Derecho y Tecnología

Revista arbitrada de Derecho y Nuevas Tecnologías
Editada por el Vicerrectorado Académico
Decanato de Investigación y Postgrado
Universidad Católica del Táchira

Editor-Director
Mariliana Rico Carrillo

Consejo de Redacción

Rafael ILLESCAS ORTÍZ (Universidad Carlos III de Madrid); Isabel RAMOS HERRANZ (Universidad Carlos III de Madrid); Apolonia MARTÍNEZ NADAL (Universidad de las Islas Baleares); Leopoldo BRANDT GRATEROL (Universidad Católica Andrés Bello); Antonio SÁNCHEZ RODRÍGUEZ (Universidad Carlos III de Madrid); José Ovidio SALGUEIRO (Universidad Católica Andrés Bello); Miguel ARRIETA ZINGUER (Universidad Católica del Táchira); David LÓPEZ JIMÉNEZ (Universidad Autónoma de Chile); María PÉREZ PEREIRA (Universidad Carlos III de Madrid). Emilio SUÑÉ (Universidad Complutense de Madrid). José Luis BARZALLO (Universidad Andina Simón Bolívar de Ecuador).

Diseño Gráfico
Nina Gabriela Vásquez

Montaje
Edy Marleni Lozano

Identificación Legal
Depósito Legal: p.p. 200202TA1209
ISSN: 1317-9306
Periodicidad: Anual

Publicación registrada en el *Catálogo Latindex*
www.latindex.org

Revista indizada en REVENCYT: Índice y Biblioteca Electrónica de Revistas Venezolanas de Ciencia y Tecnología. Código RVD012

Revista Derecho y Tecnología
Número 15
Edición 2014

Dirección:
Carrera 14 con calle 14
Apartado 366
San Cristóbal
Estado Táchira
Venezuela

Teléfonos:
(58) (0276) 344.75.72 -90.83
Fax:
(058) (0276) 344.61.83
E-mail:
derechoytecnologia@ucat.edu.ve
mrico@ucat.edu.ve

Distribución:
Universidad Católica
del Táchira
Apartado 366
San Cristóbal
Estado Táchira
Venezuela

Derecho y Tecnología

Revista arbitrada de Derecho y Nuevas Tecnologías
Editada por el Vicerrectorado Académico
Decanato de Investigación y Postgrado
Universidad Católica del Táchira

Misión

Derecho y Tecnología es una revista científica con periodicidad anual que tiene como misión difundir los trabajos de expertos nacionales e internacionales dedicados al estudio de los avances tecnológicos y jurídicos en general, con especial énfasis en las modificaciones que produce la aplicación de las Tecnologías de la Información y la Comunicación (TIC) en el campo del Derecho, fenómeno que ha dado origen al nacimiento de una nueva área de investigación jurídica.

En cada número se ofrece una publicación que contiene artículos doctrinales, recopilación de legislación nacional e internacional y la jurisprudencia nacional más destacada en la materia. La revista está dirigida a abogados, ingenieros, académicos, estudiantes y otros profesionales interesados en el estudio del impacto de las TIC en el ámbito jurídico.

A través de esta iniciativa editorial, la Universidad Católica del Táchira abre una vez más sus puertas a la investigación, con la finalidad de proporcionar un medio adecuado de difusión en esta área.

Universidad Católica del Táchira

Revista Derecho y Tecnología **15/2014**
Vicerrectorado Académico
Decanato de Investigación y Postgrado

ÍNDICE

Artículos

Reseña Legislativa

Legislación

Jurisprudencia

DOCTRINA

Transparencia vs. privacidad en el acceso y transferencia de información

Nayibe Chacón Gómez*

SUMARIO: I. Presentación y delimitación del tema. II. Contenido y alcance del Decreto No. 9.051, mediante el cual se dicta el Decreto con Rango, Valor y Fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado. III. La protección de la privacidad de los datos, información y documentos de los particulares que se encuentran en los órganos y entes del Estado. IV. Conclusiones.

Resumen

El término "transparencia" es utilizado especialmente para referirse a la necesidad que tienen los ciudadanos de conocer la gestión de la Administración Pública, principalmente en cuanto al uso que se hace de los recursos del Estado. La privacidad de la información es un derecho que tienen los ciudadanos frente a los demás ciudadanos y frente a los órganos y entes del Estado. En este trabajo, se analizan estos dos términos a la luz del Decreto venezolano con rango, valor y fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado.

Palabras clave: Privacidad de la información. Transparencia. *Open Data*. Interoperabilidad.

Abstract

The term "transparency" is used especially to refer to the citizen's need of knowing the management of the Public Administration, principally for the use that is done of the resources of the State. Information privacy is a right that the citizens have, with regards to other citizens and to the entities of the State. These two terms are analyzed in this paper under Venezuelan "Decreto con rango, valor y fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado".

Keywords: Privacy of the information. Transparency. Open Data. Interoperability.

Recibido: 4/11/2013 • Aceptado: 16/1/2014

* Profesor Asociado de la Facultad de Ciencias Jurídicas y Políticas. Universidad Central de Venezuela. nayibe.chacon@ucv.ve

I. Presentación y delimitación del tema

En Venezuela, las Tecnologías de Información y Comunicación (TIC) han revestido no solamente el carácter de hecho social[1] sino también se han agregado al catálogo de derechos de los ciudadanos. En la Constitución de la República Bolivariana de Venezuela del año 1999, se incorporaron normas sobre el empleo de las TIC como herramientas para el desarrollo del país.

Desde la promulgación de estas normas constitucionales y su proyección en la legislación nacional, el actual Ministerio del Poder Popular para la Ciencia y Tecnología ha sido el encargado de delinear la implementación de las TIC en todos los ámbitos nacionales, aunque no se encuentra solo en esta tarea de creación e implementación del *gobierno electrónico*[2] venezolano.

El 15 de junio de 2012 apareció publicado en la Gaceta Oficial de la República Bolivariana de Venezuela No. 39.945 el Decreto No. 9.051 el Decreto con

1 El empleo en todos los ámbitos de nuestra vida de los medios electrónicos, han dado lugar a que nuestra sociedad sea conocida como una "Sociedad de la Información y del Conocimiento", la cual conjuga por una parte, el concepto de Sociedad, y por otra parte, el concepto y alcance de las Tecnologías de Información y Comunicación. Por "sociedad", puede entenderse en el concepto tradicional citando a Rafael Gamboa, como la integración de "una serie de individuos, quienes reunidos en mismo espacio, acuerdan someterse a una serie de normas y, a cambio, obtendrán una serie de derechos. En este concepto de sociedad tradicional, unos son los que gobiernan, y otros son los gobernados". Y el autor Anthony Giddens, escribe en su obra *Sociología*, que sociedad «es un sistema de interrelaciones que conecta a los individuos entre sí". Por otro lado, las Tecnologías de Información y Comunicación se han definido "como sistemas tecnológicos mediante los que se recibe, manipula y procesa información, y que facilitan la comunicación entre dos o más interlocutores…las Tecnologías de Información y Comunicación son algo más que informática y computadoras, puesto que no funcionan como sistemas aislados, sino en conexión con otras mediante una red". GAMBOA BERNATE, Rafael Hernando: "Soberanía estatal en Internet; análisis desde la perspectiva de conflictos de jurisdicción y competencia en el plano nacional e internacional" en *Comercio Electrónico*, Legis Editores, S.A, Bogotá, 2005, p. 635. GIDDENS, Anthony. *Sociología*, Alianza Editorial, Tercera Reimpresión de la Segunda Edición, Madrid, 1997. Naciones Unidas, Comisión Económica Para América Latina y El Caribe – CEPAL. *Los Caminos hacia una Sociedad de la Información en América Latina y el Caribe*, Conferencia Ministerial Regional Preparatoria de América Latina y el Caribe para la Cumbre Mundial de la Sociedad de la Información. Bávaro, Punta Cana, República Dominicana, 29 al 31 de enero de 2003, p. 3.

2 A lo largo de esta investigación se citan otras definiciones de gobierno electrónico, no obstante, resulta oportuno anotar en esta presentación el concepto esclarecedor y descriptivo de la Prof. Mariliana Rico Carrillo, "*Cuando hablamos de gobierno electrónico, (e-goverment en terminología anglosajona) nos referimos a la utilización de las TIC, en particular de Internet, en los diferentes sectores del ámbito gubernamental como elemento de modernización de la gestión administrativa, que permite mejorar la prestación de servicios y facilita el contacto directo con los ciudadanos, a través de canales de comunicación que potencian su participación en el sector público*". RICO CARRILLO, Mariliana: "Las Tecnologías de las Información y Comunicación en la actividad gubernamental: gobierno electrónico y participación ciudadana", en: *Ciudadanas 2020 El Gobierno de la Información*, Instituto Chileno de Derecho y Tecnologías. Federación Iberoamericana de Derecho Informático (FIADI), Chile, 2011, pp. 208-209.

Rango, Valor y Fuerza de *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado,* el cual entró en vigencia el 15 de junio de 2014, fecha en que se venció el plazo de dos años contado a partir de dicha publicación en la Gaceta Oficial[3].

El objeto de este Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado* se encuentra consagrado en el artículo 1° en los siguientes términos: "*establecer las bases y principios que regirá el acceso e intercambio electrónico de datos, información y documentos entre los órganos y entes del Estado*[4]*, con el fin de garantizar la implementación de un estándar de interoperabilidad*", misión que intenta cubrir en 65 artículos, 4 disposiciones finales y 3 disposiciones transitorias.

En vista de que la presente investigación no podrá abarcar el conjunto de artículos, disposiciones finales y transitorias con que cuenta el Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado,* nos dedicaremos al estudio de la relación existente entre "la obligación que tienen los *órganos y entes del Estado a permitir el acceso e intercambio electrónico de datos, información y documentos*" y "*el derecho que tienen los ciudadanos a la protección de la privacidad*", específicamente en atención a la información personal de los particulares que se encuentra en posesión de estos órganos y entes del Estado en calidad de autores de la misma; es decir, datos que han sido generados por órganos y entes del Estados sobre la base de la información aportada por los ciudadanos.

3 *Decreto Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes,* Disposición Final Cuarta. "*El presente Decreto entrará en vigencia vencido el plazo de dos años contado a partir de la publicación del presente Decreto con Rango, Valor y Fuerza de Ley en la Gaceta Oficial de la República Bolivariana de Venezuela*".

4 Según el artículo 2° del *Decreto Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes,* estos "*órganos y entes del Estado*", son: 1. Los órganos del Poder Público Nacional, Estadal y Municipal. 2. Los institutos públicos nacionales, estadales, distritales y municipales. 3. El Banco Central de Venezuela. 4. Las Universidades públicas nacionales autónomas y experimentales, así como cualquier otra institución del sector universitario de naturaleza pública. 5. Las demás personas de derecho público nacionales, estadales, distritales y municipales. 6. Las sociedades de cualquier naturaleza en las cuales las personas a que se refieren los numerales anteriores tengan una participación en su capital social superior al cincuenta por ciento (50%), las que se constituyan con la participación de aquellas, o que a través de otro mecanismo jurídico, tengan el control de sus decisiones. 7. Las fundaciones y asociaciones civiles y demás instituciones creadas con fondos públicos, o que sean dirigidas por las personas a que se refieren los numerales anteriores, o en las cuales tales personas designen sus autoridades, o cuando los aportes presupuestarios o contribuciones efectuados en un ejercicio, por una o varias de las personas a que se refieren los numerales anteriores, representen el cincuenta por ciento (50%) o más de su presupuesto. 8. Los demás entes de carácter público.

II. Contenido y alcance del Decreto No. 9.051, mediante el cual se dicta el Decreto con Rango, Valor y Fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado

Resulta necesario considerar el núcleo del Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado*, el cual se encuentra en la "*implementación de un estándar de interoperabilidad*"; es decir, la creación y puesta en marcha de especificaciones técnicas, aceptadas por la industria, que permitirá a los órganos y entes del Estado el intercambio por medios electrónicos de datos, información y documentos de acceso público.

Cuando se habla de *interoperabilidad*, se hace referencia a la necesidad que tiene la Administración Pública de compartir e intercambiar información de los procedimientos que son realizados o llevados en cada una de sus dependencias, de conformidad con su propia naturaleza.

En opinión de la autora Yarina Amoroso Fernández:

> La interoperabilidad dentro del Estado es hoy en día un nudo operacional si se quiere mejorar su eficiencia. Existen factores que impulsan o aletargan implementar un sistema de interoperabilidad, con capacidad para usar datos u orquestar funcionalidades con otro sistema o proceso adhiriendo estándares comunes[5].

