica: "Quienes intervengan en un proceso podrán realizar gestiones ante el tribunal, a través de medios electrónicos, informáticos, telemáticos o de otra clase semejante, que permitan el envío de la comunicación y su normal recepción, en forma tal que esté garantizada su autenticidad, en la forma en que lo haya dispuesto el Consejo Superior del Poder Judicial.

Los medios electrónicos, informáticos, telemáticos o de otra clase semejante deberán ser accesibles a los lectores de pantalla para no videntes."

Para poder aplicar lo indicado en el artículo 12, se está en proceso de habilitar el expediente electrónico. Actualmente, el Poder Judicial se encuentra con un proyecto piloto en algunos Juzgados de Trabajo del país. No obstante, algunos despachos judiciales permiten la comunicación electrónica cuando se trate de incidencias menores del proceso judicial, tales como temas de coordinación.

c. La emisión de certificaciones, constancias y otros documentos.

Mediante el registro de los notarios en un sistema que llevaba el registro y el ingreso de una contraseña, era posible solicitar documentos al Registro e incluso terceras personas podían verificar el documento certificado mediante una clave que se daba para esos efectos.

d. La presentación, tramitación e inscripción de documentos en el Registro Nacional.

A la fecha esto no ha sido posible. No obstante, existe la posibilidad de presentar el reporte quincenal de instrumentos notariales autorizados mediante documento electrónico enviado al Archivo Nacional.

e. La gestión, conservación y utilización, en general, de protocolos notariales, incluso la manifestación del consentimiento y la firma de las partes[24].

Si bien la LCDFDDE permite que los documentos notariales sean electrónicos, hay gran discusión sobre si es posible aplicar esta normativa a esos documentos. La función notarial está regulada en el Código de Notariado, y conlleva la realización de una serie de formalidades y cumplimiento de mecanismos de seguridad físicos, en principio incompatibles con el documento electrónico. Tal es el caso del protocolo, que es el libro en el cual se realizan las escrituras públicas; papel de seguridad sobre el cual se tienen que imprimir los testimonios (copias de las escrituras) y certificaciones notariales, el uso de sello blanco, entre otros. De igual manera, el otorgamiento de las escrituras debe realizarse en presencia de las partes, lo cual en el caso del documento electrónico no necesariamente debe darse.

Para solventar estos obstáculos, se ha hablado de la posibilidad de usar un protocolo electrónico, así como de la firma digital notarial. A la fecha es poco lo que se ha hecho para implementar esta normativa en la función notarial.

f. Valor probatorio

Como indicamos al inicio, uno de los aspectos fundamentales del documento electrónico es el valor probatorio que tiene, de conformidad con la regulación de la prueba documental del Código Procesal Civil.

Es poco lo que se ha discutido al respecto en los tribunales de justicia, sin embargo, la jurisprudencia le ha reconocido valor probatorio a los documentos electrónicos:

"Sobre el valor probatorio de los documentos electrónicos, es necesario señalar que, se produjo un cambio radical con la promulgación de la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, de 30 de agosto de 2005, vigente desde el 30 de octubre de ese año. Basta con la trascripción de los siguientes preceptos para comprenderlo. (…) De lo anterior se desprende que, para todos los efectos pertinentes, los documentos electrónicos se asimilan a los escritos." [25]

Existen ciertos documentos que la Ley LCDFDDE expresamente indica que no pueden ser realizados electrónicamente. Tal es el caso de:

(i) Los actos o negocios en los que, por mandato legal, la fijación física resulte consustancial.

24 Cfr. HOCSMAN (Heriberto). Negocios en Internet. Editorial Astrea. Buenos Aires, 2005, p.388.

25 SALA PRIMERA DE LA CORTE SUPREMA DE JUSTICIA. Sentencia 000513-F-S1-2009. San José, a las diez horas del veintisiete de mayo de dos mil nueve.

(ii) Las disposiciones por causa de muerte.

(iii) Los actos y convenios relativos al Derecho de familia.

(iv) Los actos personalísimos en general.

4. EFECTOS PRÁCTICOS

Le equiparación del documento electrónico al documento tradicional, ha tenido importantísimos efectos en el aumento en la competitividad de los países[26] que incentivan el uso de las tecnologías como instrumentos de trabajo asociadas a amplia cobertura de Internet, ya que permite eficientizar el trabajo, disminuir costos administrativos, e incluso, impactos ambientales ante la disminución de papel y de costos ambientales de transporte.

a. Gobierno digital

El Gobierno Digital se refiere al uso creativo de las tecnologías de información para transformar la manera como interactúa el Gobierno con las empresas y los ciudadanos. Es una forma de modernizar al Estado, simplificando y haciendo más eficiente la prestación de servicios y la realización de trámites en la administración pública[27].