Continua la citada autora destacando que la planificación de la *interoperabilidad* forma parte de las políticas públicas y que debe emanar de la confianza a las instituciones públicas a modo de poder gestionar adecuadamente los procesos del Estado.

Así la *interoperabilidad* entre los distintos órganos y entes del Estado que permita el acceso o la transmisión de datos, información y documentos se presenta como el elemento imprescindible del llamado *Open Data*; es decir, del

> …compromiso del Estado de exponer los datos públicos que obran en su poder de forma reutilizable, con el fin de optimizar el uso de la información pública en función de un mejor servicio a la ciudadanía y una mejor gestión de gobierno así como que terceros puedan crear servicios derivados de los mismos datos[6].

5 AMOROSO FERNANDEZ, Yarina. "Open Data: una contribución necesaria al gobierno electrónico y la sociedad del conocimiento", en: *Ciudadanas 2020 El Gobierno de la Información.* Instituto Chileno de Derecho y Tecnologías. Federación Iberoamericana de Derecho Informático (FIADI), Chile, 2011, p. 15.

6 AMOROSO FERNANDEZ, Yarina. "Open Data:…", *ob. cit*., p. 11.

En el Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado* se estructura la *Plataforma Nacional de Servicios de Información Interoperables*; es decir, una plataforma tecnológica que busca el cumplimiento de la obligación que tienen los órganos y entes del Estado de implementar servicios de información interoperables, a fin de permitir el acceso e intercambio electrónico de datos, información y documentos, a cualquier órgano y ente del Estado que lo requiera.

El desarrollo, operación, mantenimiento y administración de dicha plataforma se encuentra a cargo del *Operador de la Interoperabilidad*, ente cuya finalidad es la de estandarizar, formalizar, integrar, reutilizar y compartir, por medios electrónicos, entre los órganos y entes del Estado, los datos, información y documentos que éstos poseen conforme a sus atribuciones, de acuerdo al principio de unidad orgánica y demás principios aplicables a la interoperabilidad[7].

El *Operador de la Interoperabilidad* forma parte del "*Comité Nacional de Interoperabilidad*"[8], el cual es dependiente administrativamente de la Vicepresidencia Ejecutiva, y es el encargado de "*establecer y coordinar la aplicación de los principios y políticas para el acceso e intercambio electrónico de datos, información y documentos entre los distintos órganos y entes del Estado*"[9].

A tenor del contenido del Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado*, la *interoperabilidad* es una herramienta que garantiza el desarrollo de los servicios públicos integrados y transparentes, así como, la simplificación de los trámites administrativos que sus órganos y entes ejecutan en atención a los requerimientos de los ciudadanos, en pro de la satisfacción de sus necesidades y mejora de las relaciones de éstos con el Estado, en tal sentido la *interoperabilidad* se presenta como de "interés público", y como uno de los elementos necesarios para el desarrollo de los cometidos del *gobierno electrónico*[10] en Venezuela.

7 Artículos 18 y ss., del Decreto Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado.

8 El Comité Nacional de Interoperabilidad se encuentra conformado por: 1. La Vicepresidencia Ejecutiva de la República, quien lo preside. 2. El Consejo Federal de Gobierno. 3. El Ministerio del Poder Popular con competencia en planificación. 4. El Ministerio del Poder Popular con competencia en tecnologías e información. 5. La Procuraduría General de la República. 6. La Asamblea Nacional. 7. El Tribunal Supremo de Justicia. 8. El Consejo Nacional Electoral. 9. El Consejo Moral Republicano. 10. El Banco Central de Venezuela. 11. El Operador de la Interoperabilidad.

9 Artículos 14 y ss., del Decreto Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado.

10 Las expresiones "Gobierno electrónico" y "Administración Electrónica" son definidas en la Carta Iberoamericana como sinónimas, ambas consideradas como el uso de las TIC en los órganos de la Administración para mejorar la información y los servicios ofrecidos a los ciudadanos,

Así, la *interoperabilidad* busca apoyar la función y gestión pública que desarrollan los órganos y entes del Estado, garantizando la cooperación y colaboración requerida para proporcionar servicios y procesos públicos integrados complementarios y transparentes, con el empleo de licencias tecnologías de propiedad abierta, que haría posible la reutilización de los datos, información y documentos generados, sobre la base del principio de la unidad orgánica de las instituciones que conforman la Administración Pública; es decir, la integración de éstas, que permitan alcanzar el máximo provecho de la función pública, en beneficio de los ciudadanos.

Debemos tener presente que en Venezuela desde la entrada en vigencia del Decreto No. 3.390 de fecha 23 de diciembre de 2004, publicado en la Gaceta Oficial No. 38.095 de fecha 28 de diciembre del mismo año, conocido como el "*Decreto del Software Libre*", se estableció como una obligación de la Administración Pública venezolana la utilización de programas de computación cuya licencia garantiza al usuario acceso al código fuente del programa y lo autoriza a ejecutarlo con cualquier propósito, modificarlo y redistribuir tanto el programa original como sus modificaciones en las mismas condiciones de licenciamiento acordadas al programa original, sin tener que pagar regalías a los desarrolladores previos.

En el artículo 1° de este *Decreto del Software Libre* se establece*: "La Administración Pública Nacional empleará prioritariamente Software Libre desarrollado con Estándares Abiertos, en sus sistemas, proyectos y servicios informáticos. A tales fines, todos los órganos y entes de la Administración Pública Nacional iniciarán los procesos de migración gradual y progresiva de éstos hacia el Software Libre desarrollado con Estándares Abiertos*". La justificación del empleo prioritario del Software Libre en la Administración Pública venezolana, ha sido descrita en los siguientes términos: "Dada la alta demanda y calidad de las habilidades en TI, el software que adquiere el Gobierno debe: a) ser predecible en su comportamiento y *performance*; b) tener un costo razonable de mantenimiento; c) ser de razonable esfuerzo para Integrarlo, evolucionarlo, adaptarlo; y, d) ser seguro"[11].

De igual manera, resulta meridianamente claro que actualmente los órganos y entes del Estado venezolano se encuentran inmersos en un proceso de digitalización y automatización de sus procedimientos, cuestión de la que se

orientar la eficacia y eficiencia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación de los ciudadanos. Todo ello, sin perjuicio de las denominaciones establecidas en las legislaciones nacionales.

11 BERRIZBEITIA, Jorge. Políticas de uso de Software Libre en el Sector Público Venezolano. Centro Nacional de Tecnologías de Información (CNTI), [En línea]. [Citado: 27. Enero. 2005, Disponible en: http://www.cnti.gob.ve/cnti_docmgr/sharedfiles/Politicas_Uso_Software_Libre_Sector_Publico_Vzla.pdf

derivan consecuencias de diversa índole, tanto desde la perspectiva del ciudadano como de la perspectiva de la misma Administración[12].

Por otra parte, resulta oportuno anotar que, no obstante, la consagración en el Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado*, del derecho que tienen todos los ciudadanos de estar informados de manera oportuna, adecuada y efectiva sobre los servicios desarrollados por el Estado para la eficaz y eficiente prestación de los mismos[13], y que en el texto del mencionado Decreto-ley se utilice la palabra "*transparencia*", no se refiere al derecho constitucional que tienen los ciudadanos al acceso a los archivos y registros administrativos, que se traduce en la obligación del Estado de poner a la disposición de los ciudadanos dicha información, conservando los límites aceptables dentro de una sociedad democrática en materias relativas a seguridad interior y exterior, a investigación criminal y a la intimidad de la vida privada, de conformidad con la ley que regule la materia de clasificación de documentos de contenido confidencial o secreto, de conformidad con lo establecido en el artículo 143[14] de la Constitución de la República Bolivariana de Venezuela[15].

12 "La utilización de las nuevas tecnologías en la actividad administrativa supone un cambio de paradigma de gran trascendencia, en primer lugar, para el ciudadano. La implantación de la Administración electrónica ofrece la posibilidad de ejercer vía *online*, durante las 24 horas del día, todos los días del año y sin limitaciones geográficas, el catálogo de derechos del que tradicionalmente ha sido titular, según la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en adelante LRJAP-PAC). Sin ánimo de ser exhaustivos: el derecho al conocimiento sobre el estado de la tramitación de los procedimientos en los que ostente la calidad de interesado, el derecho a la obtención de copias electrónicas de los documentos que obren en el expediente, el derecho a formular alegaciones y a aportar documentos en cualquier fase del procedimiento, son algunos de los mencionados derechos". ALAMILLO, Ignacio y Erika Henao Hoyos. "La gestión electrónica de la identidad y de la firma electrónica en el intercambio electrónico de datos entre Administraciones Públicas", [En línea]. AR: *Revista de Derecho Informático* No. 121 - Agosto del 2008. Disponible en: http://www.buscalegis.ufsc.br/revistas/files/anexos/29615-29631-1-PB.pdf

13 Decreto Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado, artículo 8°.- "*Las Oficinas de Atención al Ciudadano de los órganos y entes del Estado, deberán suministrar y ofrecer a los ciudadanos, de forma oportuna, adecuada y efectiva; información sobre los servicios desarrollados por el Estado para la eficaz y eficiente prestación de sus servicios*". **Y artículo 9**°.- "*Los ciudadanos, en forma individual o colectiva, directa, por medios de sus representantes o a través de la comunidad organizada; podrán presentar física o electrónicamente ante las Oficinas de Atención al Ciudadano de los organismos y entes del Estado; peticiones, sugerencias, reclamos, quejas o denuncias en la prestación de servicios públicos o por la irregularidad de la actuación de los servidores públicos en los términos de ésta y otras leyes aplicables*".

14 Constitución de la República Bolivariana de Venezuela, artículo 143.- "*Los ciudadanos y ciudadanas tienen derecho a ser informados e informadas oportuna y verazmente por la Administración Pública, sobre el estado de las actuaciones en que estén directamente interesados e interesadas, y a conocer las resoluciones definitivas que se adopten sobre el particular. Asimismo,* ***tienen acceso a los archivos y registros administrativos, sin perjuicio de los límites aceptables dentro de una sociedad democrática en materias relativas a seguridad interior y exterior, a***

En el contexto de la citada norma constitucional y como función del gobierno electrónico y del *Open Data*, la *transparencia* debe ser entendida como

> …el ejercicio de solicitar y entregar la información. Formar una cultura de transparencia es que las autoridades rindan cuentas a los gobernados de las decisiones que realizan en la función pública y crear una cultura ciudadana de participación, respeto y ejercicio del derecho de acceso a la información pública[16].

Dicha actuación de la Administración Pública, a tenor de lo establecido en la *Carta Iberoamericana de Gobierno Electrónico*, se encuentra fundamentada en el "*Principio de transparencia y accesibilidad*", según el cual se garantiza que la información de las Administraciones Públicas y el conocimiento de los servicios por medios electrónicos se haga en un lenguaje comprensible según el perfil del destinatario.

Por el contrario, como se ha mencionado, este novedoso Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado*, sólo atiende a la necesidad de crear la *Plataforma Nacional de Servicios de Información Interoperables*; es decir, el acceso y transmisión de datos, información y documentos entre los órganos y entes del Estado.

investigación criminal y a la intimidad de la vida privada, de conformidad con la ley que regule la materia de clasificación de documentos de contenido confidencial o secreto. *No se permitirá censura alguna a los funcionarios públicos o funcionarias públicas que informen sobre asuntos bajo su responsabilidad*". (Destacados nuestros).

15 La situación de la *transparencia* de las actividades de las dependencias de la Administración Pública en Venezuela ha sido descrito por Mercedes De Freitas en su trabajo titulado: "El acceso a la información pública en Venezuela. Transparencia vs. Opacidad", donde se destacan las siguientes percepciones: "*Identificamos un problema grave de acceso, veracidad, oportunidad e inexistencia de la información en poder de una gran parte de las instancias del Estado venezolano. Y nos referimos no sólo a información militar o de seguridad del Estado. Carecemos de información de uso común en cualquier Estado democrático, por ejemplo, sobre el presupuesto, la inversión en programas sociales, sus responsables y objetivos, entre otros puntos. Carecemos de la información sobre muchos datos e indicadores y existe desconfianza de otros, como los indicadores de mortalidad infantil y mortalidad materna, pues la data no concuerda con otros registros. La información sobre los sueldos de los funcionarios públicos se considera confidencial en Venezuela… El bloqueo a la información pública toma formas diversas en Venezuela. Una de ellas es negar el acceso a las fuentes*". La autora reconoce que en las Oficinas de Atención al Ciudadano, particularmente de la Contraloría General de la República, existía desde antes de la publicación del Decreto Ley bajo análisis, la posibilidad de realizar denuncias contra funcionarios o procesos, pero en ningún caso se contemplaba el acceso para los ciudadanos a la información actualizada de los asuntos llevados por ese órgano, menos aun "*sobre la utilización de los bienes y el gasto de los recursos que integran el patrimonio público, y cuya administración le corresponde*". DE FREITAS, Mercedes. *El acceso a la información pública en Venezuela. Transparencia vs. Opacidad,* Editorial CEC, S.A., primera edición, Caracas, 2010, pp. 29-31.

16 GARCÍA BARRERA, Mirna. "La información pública es de todos", en: *Ciudadanas 2020 El Gobierno de la Información*, Instituto Chileno de Derecho y Tecnologías, Federación Iberoamericana de Derecho Informático (FIADI), Chile, 2011, p. 79.

En materia de acceso a la información pública y transparencia, la autora Mercedes De Freitas se refiere, de manera muy precisa, al hecho que en fecha 26 de octubre de 2008, la Coalición ProAcceso intentó, sin éxito, entregar una propuesta de Ley de Acceso a la Información Pública a la Comisión de Ciencias, Tecnología y Medios de Comunicación de la Asamblea Nacional venezolana[17].

Con la publicación del Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado* no podemos decir que se haya cumplido con la tarea de crear un marco normativo que permita el acceso a la información pública y como consecuencia la *transparencia* de la gestión de la Administración Pública; sin embargo, su implementación se presenta como un paso para la articulación entre los órganos y entes del Estado, que permita dar cumplimiento a los mandatos constitucionales.

III. La protección de la privacidad de los datos, información y documentos de los particulares que se encuentran en los órganos y entes del Estado

Hechas las anteriores precisiones sobre el Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado*, lo siguiente en que puedo pensar es en algo que leí de un artículo escrito en el año 2004 por un autor español:

> …las Nuevas Tecnologías pueden facilitar muchos trámites administrativos y mejorar la gestión de los servicios públicos, pero también deben tenerse en cuenta las consecuencias que conlleva que cualquier Administración tenga acceso a datos que, en principio, no les corresponde conocer[18].

El autor de la noticia jurídico-informática continuaba en los siguientes términos:

> Puede parecer algo alarmista, pero lo cierto es que muchas veces no somos conscientes del control y la vigilancia a la que estamos o podemos estar sometidos, ni de la importancia que tiene el derecho a la *autodeterminación informativa*, que puede ser definido como la facultad de ejercer el control sobre los datos referentes a nuestra persona contenidos en ficheros o registros públicos o privados, normalmente procesados por medio de dispositivos informáticos. A parte de los conocidos derechos que confiere en relación con dichos ficheros (acceso, rectificación o cancelación) y el de oposición al tratamiento de los datos, la Ley Orgánica de Protección de Datos establece el derecho a la impugnación de valoraciones o decisiones "*cuyo único fundamento*

17 DE FREITAS, Mercedes. *El acceso a la información…, ob. cit*., p. 31.

18 PRENAFETA RODRÍGUEZ, Javier. "La privacidad en el gobierno electrónico y el DNI digital", [En línea], Noticias Jurídicas, Marzo, 2004. Disponible en: http://noticias.juridicas.com/articulos/20-Derecho%20Informatico/200403-305591621042750.html

> *sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad*". Este derecho, que tan poco se ejerce –el requerimiento de *único* es difícil de apreciar en la práctica–, permite realizar la autodeterminación informativa en su plenitud, ya que, tan importante como conocer quién tiene nuestros datos, qué datos de gestionan o lo que se ha hecho con ellos, es poder intervenir en las decisiones que se tomen basándose en dicho tratamiento[19].

En el caso venezolano, la cuestión de los datos o la información personal es más delicada aun, toda vez que nosotros no tenemos una legislación especifica en materia de protección de datos personales que son creados, administrados, almacenados, intercambiados y transmitidos por medios electrónicos.

En el sistema de interoperabilidad contemplado en el Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado*, la legitimación subjetiva para solicitar y obtener el acceso a los datos de una persona que se encuentren en los órganos y entes del Estado sólo le corresponde a dichos órganos y entes del Estado, de forma que el administrado no actúa en el procedimiento de intercambio; según lo consagrado en el marco legal, la actuación se establece entre las instituciones de la Administración Pública, que tratan a la información de los ciudadanos como un objeto sobre el cual versa el intercambio de datos.

> En otras palabras, el ciudadano se encuentra inmerso en la lógica de actuación Administración-Administración, lo que se traduce en su poca capacidad de decisión y de gestión sobre sus propios datos. Pareciera entonces que el modelo hubiera sido creado para responder a las necesidades de acceso de las Administraciones a los datos de los ciudadanos (…) el hecho de que la cesión del dato se base en la presunción de que la Administración requirente efectivamente cuenta con el consentimiento del administrado hace que puedan resultar vulnerados derechos como el derecho fundamental a la protección de datos personales[20].

En opinión de Yarina Amoroso Fernández, el ciudadano se presenta como el "eje central" de todo el proceso de *interoperabilidad*, ya que es a él a quien va dirigida la eficiencia en la ejecución de la función pública.

> Este es el concepto base, cuando se trata de conceptualizar el Gobierno electrónico, los ciudadanos ya no son un elemento más dentro de los procedimientos administrativos o jurídicos. El ciudadano tiene que ser considerado como centro en cualquier solución que se piense[21].

19 PRENAFETA RODRÍGUEZ, Javier. "La privacidad en el Gobierno…", *ob. cit.*
20 ALAMILLO, Ignacio y Erika Henao Hoyos. "La gestión electrónica…", *ob. cit*.
21 AMOROSO FERNANDEZ, Yarina. "Open Data:…", *ob. cit*., p. 14.

Entonces, teniendo claro que el ciudadano es el motor que impulsa mejorar las relaciones y las gestiones de las distintas dependencias de la Administración Pública, resulta evidente que se requieren algún tipo de garantías que permitan disminuir o atenuar los factores de vulnerabilidad a que se encuentran sometidos los datos, la información y los documentos en manos de los órganos y entes del Estado.

En este sentido, se puede anotar que la información personal o los datos de cada individuo han sido objeto de protección desde el reconocimiento del impacto del uso de las TIC en los derechos de las personas. Es en el año 1967 en el seno del Consejo de Europa donde se constituyo una Comisión para estudiar los alcances y consecuencias del mencionado impacto. Posteriormente, y luego de varias transformaciones se alcanza la "*…madurez de la protección de datos (tercera generación, 1980-1998). En este período se contemplan una serie de derechos de los ciudadanos para hacer efectiva la protección de sus datos, así como medidas de seguridad por parte de los responsables de los mismos*"[22].

Actualmente, la protección de datos se tiene como un derecho fundamental, derivando por una parte, en la promulgación de leyes para la protección de los datos; y por otra parte, en la creación de entes de la Administración Pública que velan por el correcto uso de la información personal que se encuentra en posesión de entes públicos o privados.

En la Constitución de la República Bolivariana de Venezuela del año 1999, se consagran dos artículos, que han servido de fundamento para la protección de los derechos de la información personal.

El artículo 28[23] consagra el llamado "*Habeas Data*", entendido como:

> …el derecho de toda persona a interponer la acción de amparo para tomar conocimiento de los datos a ella referidos y de su finalidad; sea que ellos reposen en registros o bancos de datos público, o los privados destinados a proveer

22 PUENTE de la MORA, Ximena. "Protección de datos personales en posesión de los particulares en México: avances y desafíos", en: *Memorias del XIV Congreso Iberoamericano de Derecho e Informática*. Universidad Autónoma de Nuevo León, Federación Iberoamericana de Asociaciones de Derecho e Informática (FIADI), México, 2010, p. 912.

23 Constitución de la República Bolivariana de Venezuela, artículo 28.- "*Toda persona tiene el derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y de solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley*".

> informes y, en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos[24].

El artículo 60[25] del texto constitucional corresponde principalmente al derecho a la privacidad, entendido como:

> …derecho de la persona de decidir por sí mismo en qué medida desea compartir con otros sus pensamientos, sus sentimientos y su vida personal, constituye pues una respuesta jurídica a las aspiraciones de cada persona por alcanzar un ámbito de desarrollo interior, ajeno a la intromisión y difícil de delimitar porque lo que para una persona puede ser privado para otra no lo es[26].

Así, los autores nacionales[27] han entendido que la creación y almacenamiento de los datos personales deben seguir unos "*Principios Generales*" para que sean tenidos como lícitos: (1) cuando se encuentren debidamente inscritos, observando en su operación los principios que establezcan las leyes y las reglamentaciones que se dicten en consecuencia; (2) los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública; (3) la información personal que se recoja a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido; (4) la recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la ley; (5) los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquéllas que motivaron su obtención; (6) los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario; (7) los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate; (8) los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular; y (9) los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

24 ORTIZ ORTIZ, Rafael. *Habeas Data. Derecho Fundamental y Garantía de la Protección de Derechos de la Personalidad. (Derecho a la Información y Libertad de Expresión),* Editorial Frónesis, Caracas, 2001, p. 70.

25 Constitución de la República Bolivariana de Venezuela, artículo 60.- "*Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos*".

26 PUENTE DE LA MORA, Ximena. "Nuevas tendencias del derecho a la privacidad. Caso Naomi Campbell", en: *Revista de Investigación y Análisis DEJURE*, Año 6, Segunda, Número 4, Colima, México, Febrero 2006, p. 58.

27 SALAZAR CANO, Edgar. "El Habeas Data en el Derecho Comparado", en: *Anuario* Nº 29, Facultad de Derecho, Universidad de Carabobo, Valencia, 2006, pp. 125-126.

Estos artículos de la Constitución de la República Bolivariana de Venezuela han sido objeto de atención por parte del Tribunal Supremo de Justicia, especialmente de la Sala Constitucional[28]. De los casos tratados[29] se puede concluir que la protección de datos personales en Venezuela ha estado dirigida principalmente a registros o bases de datos que se encuentran en posesión de órganos y entes del Estado, en archivos de acceso exclusivo o restringido de los funcionarios o del personal que labora en esas instituciones, y no se han tratado, aun, solicitudes de protección a la privacidad de información que se encuentra en posesión de terceros particulares o en las redes abiertas, especialmente en Internet.

Ahora bien, en lo que respeta al Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado*, debemos advertir que la protección de los datos personales se puede identificar en dos elementos, claramente diferenciados. Por una parte, el elemento adjetivo, contenido en el concepto de *seguridad de la información* como herramienta de protección; y por otra parte, el elemento sustantivo, que se encuentra referido a la naturaleza de los datos, la información o los documentos que permitirá la *denegación al acceso y transferencia de los datos, información y documentos*.

El primer elemento, la *seguridad de la información* o *seguridad de los servicios*[30], se refiere al otorgamiento de condiciones y medidas de protección, que garanticen un estado de inviolabilidad de influencias o de actos hostiles

28 Es importante anotar que este trabajo no pretende hacer un análisis de las fundamentaciones del Derecho Constitucional, sino presentar de manera integral la problemática de la protección de las personas (naturales y jurídicas) que generan información al alcance de terceros a través del empleo de los medios informáticos en la Sociedad de la Información.

Para el análisis de Derecho Constitucional de la figura del Habeas Data y del derecho a la privacidad, invitamos al estudio del siguiente trabajo: BREWER-CARÍAS, Allan R. *El proceso constitucional de las acciones de Habeas Data en Venezuela: las sentencias de la Sala Constitucional como fuente del Derecho Procesal Constitucional.* [En línea], Disponible en: *www.allanbrewercarias.com.*

29 Sentencias del Tribunal Supremo de Justicia, Sala Constitucional: 1) Sentencia No. 1050/ 2000, Fecha: 23/08/2000, Caso: Ruth Capriles Méndez y otros, Solicitud de Habeas Data. En: http://www.tsj.gov.ve/decisiones/scon/Agosto/1050-230800-00-2378%20.htm; 2) Sentencia No. 332/2000, Fecha: 14/03/2000, Caso: ISACA Compañía Anónima, Solicitud de Habeas Data. En: http://www.tsj.gov.ve/decisiones/scon/Marzo/332-140301-00-1797%20.htm; 3) Sentencia No. 2828/2004, Fecha: 07/12/2004, Caso: Pedro José Cabello Bonillo, Acción de Amparo En: http:/ /www.tsj.gov.ve/decisiones/scon/Diciembre/2829-071204-04-0733%20.htm; 4) Sentencia No. 1281/2006, Fecha: 26/06/2006, Caso: Pedro Reinaldo Carbone Martínez, Acción de Amparo. En: http://www.tsj.gov.ve/decisiones/scon/Junio/1281-260606-05-1964.htm; 5) Sentencia No. 1511/ 2009, Fecha: 09/11/2009, Caso: Mercedes Josefina Ramírez, Acción de Habeas Data. En: http:/ /www.tsj.gov.ve/decisiones/scon/Noviembre/1511-91109-2009-09-0369.html.