En este momento diferentes entidades en el país utilizan firma digital, ya sea para trámites como administración de justicia, ciudadanos o del gobierno central, además de comercio o mercados electrónicos. Entre ellas, entidades financieras, como bancos, cooperativas y mutuales o instituciones del Estado como la Contraloría General de la República (CGR), el Poder Judicial, el Ministerio de Hacienda (Comprared), Merlink (compras del Estado), la Compañía Nacional de Fuerza y Luz (CNFL), la Caja Costarricense de Seguro Social (CCSS), entre otras.

b. Teletrabajo y decisiones de jerarca a distancia

El término "teletrabajo" refiere a la posibilidad de que el trabajo se realice en un lugar diferente del que se ocupa cuando la persona lo está realizando normalmente. Se utilizan medios informáticos para comunicarse durante la realización de la actividad, lo que permite el envío de insumos y resultados.

La ausencia física del sitio de trabajo se suple con los medios informáticos y telemáticos, lo que permite que el trabajador permanezca en su casa, sin tener que desplazarse al sitio de trabajo, no obstante, la información sí se desplaza por medio de tecnología.

El teletrabajo es un sistema que se utiliza mucho en empresas privadas, y que en Costa Rica ha sido considerado una medida de importancia para cumplir metas ambientales de reducción de carbono.

No obstante, en la función público pareciera ser más problemático. Si bien es cierto no es propiamente teletrabajo, muchos funcionarios realizan labores fuera de sus oficinas debido a que tienen que atender compromisos de la Administración Pública en otras áreas del país, o bien fuera del país. Podrá un funcionario público tomar una decisión no estando presente en el país? Al respecto,

26 Cfr. http://www.toc.cl/?p=162 .

27 http://www.gobiernofacil.go.cr/e-gob/gobiernodigital/quienessomos.htm

la Procuraduría General de la República ha abordado el tema de la siguiente manera:

"*La adopción de una decisión a distancia está ligada a aspectos de autenticidad y seguridad, particularidad que se plantea por el uso de los medios electrónicos. Cómo determinar que la decisión que se ha adoptado en el exterior ha sido efectivamente adoptada por el funcionario competente y su contenido corresponde a la voluntad del mismo? El punto es si solventados estos otros problemas de autenticidad del acto, inalterabilidad de la decisión, el Regulador puede adoptar una medida de las previstas en el artículo 57 de la Ley de la ARESEP estando en el exterior. … El artículo 5 de la Ley 8454 de 30 de agosto de 2005, Ley de Certificados, Firmas Digitales y Documentos Electrónicos, en forma expresa, indica que la utilización de los documentos electrónicos es válida para la tramitación, gestión y conservación de expedientes administrativos, lo que incluye la recepción, práctica y conservación de prueba, incluida la recibida por archivos y medios electrónicos. El uso del expediente electrónico solo sería inválido si la ley impone la fijación física. En consecuencia, un procedimiento puede ser tramitado electrónicamente. … Y aún en el caso de que el expediente no sea tramitado electrónicamente, determinados documentos pueden ser producidos o tramitados electrónicamente. Hacemos alusión a archivos y documentos electrónicos.*"[28]

Como se desprende de lo anterior, la LCDFDDE claramente permite no solo la tramitación de un expediente administrativo de manera electrónica, sino también que el acto administrativo final sea electrónico, pero debe tener firma digital certificada, por ser un documento público.

c. Medio para lograr objetivos ambientales

Uno de los efectos prácticos que tiene la utilización de los documentos electrónicos es la utilización de menos recursos. Es por ello que con el objetivo de compensar la huella de carbono, muchas empresas han incentivado el uso de expedientes electrónicos, documentos electrónicos[29], teletrabajo, entre otros, como parte de las medidas para compensar su huella de carbono[30].

Los desarrollos tecnológicos y el derecho son productos de la sociedad[31]. No obstante, el derecho se adapta más lentamente que la tecnología a los requerimientos sociales. A pesar de que puede existir una necesidad social, siempre hay cierta resistencia de los operadores jurídicos de modificar las instituciones tradicionales para adaptarla a las nuevas necesidades, especialmente cuando en la cultura costarricense "los papelitos hablan", y se dan cuestionamientos de ciertos sectores sobre la seguridad que las tecnologías puedan dar. No obstante, en la medida en que la tecnología se haga más accesible y se incrementen los niveles de seguridad, es posible que demos un vuelco a la prevalencia del documento electrónico sobre el papel.

28 PROCURADURÍA GENERAL DE LA REPÚBLICA. Dictamen N. 358 del 3 de octubre del 2007.

29 REED, (Kristin). Haciendo lo correcto: Guía para responsabilizarnos de las emisiones de gases efecto invernadero de CARE. Nairobi, 2007. Online: http://www.careclimatechange.org/files/CARE_docs/CARE_Going_Carbon_Neutral_SP.pdf.

30 Para algunos, el uso de las tecnologías implica más bien un aumento de la huella, ya que debe considerarse un efecto acumulado de la producción de los productos tecnológicos aunado a los requerimientos energéticos para su funcionamiento. Actualmente, el sector de las Tecnologías de la Información representa alrededor del 2% de las emisiones de gases efecto invernadero en el mundo. Con el fin de contrarrestar esto, se ha llevado a la tendencia o concepto del Green TIC.

31 Cfr. HACKETT (Edward) y otros. The Handbook of Science and Technology Studies. Tercera edición. MIT Press. London, 2008.