30 *Decreto Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado*, artículo 34.- "*Los servicios de información interoperables deberán ser seguros, garantizando la privacidad, confidencialidad e integridad de los datos, información y documentos de acceso público*".

específicos que puedan proporcionar el acceso a la data de personas no autorizadas, o que afecten la operatividad de las funciones de un sistema de computación, bajo los principios de confidencialidad, integridad y disponibilidad de la información.

Los autores Ignacio Alamillo y Erika Henao Hoyos, sobre este punto, destacan que la *Ley española 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos*, reconoce la importancia de la seguridad, dedicando varios de sus artículos al desarrollo del tema de la identificación, la autenticación y la firma electrónica, tanto por parte de los ciudadanos como por parte de las propias Administraciones Públicas (personal al servicio de las Administraciones Públicas, sede electrónica, sello de órgano).

> Los principios de proporcionalidad y de seguridad se encuentran consagrados en la *Ley española 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos*. El primero hace referencia a que la exigencia de un determinado nivel de acreditación debe circunscribirse a la naturaleza y circunstancias de los distintos trámites y procedimiento. Este principio actúa como límite superior, no pudiendo exigirse un nivel de seguridad más alto que el que resulta adecuado y necesario en el procedimiento tradicional basado en soporte papel. El segundo, establece que en el escenario telemático se exigirán al menos el mismo nivel de garantías exigidas en los trámites y procedimientos llevados a cabo por los conductos tradicionales. Este principio actúa como límite inferior, garantizando un tratamiento equivalente en términos de seguridad a los diferentes canales de tramitación (en soporte papel y en soporte electrónico)[31].

Así, para el caso particular del intercambio de datos entre Administraciones Públicas, se establece el uso de mecanismos que ofrezcan los máximos grados de seguridad; que según la legislación de ese país, puede ser alcanzado combinando la ley general de firma electrónica y la ley especial de identidad y firma electrónica en el sector público, lo cual conduce a un modelo en el que necesariamente han de existir diferentes sistemas y mecanismos de identidad y firma, como son: contraseñas estáticas, contraseñas dinámicas, mecanismos de segundo factor de autenticación, certificados en soporte *software*, certificados en soporte *hardware*, biometría, entre otras posibilidades.

En el análisis de las cuestiones de seguridad, los citados autores van más allá del uso bajo los estándares de interoperabilidad de los datos, información y documentos de las Administraciones Públicas españolas, y anotan los soluciones a las que se han arribado sobre estos temas, dado que se encuentran dentro de las prioridades máximas del programa de Administración Electrónica de la Unión Europea, recogido en la Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, "*Plan de*

31 ALAMILLO, Ignacio y Erika Henao Hoyos. "La gestión electrónica…", *ob. cit*.

acción sobre Administración electrónica i2010: Acelerar la Administración electrónica en Europa en beneficio de todos", de fecha 25 de abril de 2006, que recoge y evoluciona el importante Acuerdo Signposts, adoptado a partir de la Declaración de Manchester de 2005[32].

En el caso venezolano, el Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado*, establece la utilización de la firma electrónica[33] en las actuaciones administrativas así como del sistema de certificación electrónica[34], con la finalidad de garantizar la integridad y autenticidad de los datos, información y documentos que se intercambien electrónicamente, ya sea que su original se encuentre en medio impreso o electrónico; conforme a las normas técnicas de seguridad de la información que dicte la autoridad competente en la materia; es decir, la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE)[35].

32 ALAMILLO, Ignacio y Erika Henao Hoyos. "La gestión electrónica…", *ob. cit*.

33 El *Decreto No. 1.204 con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas*, publicado en la Gaceta Oficial No. 37.148 de fecha 28 de febrero de 2001, establece los siguientes aspectos de las firmas electrónicas: i.- Definición Legal: "información creada o utilizada por el Signatario, asociada al Mensaje de Datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado". ii.- Reconocimiento del valor probatorio: la Firma Electrónica que permita atribuir autoría a los Mensajes de Datos tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa. iii.- Requisitos para la validez y eficacia probatoria: la Firma Electrónica deberá: a) garantizar que los datos utilizados para su generación pueden producirse sólo una vez, y asegurar, razonablemente, la confidencialidad; b) ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento, y; c) no alterar la integridad del Mensaje de Datos. iv. Efectos jurídicos: cuando la Firma Electrónica no cuente con los requisitos para su validez y eficacia probatoria, podrá constituir un elemento de convicción valorable conforme a las reglas de la sana crítica. v.- Firma Electrónica Certificada: es aquella que ha sido debidamente certificada por un Proveedor de Servicios de Certificación Electrónica.

34 El Decreto No. 1.204 con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas, establece los siguientes aspectos de los certificados electrónicos: i.- Definición legal: "Mensaje de Datos proporcionado por un Proveedor de Servicios de Certificación que le atribuye certeza y validez a la Firma Electrónica". ii.- Función: garantiza la autoría de la Firma Electrónica que certifica así como la integridad del Mensaje de Datos. iii.- Carácter: no confiere la autenticidad o fe pública que conforme a la ley otorguen los funcionarios públicos a los actos, documentos y certificaciones que con tal carácter suscriban. iv.- Contenido: 1) identificación del Proveedor de Servicios de Certificación que proporciona el Certificado Electrónico, indicando su domicilio y dirección electrónica; 2) el código de identificación asignado al Proveedor de Servicios de Certificación por la Superintendencia de Servicios de Certificación Electrónica; 3) identificación del titular del Certificado Electrónico, indicando su domicilio y dirección electrónica; 4) las fechas de inicio y vencimiento del periodo de vigencia del Certificado Electrónico; 5) la Firma Electrónica del Signatario; 6) un serial único de identificación del Certificado Electrónico, y; 7) cualquier información relativa a las limitaciones de uso, vigencia y responsabilidad a las que esté sometido el Certificado Electrónico.

35 El *Decreto No. 1.204 con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas*, establece los siguientes aspectos de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE): i.- Características: servicio autónomo con autonomía presupuestaria, administrativa, financiera y de gestión, dependiente del Ministerio del Poder Popular para la Ciencia, Tecnología e Innovación. ii.- Objeto: acreditar, supervisar y controlar a los Proveedores de Servicios de

El segundo elemento, la *denegación al acceso de los datos, información y documentos*[36], es la posibilidad que tiene un órgano o ente del Estado[37] de negarse al acceso o intercambio solicitado a través del *Operador de la*

Certificación Electrónica, públicos o privados. iii.- Competencias: 1) Otorgar la acreditación y renovación a los Proveedores de Servicios de Certificación Electrónica. 2) Revocar o suspender las acreditaciones otorgadas. 3) Mantener, procesar, clasificar, resguardar y custodiar el Registro de los Proveedores de Servicios de Certificación Electrónica. 4) Verificar que los Proveedores de Servicios de Certificación Electrónica cumplan con los requisitos previstos por la ley. 5) Supervisar las actividades de los Proveedores de Servicios de Certificación Electrónica. 6) Liquidar, recaudar y administrar las tasas establecidas en la ley. 7) Liquidar y recaudar las multas establecidas en la Ley. 8) Administrar los recursos que se le asignen y los que obtenga en el desempeño de sus funciones. 9) Coordinar con los organismos nacionales o internacionales cualquier aspecto relacionado con el objeto de la ley. 10) Inspeccionar y fiscalizar la instalación, operación y prestación de servicios realizados por los Proveedores de Servicios de Certificación Electrónica. 11) Abrir, de oficio o a instancia de parte, sustanciar y decidir los procedimientos administrativos relativo a las presuntas infracciones de la ley. 12) Requerir a los Proveedores de Servicios de Certificación Electrónica o sus usuarios, cualquier información que considere necesaria y que este relacionada con las materias de su competencia. 13) Actuar como mediador en la solución de conflictos que se susciten entre los Proveedores de Servicios de Certificación Electrónica y sus usuarios, sin perjuicio de las atribuciones que tenga el organismo encargado de la protección, educación y defensa del consumidor y el usuario, conforme a la ley que rige la materia. 14) Seleccionar los expertos técnicos o legales que considere necesarios para facilitar el ejercicio de sus funciones. 15) Presentar un informe anual sobre su gestión al Ministerio de adscripción. 16) Tomar las medidas preventivas o correctivas que considere necesarias conforme a lo previsto en la ley. 17) Imponer las sanciones establecidas en la ley. 18) Determinar la forma y el alcance de los requisitos para la acreditación de los Proveedores de Servicios de Certificación Electrónica. 19) Las demás que establezca la ley y sus reglamentos.

36 *Decreto Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado*, artículo 57.- "*La denegación de acceso a los datos, información y documentos que presente un órgano o ente del Estado, deberá estar justificada en alguna disposición legal y sólo se limitará a lo expresamente establecido en la ley. Si el dato, información o documento denegado se encuentra en algún documento que contenga datos o información no confidencial, el órgano o ente del Estado deberá separarlo y permitir el acceso e intercambio electrónico de aquellos que no tengan carácter confidencial*". Artículo 58.- "*La denegación de acceso a los datos, información y documentos deberá ser notificada por el órgano o ente requerido ante el operador de la interoperabilidad, dentro de los diez días hábiles siguientes a su solicitud, acompañada de un informe en el cual se expongan los fundamentos que la sustente. Una vez recibido el informe, el operador de interoperabilidad pondrá en conocimiento del mismo órgano o ente que haya solicitado acceder al dato, información o documentos, para que este manifieste si ratifica o no su solicitud*". Artículo 59.- "*Ratificada la solicitud de acceso e intercambio electrónico de dato, información o documento, el operador de la interoperabilidad convocará a los órganos o entes involucrados a fin de conciliar sus diferencias. Agotada la fase conciliatoria sin llegar a un acuerdo,* el *operador de la interoperabilidad remitirá las actuaciones al Comité Nacional de la Interoperabilidad, para que éste, dentro de un lapso de treinta días hábiles, se pronuncie sobre la procedencia o no de la solicitud de acceso e intercambio electrónico del dato, información o documento requerido. El Comité Nacional de la Interoperabilidad podrá en su decisión establecer todas las medidas necesarias para el adecuado y seguro intercambio electrónico del dato, información y documento, de ser el caso*".

37 La denegación de acceso o intercambio de dato, información o documento también puede ocurrir de oficio, de conformidad con lo establecido en el artículo 60, *eiusdem*.- "*El operador de*

Interoperabilidad por parte de otro órgano o ente del Estado, en virtud de la naturaleza de los datos, la información y los documentos requeridos.

Esta negativa debe ser justificada en alguna disposición legal; no obstante, debemos tener en cuenta que el Decreto *Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado*, no establece las causales de justificación para la denegación al acceso o intercambio de datos, información y documentos. Por el contrario, establece, con carácter obligatorio, que los órganos o entes del Estado compartirán los datos, información y documentos, dejando claro que las excusas tendrán como finalidad la garantía de la protección al honor, vida privada, intimidad, propia imagen, confidencialidad y reputación de los ciudadanos y ciudadanas. En este mismo orden de ideas, se establece que la solicitud de acceso o intercambio de datos, información y documento no es exigible, si la misma resulta impertinente, inadecuada o excesiva en relación al ámbito y fines del proceso que se desea ejecutar, valoraciones que deberá realizar el Operador de la Interoperabilidad al momento de tramitar la solicitud formulada por un órgano o ente del Estado[38].

Finalmente, en el ámbito de la *Carta Iberoamericana de Gobierno Electrónico*, la protección de datos personales se presenta dentro del derecho de los ciudadanos al gobierno electrónico, en los siguientes términos:

> …se reconoce el derecho de todo ciudadano de solicitar ante los organismos competentes la actualización, la rectificación o la destrucción de aquellos datos contenidos en registros electrónicos oficiales o privados, si fuesen erróneos o afectasen ilegítimamente sus derechos. Para garantizar este derecho, se tiene que asegurar a todo ciudadano el acceso a la información y a los datos que sobre sí mismo o sobre sus bienes consten en registros oficiales o privados, con las excepciones que justificadamente se establezcan, así como se debe facilitar el conocimiento del uso que se haga de dichos datos y su finalidad.

la interoperabilidad, cuando lo estime conveniente, podrá someter a la consideración del Comité Nacional de Interoperabilidad, la denegación de acceso a los datos, información y documentos presentada por un órgano o ente del Estado, aun en aquellos casos en los cuales el solicitante no haya ratificado su solicitud".

38 *Decreto Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado,* artículo 43.- "*Los órganos o entes del Estado están obligados a compartir los datos de autoría, y sólo podrán excusarse de compartir los datos, información y documentos que manejan cuando la ley expresamente así lo limite, a fin de garantizar la protección al honor, vida privada, intimidad, propia imagen, confidencialidad y reputación de los ciudadanos. La obligación de compartir datos de autoría, información y documentos de acceso público no será exigible cuando la solicitud de estos sea impertinente, inadecuada o excesiva en relación al ámbito y fines del proceso que se desea ejecutar*".

IV. Conclusiones

Cuando se habla de la Sociedad de la Información no solo se refiere a las personas que son capaces de producir y descodificar información, lo cual les permite participar de relaciones de interconexión con otros actores de esta sociedad, también se alude a las instituciones políticas, económicas y jurídicas, entre otras, que hacen uso de las TIC para el desarrollo de sus actividades.

Esta realidad de interacción social trae consigo requisitos o necesidades para lograr la incorporación de una persona o de un país a la Sociedad de la Información, no son exclusivamente problemas de tipo tecnológico, tales como tener o no computadoras conectadas en red; el elemento fundamental que determina su desarrollo está estrechamente relacionado con condicionantes económicas, sociales, culturales y muy principalmente jurídicas.

La evaluación del régimen jurídico de los servicios relacionados con las TIC, debe perseguir la competencia y la eficiencia, reconociendo los derechos de las personas no solo en las relaciones de uso y consumo que se den a través de la utilización de estas tecnologías, sino también de la garantía de los derechos fundamentales, en todos los aspectos de la Sociedad de la Información, desarrollándose un catálogo de instrumentos jurídicos que permitan hacer efectivos estos derechos.

Es así como la incorporación de las TIC, y el desarrollo de los aspectos económicos, sociales y políticos de la Sociedad de la Información suponen una transformación del concepto y del contenido tradicional de las relaciones de los ciudadanos con los órganos y entes públicos.

En este sentido, debemos tener presente que la llamada “revolución tecnológica”, que comprende los avances científicos que se han venido produciendo a lo largo del tiempo en el campo de la informática requiere la adecuación de los conocimientos científicos a nivel general y particularmente, en la evaluación de los factores de vulnerabilidad de la información de los particulares en poder de los órganos y entes del Estado.

> En definitiva, las Tecnologías de la Información y la Comunicación pueden mejorar la prestación de servicios a los ciudadanos, pero también –al igual que sucede con las empresas privadas– generan un riesgo para la privacidad de los ciudadanos, por lo que deben establecerse las correspondientes garantías, tanto técnicas como jurídicas. La implantación de identificadores únicos, el intercambio de datos entre Administraciones o registros públicos, el desarrollo de intranets, la utilización de Internet para realizar todo tipo de trámites,... y, en general, la implantación de las Tecnologías de la Información tanto para mejorar la organización interna de las Administraciones Públicas como la prestación de los servicios que se ofrecen al ciudadano requiere, previamente a poner en marcha un proyecto de forma global, la definición de los requerimientos técnicos y jurídicos que debe cumplir, y la realización de estudios, análisis, pruebas y validaciones encaminadas a determinar tanto la fiabilidad de la tecnología utilizada

> como el impacto, beneficios y riesgos que conllevan para el ciudadano, así como la conformidad de éstas medidas con la legislación vigente, todo ello de una forma transparente y que permita su discusión política[39].

Para finalizar anotaremos las oportunas conclusiones de los autores Ignacio Alamillo y Erika Henao Hoyos, en el ya citado trabajo: *La gestión electrónica de la identidad y de la firma electrónica en el intercambio electrónico de datos entre Administraciones Públicas:*

> Como consecuencia ineludible de lo anterior, es posible afirmar que para el establecimiento de relaciones electrónicas tanto entre la Administración y el administrado, como entre diferentes Administraciones, e incluso en las relaciones internas de una misma Administración, resulta imperiosa la necesidad de emplear los instrumentos adecuados que garanticen circunstancias como la identidad del actor y la integridad y autenticidad de los datos y documentos. De no ser así, sería imposible la construcción de un entorno de confianza en el cual los actores puedan interactuar, y se frustran los beneficios de la digitalización de los trámites y procedimientos administrativos[40].

Las TIC deben ser utilizadas para el logro de la mayor eficiencia y efectividad organizacional del Estado y el logro de los máximos ahorros; así el modelo de gobierno electrónico debe ser un modelo de servicios, de fácil acceso, ubicación, conocimiento en tecnologías y capacitación de los actores, sin dejar de lado la seguridad y protección de la información de los ciudadanos.

39 PRENAFETA RODRÍGUEZ, Javier. “La privacidad en el Gobierno…”, *ob. cit.*
40 ALAMILLO, Ignacio y Erika Henao Hoyos. “La gestión electrónica…”, *ob. cit*.

Comunicaciones judiciales por medios electrónicos como vía de emplazamiento alternativo al demandado en el proceso civil ordinario venezolano

Mariana Buitrago Rodríguez*

SUMARIO: I. Introducción. II. La citación del demandado en el proceso civil venezolano. 1. Aspectos formales de la citación. 2. Mecanismos previstos en el procedimiento civil para práctica de la citación. III. Del documento de citación en papel al soporte electrónico. 1. Los principios del entorno electrónico aplicables a la citación electrónica. 2. La equivalencia funcional del mensaje de datos que contiene la citación electrónica con la citación tradicional. IV. La citación judicial por medios electrónicos 1. La incorporación de medios electrónicos en la administración de justicia. 2. Referencia a la legislación española respecto de la citación judicial por medios electrónicos. 3. El sistema Lexnet. 3.1. Funcionamiento 3.1.1. Condiciones de ingreso 3.1.2. Presentación de escritos. 3.1.3. Envío de comunicaciones judiciales: citaciones y notificaciones. 3.2. Ventajas del sistema. 4. Futuro de la citación electrónica en el proceso civil venezolano respecto a la experiencia española. V. Consideraciones finales.

Resumen

Este artículo estudia la posibilidad jurídica de usar medios electrónicos en las citaciones judiciales bajo los principios de la legislación venezolana. Se toma como referencia la legislación procesal que rige la citación y la legislación especial que regula el uso de los mensajes de datos y las firmas electrónicas. También se analiza la experiencia española a través del sistema Lexnet para el envío de comunicaciones electrónicas en el entorno judicial, con la finalidad determinar si es posible la utilización de sistemas

Recibido: 5/12/2013 • Aceptado: 15/2/2014

* Abogada egresada de la Universidad Católica del Táchira. Especialista en Derecho Procesal Civil Universidad Santa María (Venezuela). Profesora asociada de la Universidad de Los Andes. buitragomariana@gmail.com

similares que permitan realizar citaciones judiciales a través de medios electrónicos en Venezuela.

Palabras clave: Citación judicial. Tecnologías de Información y la Comunicación. Documentos electrónicos. Firmas electrónicas.

Abstract

This paper examines the legal possibility of using electronic means in subpoenas under principles in Venezuelan law. It refers to the procedural law governing subpoenas, and to the special legislation regulating data messages and electronic signatures in Venezuela. The Spanish experience through Lexnet system to send electronic communications in the legal environment is also analyzed, in order to determine whether the use of similar systems allowing subpoenas through electronic means is possible in Venezuela.

Keywords: Subpoena. Information Technology and Communication. Electronic Documents. Electronic Signatures.

I. Introducción

El proceso de modernización en el que las sociedades actuales se encuentran inmersas, exige que día a día los países y sus gobiernos tomen las acciones necesarias para adoptar los avances tecnológicos que beneficien a la población y que hagan más ágiles, prácticas y sencillas las relaciones de la Administración Pública con los administrados.

La tendencia actual en el Derecho comparado es la incorporación de la informática jurídica a través de las técnicas electrónicas para facilitar la aplicación del Derecho y la agilización de procedimientos, así como la administración de información que consecuencialmente permita la práctica de actos judiciales comunicacionales por medios electrónicos, que propenda la obtención de una justicia rápida, efectiva y eficaz. Países como España –tomando en cuenta la realidad globalizadora y asumiendo la importancia que tiene para la paz interna de un país la administración de justicia, así como la celeridad en obtener la misma, y en aras de conseguir la aplicación de justicia no tardía– han modificado sus sistemas de citaciones judiciales en materias tales como: civil, administrativa, tributaria, contencioso administrativa, laboral, disciplinaria, entre otras, para dar paso a la nueva era de las comunicaciones electrónicas judiciales, en donde priva el Derecho procesal electrónico, es decir, la informática jurídica de gestión.

Sin embargo, la administración de justicia venezolana desde siempre ha seguido el modelo romanista en sus actuaciones, discurriendo por ende los procesos judiciales en parámetros eminentemente formalistas que propugna la escritura y el soporte papel como medio para comprobar dichas actuaciones procesales, impidiendo, por tanto, una aceptación legislativa manifiesta de los

avances tecnológicos a excepción del proceso laboral –que a partir del año 2002– plasma en la Ley Orgánica Procesal del Trabajo una forma de comunicación judicial que según dispone el segundo aparte del artículo 126 *ejusdem*[1] consagra la figura de la notificación electrónica del demandado a instancia de parte o por oficio, siempre y cuando se acuerde la utilización del medio electrónico y que este medio le pertenezca al demandado.

De acuerdo con esta realidad práctica y jurídica presente en los procesos judiciales venezolanos, salvo la excepción mencionada, se hace necesario hacer referencia a uno de los actos más emblemáticos y formales para un proceso civil, tal como lo es, el acto de comunicación judicial de citación al demandado.

La citación judicial al demandado ha sido concebida en el sistema venezolano como la formalidad necesaria para la validez del juicio, pudiéndose verificar el cumplimiento de la misma a través de tres modalidades para su práctica, vale decir, la personal o *in facem*, la materializada por medio de carteles y la realizada por correo certificado con aviso de recibo. Pero estas modalidades funcionan como formalidades necesarias para la validez del juicio contextualizadas en una época histórica cuyas comunicaciones más avanzadas se verificaban por medio de correo convencional, que se constituían en formalismos y no bajo el esquema de la búsqueda de una justicia breve, oportuna, rápida y efectiva, que esté exenta de dilaciones y formalismos, principios estos que ampara el texto constitucional venezolano del año 2000.

De allí, que la citación en los procesos civiles ordinarios venezolanos se convierte en un acto judicial que tiene por norte imponer al demandado del conocimiento de la pretensión que el actor ha ejercido en su contra, a través del llamado que le hace el juez del tribunal ordenándole comparecer en el día señalado para que dé contestación a la demanda y ejerza su derecho a la defensa, es decir, colocando al sujeto demandado, que conforma la parte pasiva de la relación jurídico-procesal, directamente en contacto con el órgano jurisdiccional que tendrá la tarea de administrar la justicia.

Empero, la implementación de la citación judicial civil a través de comunicaciones judiciales por medios electrónicos para una persona jurídica demandada, es una experiencia novedosa que implica una inversión tecnológica por parte de la administración de justicia venezolana para modernizar y optimizar los sistemas de llamamiento llevados a cabo por el Estado venezolano, en virtud de que una de las inconformidades por parte de los usuarios del sistema de administración de justicia patrio, es la lentitud con que se administra justicia, y ella inicia con la citación a los procesos civiles ordinarios, donde el desgaste humano, desembolso de dinero y el gasto de papel conspiran contra la celeridad de los procesos judiciales.

1 Véase art. 126 Ley Orgánica Procesal del Trabajo. Gaceta Oficial de la República Bolivariana de Venezuela, 37.504, agosto 13 de 2002

II. La citación del demandado en el proceso civil venezolano

La citación como figura jurídica procesal, no está definida por el legislador venezolano dentro de las normas del Código de Procedimiento Civil. De allí que el trabajo de los doctrinarios patrios, sea eminentemente importante para aclarar el tema en cuestión.

Rengel, (1992)[2] señala en sentido amplio que la citación *"es la acción y efecto de llamar a una persona a concurrir a un lugar con un objeto determinado"*. Sin embargo, y aun cuando la citación esté relacionada con el llamamiento que se le hace a una persona, esta definición es amplísima para ser considerada como tal dentro del mundo de los actos procesales, porque, si bien es cierto que la citación es un llamado a una persona –natural o jurídica–, no se precisa ante quién debe acudir la persona que es requerida, tampoco la razón ni el propósito por el cual se requiere la presencia de aquella. Por tanto, es necesario precisar una definición más específica de la figura jurídica de la citación.

Moros (1995)[3] siguiendo la orientación de la extinta Corte Suprema de Justicia venezolana, define la citación como un *"acto formal de un Juez o de un Tribunal por el cual se ordena a una persona a comparecer ante él, en día y hora fijas con un objeto determinado del cual se le da conocimiento"*. De acuerdo con la postura anterior se puede considerar la citación, como un acto de carácter eminentemente judicial que emana del Juez –aún cuando la práctica de la misma se haga efectiva por medio de agentes de la jurisdicción– y que ordena a través de ese llamamiento, la comparecencia en día determinado, de una persona natural o jurídica –mediante su representante legal o apoderado judicial–, para realizar o presenciar una diligencia que afecte a un proceso judicial.

Por su parte Bello (1989)[4], señala que la citación en el proceso civil ordinario, tiene un efecto dual y en este sentido dispone que:

> Contiene el acto de citación un doble efecto, por una parte el poner en conocimiento al demandado de la pretensión que en su contra ha ejercido el actor, y por la otra el llamado que a su vez le hace para que acuda al tribunal en la oportunidad que se indique con el fin de que proceda a ejercer sus defensas en la pretensión del actor.

De la precisión anterior se puede indicar que, el primer efecto de la citación, está referido a la puesta a derecho del demandado valiéndose de dicha diligencia

2 Arístides RELGEL ROMBERG: *Tratado de Derecho Procesal Civil Venezolano*. Vol. II. Caracas: Editorial Arte, 1992, p. 277.

3 MOROS FUENTES, Carlos: *Citaciones y Notificaciones*. 2da. Edición. Caracas: Editorial Componentes, 1.995, p. 17.

4 BELLO LOZANO, Humberto: *Procedimiento Ordinario*. 6ª edición, Caracas: Mobil Libros, 1989, p. 105.

procesal, esto es, se le hace saber al demandado que debe estar al tanto de que en su contra cursa una causa judicial, en tanto que el segundo efecto que el procesalista señala es la materialización de la garantía individual y del derecho a la defensa, ya que, con la citación se pretende que el demandado haga lo propio para ejercer su derecho a la defensa, por ser considerado este acto judicial como un instituto de rango constitucional, que deriva de la garantía del derecho a la defensa en todo grado y estado de la causa previsto en el artículo 49 de la Constitución de la República Bolivariana de Venezuela[5], siendo este derecho desarrollado en el artículo 215 del Código de Procedimiento Civil.

1. Aspectos formales de la citación

Uno de los puntos importantes dentro del mundo procesal está referido a los aspectos formales de la citación, puesto que, para poner en conocimiento al demandado y requerir su comparecencia para la contestación de la demanda, se deben agotar los extremos previstos en el Código de Procedimiento Civil.; tales como: (a) La identificación del demandado; (b) la orden de comparecencia; (c) la compulsa del libelo con orden de su exactitud y (e) la entrega al alguacil.

En cuanto a la identificación del demandado, señala Rivera (2000)[6], *"Es un presupuesto para la constitución del proceso, en consecuencia para entablar la litis se requiere la identificación contra quién va dirigida la demanda"*. Ello es evidente puesto que se requiere la identificación suficiente del demandado, teniendo como requerimientos mínimos el nombre y el apellido del demandado, pudiendo en todo caso solicitar el funcionario del tribunal al demandante, el número de la cédula de identidad de la parte demandada, o el número de identificación fiscal –en caso de ser persona jurídica– así como la dirección de ésta, debiendo coincidir estos aspectos tanto en la orden de comparecencia como en la compulsa del libelo; caso contrario, puede demandarse la nulidad de la citación, por indeterminación del sujeto pasivo de la relación jurídica procesal.

Sobre la orden de comparecencia, es menester señalar que una vez que el tribunal verifique que el escrito libelar contiene los extremos de los artículos 340 y 346 *ejusdem*[7], el Juez procede a admitir la demanda y emitirá la orden de comparecencia del demandado, debiendo contener esta actuación judicial, la clara y precisa identificación de la parte demandada, así como la información

5 Véase art. 49 Constitución de la República Bolivariana de Venezuela. Gaceta Oficial, 5.453 (Extraordinaria), marzo 24 de 2000.Véase art. 215 Código de Procedimiento Civil. Gaceta Oficial de la República de Venezuela, 4.209 (Extraordinaria), septiembre 18 de 1990.

6 RIVERA MORALES, Rodrigo: *Las nulidades en el Derecho Civil y Procesal. Táchira*: Ediciones Jurídicas J. Santana, 2000, p. 283.Véase art. Código de Procedimiento Civil. Gaceta Oficial de la República de Venezuela, 4.209 (Extraordinaria), septiembre 18 de 1990.

7 Véase arts. 340, 346, Código de Procedimiento Civil. Gaceta Oficial de la República de Venezuela, 4.209 (Extraordinaria), septiembre 18 de 1990.

necesaria para que la parte demandada conozca que existe un juicio en su contra por ello debe indicarse los términos en los que se le demanda, la petición o pretensión del actor demandante, la oportunidad o lapso que tiene el demandado para comparecer a dar contestación al escrito libelar. Esta orden de comparecencia debe estar firmada por el juez del tribunal de la causa, todo ello de conformidad con lo que establece el artículo 342 del referido Código[8].

A falta de cualquiera de estos requisitos, la orden de comparecencia se hace anulable según lo establece Rivera (ob. cit.),[9] ya que *"estas formalidades son esenciales, porque están vinculadas al derecho de defensa mismo"*. La posición anterior, es razonable ya que, si no se tiene certeza de estos requisitos mínimos y *supra* señalados ¿cómo se le puede pedir al demandado que organice su defensa? ¿A qué lugar podrá acudir el sujeto demandado a enervar la pretensión del actor? ¿Cuál sería el plazo que tiene el demandado para hacer efectivo su derecho a la defensa? La imprecisión de estos requerimientos comporta la indefensión del demandado, ya que a falta de indicación de alguno de ellos, se impide o se obstaculiza concretamente la posibilidad que tiene el demandado de hacer valer su derecho de defensa.

En cuanto al requisito de la compulsa del libelo con certificación de su exactitud, éste forma parte del mismo conocimiento que debe tener el demandado, que en su contra cursa una pretensión, y más puntualmente en los términos en que quedó formulada la demanda, y esto sólo es posible por medio de las copias del libelo, debiendo en todo caso ser certificadas para evitar manipulación por parte de cualquier interesado o para impedir que el demandado pueda conseguirse con algún argumento no evidenciado que pueda entorpecer su defensa. Sin embargo, ello no obsta para que el demandante pueda dentro del supuesto previsto en la ley, reformar la demanda en los términos que crea conveniente, pero igualmente se le concederá a la parte demandada otros veinte días para la contestación sin que medie nueva citación.

Por todo ello, la institución de la citación es una de las pocas que están previstas en nuestra ley procesal, y que está plagada de formalismos precisos, por lo que el inflexible cumplimiento de tales formalidades es tan importante como la finalidad misma de la ley, que no es otra que la de poner en conocimiento de una persona el hecho que ha sido demandada.

2. Mecanismos previstos en el procedimiento civil para práctica de la citación

La citación como una comunicación y acto judicial es una sola, en tanto que las formas previstas por la ley para citar, son maneras de materializar el acto al

8 Véase arts. 342, Código de Procedimiento Civil. Gaceta Oficial de la República de Venezuela, 4.209 (Extraordinaria), septiembre 18 de 1990.

9 RIVERA, R.: *Las nulidades … op. cit*., p. 2000, p. 284.

demandado, que es llamado por el Juez y que busca que aquel acuda a hacerse parte en el proceso. Por ello, las formas o maneras de citar, son mecanismo o vehículos legales que han sido previstos para que a través de ellos el funcionario judicial cumpla la orden del juez y llame al demandado para que éste como sujeto pasivo de la relación procesal, se presente en el proceso civil que cursa en su contra y deponga las defensas que crea necesarias, como ya se dijo.

Pero para que ello suceda y en caso de tratarse de persona natural, es indispensable agotar en primer momento el arquetipo de citación personal prevista en el artículo 218 del Código de Procedimiento Civil venezolano, y que es conocida en la doctrina nacional como la citación *in faciem*. Pero, siendo imposible la práctica de este tipo de citación, debe el actor o demandante proceder a seleccionar entre el tipo de citación por correo con aviso de recibo o la citación por carteles, tomando en cuenta los supuestos para proceder, los requerimientos y las formalidades necesarias para la práctica de una cualquiera de estas modalidades de citación.

En cuanto a la citación por correo certificado con aviso de recibo, vale mencionar que este tipo de modalidad sólo es posible en los casos de impracticabilidad de la citación personal del demandado y que éste sea una persona jurídica, teniendo su previsión legal en el artículo 219 *ejusdem*, y presenta como trámite[10] el contenido tanto en el Código de Procedimiento Civil como en la normativa interna para citaciones y notificaciones judiciales por correo del año 1986[11]. El ámbito de aplicación es uno de los factores particulares de este

10 Acordada por parte del juez del tribunal de la causa este tipo de citación, el funcionario del tribunal (alguacil), deberá trasladarse a la oficina del Instituto Postal Telegráfico de Venezuela (IPOSTEL) para depositar en dicha oficina de correo, en un sobre abierto los documentos relativos a la citación. Posteriormente a dicho depósito le exigirá al funcionario de IPOSTEL un recibo, donde el funcionario receptor de la documentación deje constancia de los documentos que fueron entregados por el alguacil del tribunal y que consecuencialmente estarán dentro del sobre; además de los datos necesarios para poder ubicar al destinatario de esta correspondencia (nombre, apellido, dirección para practicar la citación por correos), así como también la fecha en que recibió esos documentos de manos del alguacil.

El funcionario de correo, tendrá siete (07) días hábiles contados a partir del día siguiente de la recepción de los documentos antes mencionados para practicar la entrega de la citación. Pero, de ser infructuosa tendrá una segunda oportunidad para poder llevar a cabo el mandato encomendado, siempre dentro de días hábiles continuos.

En caso de conseguir a la persona investida por la ley para recibir dicha documentación, el repartidor postal telegráfico deberá identificar en el aviso de recibo -que previamente ha de adquirir la parte actora interesada de la práctica de la citación *in commentum*,- tanto el nombre, como el apellido, la cédula de identidad, de la persona que sirve de aceptante de la comunicación, así como el cargo que desempeña en la empresa y solicitará de dicho receptor, la rúbrica en dicho formulario, que irá acompañada de la firma autógrafa del funcionario de la oficina de IPOSTEL, además de la hora y día en que se practicó la entrega de la citación por este mecanismo. A vuelta de correo este formulario de aviso de recibo, deberá ser agregado al expediente por el secretario del tribunal, indicando este funcionario judicial, la fecha de la mencionada diligencia.

11 Véase Reglamento Interno para Citaciones y Notificaciones Judiciales por Correo. Gaceta Oficial, 3.694 (Extraordinaria) enero, 22 de 1986.

tipo de citación ya que sólo podrá practicarse en la oficina de la persona jurídica, o en el lugar donde ésta ejerce su industria o comercio.

La tercera modalidad de citación es la que se lleva a cabo por carteles, es decir, por publicaciones en prensa y que está prevista en el artículo 223 *ejusdem*[12]. Esta manera de citación puede verificarse a petición del interesado (demandante o actor de la causa) en defecto de la citación personal aun cuando se hubiere pedido la citación por correo certificado con acuse de recibo siempre de persona jurídica y no se haya podido lograr.

III. Del documento de citación en papel al soporte electrónico

La creencia arraigada de que el papel es el único soporte de registro para un documento escrito data de los albores de la historia - doscientos años antes de Cristo con la invención del papel realizada por el imperio chino y se mantuvo hasta el período 1960-1970, cuando se da un vuelco a esa concepción gracias a la aparición de Internet y de los primeros documentos que se trasmitieron y registraron por intermedio de dispositivos electrónicos.

Con la llegada de la era de la tecnología se deja a un lado la utilización del papel como soporte probatorio de lo actuado para dar paso a los actos de comunicación judicial soportados en mecanismos electrónicos, pues lo único que cambia es el soporte en el que es registrada, enviada y almacenada la información.

Álvarez Cienfuegos, citado por Rico (2005)[13] señala que *"El documento como una realidad corporal refleja una realidad fáctica con trascendencia jurídica, no puede identificarse con el papel como soporte, ni con la escritura como unidad de significación"*. Por ello, las consideraciones anteriores avalan la posibilidad de nuevos soportes de información en el sentido de que el documento que consta en papel no es el único medio de registro que puede ser utilizado para comprobar su existencia. En efecto, el documento escrito, no debe ser entendido de forma exclusiva ni excluyente como la información contenida en un trozo de papel ya que si el documento refleja una realidad, la misma puede ser dada a conocer por medio de otros instrumentos creados por el hombre para facilitar la transmisión, conservación y almacenamiento de la información que consta en el documento.

De allí, que valga señalar que existe una equivalencia funcional entre el soporte papel y el soporte por medio electrónico, puesto que ambos documentos seguirán siendo en esencia la representación material destinada a reproducir una manifestación del pensamiento dentro de la cual no sólo caben las representaciones escritas denominadas instrumentos que no son más que una

12 Véase art. 223, Código de Procedimiento Civil. Gaceta Oficial de la República de Venezuela, 4.209 (Extraordinaria), septiembre 18 de 1990

13 RICO CARRILLO, Mariliana: *Comercio electrónico Internet y Derecho*, 2da. edición. Bogota: Legis Editores, 2005, p. 94

especie de documentos sino también otros documentos de carácter no instrumental.

En consecuencia, si la citación judicial al demandado es un acto de comunicación procesal del juez y básicamente se hace por escrito, nada obsta para que este acto procesal pueda ser elaborado o realizado a través de un soporte que no sea el papel porque, en todo caso no se estaría alterando ninguno de los requisitos de fondo que debe reunir el mencionado acto de comunicación judicial por el contrario, se estaría utilizando un soporte distinto al tradicional: el electrónico, que permite el envío y recepción del documento a través de las Tecnologías de la Comunicación e Información (TIC), para llevar a feliz arribo la entrega de la citación a su destinatario, quien es el primer interesado en recibir la comunicación judicial para poder enervar la demanda que en su contra ha interpuesto el demandante y de esa manera, al tener conocimiento oportuno y veraz de dicha situación, podrá en todo caso preparar la contestación que crea conveniente.

1. Los principios del entorno electrónico aplicables a la citación electrónica

Se han formulado cinco principios en el entorno negocial electrónico con la intención de darle fuerza a la equivalencia del documento electrónico con el documento tradicional. Estos principios han sido considerados por Illescas (2001)[14] como *"…principios con vocación universal. Reglas o principios básicos, y de aplicación general"*. En este sentido, se deben considerar estos principios como las bases fundamentales mínimas, de aplicación jurídica, nacional e internacional, que permiten servir a la ciencia del derecho, en tanto y cuanto no sean plenamente regulados en los dispositivos normativos legales de cada país y a la luz de los avances tecnológicos.

Por lo que será necesario admitir que dichos principios sólo son reglas mínimas no defectuosas, ni incorrectas, que se han reconocido para todos los ordenamientos jurídicos que pretendan reglamentar el derecho del comercio electrónico, facilitando en todo caso su uso y asegurando la confianza jurídica y práctica que proclama la aceptación general de los mismos, para así permitir vislumbrar los cambios legales bajo la orientación tecnológica, sin que exista pugna entre lo analógico - tradicional, y los avances tecnológicos. Los principios en referencia se pueden particularizar básicamente en: (a) la equivalencia

14 ILLESCAS ORTIZ, Rafael: *Derecho de la contratación electrónica*. Madrid: Civitas ediciones S.L., 2001, p. 37

funcional[15]; (b) la neutralidad tecnológica[16]; (c) la inalteración del derecho preexistente de obligaciones [17]y contratos; (d) la buena fe y (e) la libertad de pacto.

De los principios *supra* mencionados cabe señalar que sólo tres operan en función del tema de la citación judicial practicada por medios electrónicos, porque tanto el principio de la buena fe, como el principio de la libertad contractual no aplican dentro de un Derecho eminentemente público como lo es el Derecho procesal civil puesto que estos principios están referidos a la actividad eminentemente contractual y comercial y no a una actividad procesal. Por tanto, los principios que son aplicables como reglas universales a la inclusión de la citación judicial por medios electrónicos son el principio de la equivalencia

15 ILLESCAS ORTIZ, acerca del principio de la equivalencia funcional señala que: "*La función jurídica que en toda su extensión cumple la instrumentación escrita y autógrafa –o eventualmente su expresión oral- respecto de cualquier acto jurídico la cumple de igualmente su instrumentación electrónica, a través de un mensaje de datos, con independencia del contenido, dimensión, alcance y finalidad del acto así instrumentado. Por tanto, este principio, constituye el basamento para afirmar la no discriminación del mensaje de datos que contiene una declaración de voluntad del hombre, que es representada por el documento electrónico, frente a las declaraciones de voluntad simbolizadas desde siempre por el documento tradicional. De esta manera, el mensaje de datos tendrá la misma eficacia probatoria que su análogo siempre que se cumplan los requisitos previstos en la ley*". *Vid.* ILLESCAS ORTIZ, R.: *Derecho de la contratación electrónica, op. cit*., p. 41.

En el Derecho venezolano este principio se encuentra consagrado en el Decreto con Rango y Fuerza de Ley de Mensajes de Datos y Firmas Electrónicas. Gaceta Oficial de la República Bolivariana de Venezuela, 37.148, febrero 28 de 2001, artículo 4*:* "*Los mensajes de datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos*". Sin embargo, cabe aclarar que el dispositivo normativo referido, señala que cuando se exija que la información conste por escrito, el requerimiento en el mensaje de datos queda satisfecho siempre y cuando (a) el mismo pueda ser accesible para posterior consulta, (b) el mensaje de datos sea conservado en el formato en el que se generó, envió o recibió o en algún formato en el que sea demostrable la exacta producción de la información, y (c) debe conservar de igual forma los datos de identificación del emisor del mensaje (autoría- firma electrónica) y del receptor del mismo, así como también la fecha, hora de emisión y recepción de éste y que las declaraciones de voluntad no estén viciadas.

16 En referencia al principio de neutralidad tecnológica, RICO CARRILLO señala que: "*Este principio se basa en el respeto al uso de cualquier tecnología que se utilice o pueda usarse en el futuro a efectos de trasmitir un mensaje de datos o insertar una firma electrónica, por lo tanto implica no favorecer unas tecnologías sobre otras con la finalidad de evitar posibles obsolescencias legales*". Vid. RICO CARRILLO M.: *Comercio electrónico, Internet y Derecho, op. cit.* p. 69. Por lo que este principio se fundamenta en la premisa de la no exclusión ni inclusión de ningún tipo de tecnología en los instrumentos legales que abriguen las normas referentes al uso de las TIC, puesto que, al establecer un tipo de tecnología específica, la misma puede caducar si estás no son realmente neutras y amplias, arrastrando consigo a la labor legislativa. Por ende, las normas legales no deben taxativamente establecer una tipología única o exclusiva en el uso de tecnologías, ya que las mismas pueden de un momento a otro entrar ser suplantadas o superadas por otras tecnologías que se puedan considerar en el futuro.

17 En cuanto a este principio, RICO CARRILLO indica que "…*los elementos esenciales del negocio jurídico no deben modificarse cuando el contrato se perfecciona por vía electrónica, ya que se trata sólo de un nuevo medio de representación de la voluntad negocial*". Vid. RICO

funcional, el principio de la neutralidad tecnológica y el principio de no alteración del derecho preexistente. En tal sentido, vale la pena hacer las consideraciones siguientes:

1. En cuanto al principio de la equivalencia funcional respecto a la citación del demandado en un proceso civil como acto de comunicación puede estar soportado en un documento electrónico. Vale reflexionar que el acto judicial de citación vendría a ser representado a través del mensaje de datos que emite el juez como autor de dicha comunicación, no pudiendo este sujeto desconocer la manifestación de voluntad por él expresada en el mensaje enviado, puesto que no podrá desacreditar en ningún momento, ni relegar la existencia del mensaje de datos por la utilización de un formato distinto al utilizado tradicionalmente, debido a que el emisor debe en todo caso suscribir el mensaje de datos por medio de un mecanismo como la firma electrónica. De igual forma, el principio de la equivalencia funcional permite equiparar los efectos producidos por el documento tradicional en soporte papel y con firma autógrafa, a los efectos que se derivan del documento electrónico en soporte digital y con firma electrónica.

En consecuencia, para que la citación al demandado por medios electrónicos tenga la misma eficacia funcional que la citación práctica por medios tradicionales, debe cumplirse además de los requisitos de fondo para este tipo de comunicación judicial, con los requerimientos normativos establecidos para cualquier mensaje de datos.

2. En cuanto al principio de la neutralidad tecnológica para regular los dispositivos legales que contendrá la citación electrónica, debe señalarse que el trabajo del legislador es redactar la norma que permita y regule la citación por medios electrónicos para procesos judiciales, sin señalar de forma exclusiva algún mecanismo específico pues así generará inevitablemente obsolescencias al texto normativo en el futuro.

3. Finalmente en cuanto al principio de la no alteración del Derecho preexistente cabe mencionar que en caso de inclusión legislativa de la citación judicial del demandado por medios electrónicos, no se puede ni debe variar, alterar o modificar la naturaleza del sistema tradicional de citaciones judiciales, pues lo único que se puede modificar en todo caso es su especial forma de representación, es decir, el soporte que contiene como documento a la citación.

CARRILLO, M.: *Comercio electrónico, Internet y Derecho, op. cit*. p. 71. De tal manera que no debe existir variación, alteración, transformación o modificación sustancial del Derecho contractual u obligacional actual, ya que, la electrónica y su aplicación jurídica comprende simplemente la coexistencia de un nuevo soporte, así como también de un medio distinto de trasmitir la voluntad del hombre en cuanto a determinados actos. ..

2. La equivalencia funcional del mensaje de datos que contiene la citación electrónica con la citación tradicional

La citación del demandado como documento que es, puede realizarse a través de un documento electrónico blindado o protegido por los mecanismos que la ley y la informática dispongan para acompañar la emisión del mensaje de datos, asegurando por tanto, su confiabilidad, integridad y autoría, ya que por medio de la firma electrónica y los certificados electrónicos de protección o blindaje del mensaje de datos previstos en la Ley de Mensajes de Datos y Firmas Electrónicas, las citaciones judiciales que lleguen a practicarse bajo estas fórmulas, pueden ser valoradas como si se tratase de un documento en soporte papel.

En tal sentido, el mensaje de datos que posee la información de gestión judicial referida al acto comunicacional de citación del demandado, que emana del tribunal y que está protegida por el mecanismo de la firma electrónica produciría como efecto la plena confianza de que ese llamamiento o citación, se ha mantenido inalterable desde que se generó por la autoridad judicial, garantizándose de esta manera la confiabilidad, la integridad y la seguridad que ofrece la firma electrónica que es debidamente certificada por un proveedor de servicios. Pero debe puntualizarse que este mensaje solo al estar blindado a través de la firma electrónica certificada por un prestador de servicio de certificación, adquiere la validez y confianza de la orden de comparecencia emanada del juez.

Por ello, el prestador de servicio de certificación hará lo necesario para que concurran todos los requisitos previstos en la Ley de Mensaje de Datos y Firmas Electrónicas[18] y pueda garantizar la autoría de la firma electrónica del juez del tribunal a través del certificado electrónico, pero nunca garantizará la autenticidad o dará la fe pública que según la ley pueden otorgar los funcionarios públicos a las actuaciones suscritas por éstos.

De allí, que el documento electrónico –mensaje de datos– que contiene la orden de comparecencia del demandado puede ser equiparado funcionalmente al documento tradicional en soporte papel ya que, lo que cambia simplemente es el soporte en el que se da a conocer la información y no la información comunicacional de citación al demandado en un proceso civil.

Por tanto, la administración de justicia puede utilizar y optimizar su labor comunicacional en la gestión judicial con respecto a las partes, con mecanismos alternos a los establecidos por el redactor del Código de Procedimiento Civil, y que sean cónsonos con las TIC y las bondades que éstas ofrecen tales como la celeridad, la seguridad, la confiabilidad, la integridad y la desmaterialización del documento.

18 Véase artículo 16 del Decreto con Rango y Fuerza de Ley de Mensaje de Datos y Firmas Electrónicas.

Respecto al escrito de demanda, que debe ser compulsado tantas copias como partes demandadas aparezcan, puede suplirse el requerimiento del soporte papel, solicitando al actor la entrega en formato digital del libelo de demanda, debiendo el mismo estar acompañado de una firma electrónica garantizada por el prestador de servicios de certificación[19].

Por lo antes expuesto, se puede considerar que el documento de citación judicial en soporte electrónico tiene la misma equivalencia funcional del documento de citación en soporte papel, y para tenga la validez y la eficacia probatoria que la ley otorga a los documentos escritos, debe respetarse los requisitos de recuperabilidad, integridad y autoría de la información del mensaje de datos y la formalidad de la firma electrónica.

IV. La citación judicial por medios electrónicos

1. La incorporación de medios electrónicos en la administración de justicia

Diversos países con sistemas basados en los principios de corte romanista o los seguidores de los principios del *common law*, han ido adoptando para la realización de los procedimientos administrativos, legislativos y judiciales, la utilización de las TIC permitiendo optimizar la labor del Estado frente a las peticiones de los ciudadanos, creando una nueva cultura de la aplicación del Derecho y del acceso a la justicia a través de la inclusión de mecanismos que permitan la utilización de la informática jurídica de gestión judicial, para cumplir con los principios de justicia expedita, sin dilaciones indebidas y sin formalismos inútiles que reflejan la máxima: justicia tardía no es justicia.

Modernizar u optimizar los sistemas utilizados en la administración de justicia ha sido un reto para los Estados, porque ello implica la actualización de la infraestructura del sistema de administración de justicia que se había arraigado por años en los tribunales, así como también a la preparación de las personas que laboran en esta área (sean estos en calidad de empleados de la rama judicial, operadores de justicia), así como a los propios abogados y usuarios, que deben adaptarse a la automatización de la información legal y a los nuevos procesos de administración de justicia.

Al efecto, Rico (ob.cit.) señala que: *"El nacimiento y la difusión de la informática, facilitan la labor del jurista al suministrarle una serie de herramientas que agilizan el desarrollo del Derecho, permitiendo la automatización de la información legal y de los procesos de administración de justicia"*. Por ello, una de las formas de poder optimizar la administración de justicia, es permitir a los funcionarios judiciales como a los usuarios del

19 Véase artículo 6 del Decreto con Rango y Fuerza de Ley de Mensaje de Datos y Firmas Electrónicas

sistema judicial, la incorporación de la informática jurídica como ciencia de auxilio a los legisladores, y técnica de aplicación del Derecho, por lo que se puede incorporar al acto de citación-notificación sin que ello contribuya para desconocer ni desaplicar las modalidades existentes para la práctica de citaciones en Venezuela.

2. Referencia a la legislación española respecto de la citación judicial por medios electrónicos

España en el año 1995 dictó el Real Decreto Legislativo 2/1995 en fecha 7 de abril[20], previéndose en el artículo 53. 1. que:

> Los actos de comunicación se efectuarán en forma que se garanticen el derecho a la defensa y los principios de igualdad y de contradicción. Habrán de practicarse por los medios más rápidos y eficaces que permitan su adecuada constancia y las circunstancias esenciales de la misma.

Aunque este Decreto se encuentra actualmente derogado, es importante puntualizar que el redactor de la norma, incluyó en la citada disposición que los actos de comunicación (llámense citaciones o notificaciones) deben practicarse por los medios más rápidos, idóneos y eficaces, para de esta manera garantizar el derecho a la defensa de las partes.

Considera el mismo Decreto legislativo y específicamente en el artículo 56 en los ordinales 4 y 5 que para procedimientos laborales se permite que los actos de comunicación judicial puedan llevarse a cabo utilizando transmisión de textos, medios electrónicos, telemáticos, infotelecomunicaciones, o cualquier otra clase de medios y en soportes de cualquier naturaleza, siempre que tengan plena validez y eficacia y para ello debe cumplirse con los requisitos exigidos por las leyes españolas, admitiendo por ello, la utilización de los actos de comunicación judicial por medios no tradicionales.

En el año 2000, España dicta en fecha 7 de enero, la Ley 1/2000 de Enjuiciamiento Civil[21], en la misma el legislador sienta bases para permitir que los ciudadanos puedan comunicarse con la administración de justicia a través de plataformas técnicas que permitan el envío y la recepción de escritos y

20 Aunque el este Decreto fue derogado en 2011, resulta de utilidad en cuanto pone de manifiesto que las citaciones o notificaciones deben practicarse por los medios más rápidos, idóneos y eficaces, para de esta manera garantizar el derecho a la defensa de las partes. Véase: Noticias jurídicas: Real Decreto Legislativo 2/1995, de 7 de abril, por el que se aprueba el Texto Refundido de la Ley de Procedimiento Laboral http://noticias.juridicas.com/base_datos/Laboral/rdleg2-1995.html. [Consulta: 2013, Febrero 12].

21 Boletín Oficial de Estado número 7 Ley 1/2000, de 8 de enero, sobre Enjuiciamiento Civil. [Documento en línea] Disponible en: http://civil.udg.edu/normacivil/estatal/LEC/default.htm. [Consulta: 2013, Enero 18].

viceversa, siempre que las oficinas judiciales dispongan de estos medios, todo con arreglo a lo dispuesto en los artículos 135.5.[22], y 162[23] *ejusdem*.

Con la entrada en vigencia de este instrumento legal, surgieron un sinfín de detractores que formularon críticas en cuanto a la inclusión de estos medios técnicos, por no existir para el momento de entrada en vigencia de ese instrumento legal, una estructura o plataforma tecnológica de la administración de justicia española, teniendo ésta que afrontar la inconsistencia del texto legal y la realidad del estrado, ya que, aun cuando la legislación fue expedita al incorporar los medios técnicos, no así la transformación sufrida de la planta judicial civil.

En enero de 2007, se dicta el Real Decreto 84/2007[24], que implementa en la administración de justicia española, el sistema informático de telecomunicaciones denominado Lexnet para la presentación de escritos y documentos, así como el traslado de copias y la realización de actos de comunicación procesal por medios

22 Artículo 135. Presentación de escritos, a efectos del requisito de tiempo de los actos procesales:

> 5. Cuando las Oficinas judiciales y los sujetos intervinientes en un proceso dispongan de medios técnicos que permitan el envío y la normal recepción de escritos iniciadores y demás escritos y documentos, de forma tal que esté garantizada la autenticidad de la comunicación y quede constancia fehaciente de la remisión y recepción íntegra y de la fecha en que se hicieren, los escritos y documentos podrán enviarse por aquellos medios, acusándose recibo del mismo modo y se tendrán por presentados, a efectos de ejercicio de los derechos y de cumplimiento de deberes en la fecha y hora que conste en el resguardo acreditativo de su presentación. En caso de que la presentación tenga lugar en día u hora inhábil a efectos procesales conforme a la ley, se entenderá efectuada el primer día y hora hábil siguiente.
>
> A efectos de prueba y del cumplimiento de requisitos legales que exijan disponer de los documentos originales o de copias fehacientes, se estará a lo previsto en el artículo 162.2 de esta Ley.
>
> Cuando la presentación de escritos perentorios dentro de plazo, por los medios técnicos a que se refiere este apartado, no sea posible por interrupción no planificada del servicio de comunicaciones telemáticas o electrónicas, el remitente podrá proceder a su presentaciónen la Oficina judicial el primer día hábil siguiente acompañando el justificante de dicha interrupción

23 Artículo 162. Actos de comunicación por medios electrónicos, informáticos y similares.

1. Cuando las oficinas judiciales y las partes o los destinatarios de los actos de comunicación dispusieren de medios electrónicos, telemáticos, infotelecomunicaciones o de otra clase semejante, que permitan el envío y la recepción de escritos y documentos, de forma tal que esté garantizada la autenticidad de la comunicación y de su contenido y quede constancia fehaciente de la remisión y recepción íntegras y del momento en que se hicieron, los actos de comunicación podrán efectuarse por aquellos medios, con el resguardo acreditativo de su recepción que proceda.

24 Boletín Oficial de Estado número 38. (2007 febrero, 13). Real Decreto 84/2007, de 26 de enero, sobre implantación en la Administración de Justicia del sistema informático de telecomunicaciones Lexnet para la presentación de escritos y documentos, el traslado de copias y la realización de actos de comunicación procesal por medios telemáticos. [Documento en línea] Disponible en: http://noticias.juridicas.com/base_datos/Admin/rd84-2007.html [Consulta: 2013, Enero 18].

telemáticos que, está constituido por un diseño basado en un correo electrónico seguro que proporciona máxima certeza y fiabilidad en la comunicación mediante la utilización de firma electrónica reconocida, que otorga garantía de autenticidad –ya que, el emisor del documento es quién dice ser y no otro–, además de asegurar la integridad del mensaje –pues el contenido del documento no puede alterarse durante su transmisión– y cerciorar el no repudio debido.

Caballero de la Torre[25] (2004) define a Lexnet como *"Una plataforma de intercambio seguro de información entre una gran diversidad de agentes que en su trabajo diario o por cualquier circunstancia necesitan operar con la Justicia"*. De manera que este escenario electrónico, ha sido la conjunción de la fusión de distintos estándares tecnológicos, donde se ha optado por la utilización de lenguajes, herramientas, protocolos, en Red cerrada o Intranet, para la constitución de un sistema de comunicaciones electrónicas que permite el intercambio de mensajes de datos que están blindados por mecanismos de protección como la firma electrónica reconocida, el sellado de tiempo y la custodia de mensajes.

3. El sistema Lexnet

El procedimiento utilizado consiste en un sistema amigable e informático de comunicaciones que permite el intercambio de información en formato electrónico de forma segura entre los órganos judiciales y los distintos agentes verbigracia procuradores, fiscales, graduados sociales entre otros. De allí que se establezca que el funcionamiento del sistema de Red cerrada y correo electrónico seguro modelo español Lexnet, es semejante al proceso de envío de un correo electrónico, por ser este un mecanismo automatizado y mecánico de transmisión de información fuera de línea u off line, que no requiere que el usuario esté en frente de su computadora y conectado al sistema en tiempo real para poder recibir la información.

Todo ello es posible gracias a que se compila la información que es enviada por el sistema Lexnet, mediante un proceso mecánico y automatizado de trabajo, consistente en la remisión (envío) y la recepción íntegra de la comunicación judicial de citación o de la notificación y de su contenido por medio del mensaje de datos.

La información es almacenada en los buzones electrónicos que se alojan en el servidor de correo Lexnet y que a través del programa informático o *webmail* provee una interfaz web que permite la circulación correcta y sencilla de información entre varias aplicaciones, es decir, permite que al abrirse el correo

25 CABALLERO DE LA TORRE, M (2004) "Lexnet un sistema de información para la notificación telemática y la cooperación" [Documento en línea] Disponible en: http://www.csi.map.es/csi/tecnimap/tecnimap_2004/comunicaciones/tema_04/4_021.pdf. [Consulta: 2009, Febrero 12], p. 21.

que contiene la información se verifique la conversión del cifrado de información que conlleva a una información ininteligible, a, una inteligible a través de imágenes y palabras que hacen verificar el mensaje de datos y sus adjuntos.

Sin embargo es de hacer notar que la diferencia entre este sistema y los correos electrónicos genéricos, es que Lexnet, es un sistema de Red cerrada y de correo electrónico seguro que proporciona la máxima certeza y fiabilidad para los usuarios del sistema. Todo ello es atribuido, a que el mensaje recibido es blindado mediante un sistema criptográfico (mensaje cifrado) que requiere de existencia y uso de claves privadas que proporciona seguridad, a la par de la inclusión de una firma electrónica reconocida y enviada por la autoridad competente bajo los cánones de certeza, garantizando, por tanto, la integridad, confidencialidad y autenticidad de las comunicaciones que son recibidas en esa página de correo.

La firma electrónica segura y la incorporación de gestión electrónica de procesos comunicacionales judiciales en aspectos operacionales de los requisitos y estructuras de las comunicaciones, hacen que coincidan los tiempos de estos dos momentos de la gestión jurídica, vale decir permite fluir la información que soporta los actos de comunicación judicial; además de hacer seguimiento tanto del envío como de la recepción y lectura de las comunicaciones judiciales, la lectura del expediente, el estado de la causa, entre otros.

3.1 Funcionamiento

3.1.1. Condiciones de ingreso

El usuario del sistema debe ser abogado, ya que el sistema de Red cerrada y correo electrónico seguro Lexnet, está dirigido exclusivamente al uso profesional de los sujetos que intervienen directamente en los procesos judiciales debiendo introducir la tarjeta criptográfica (que contiene el certificado digital) que es emanado de la Autoridad de la Certificación de la Abogacía (ACA) en un lector de tarjetas –que le es entregado al usuario al momento de su certificación–. Estas tarjetas autentican y cualifican a sus poseedores. Cada usuario deberá utilizarla como su identificación digital. Será imprescindible su posesión para utilizar Lexnet. Por ello, el usuario no certificado no podrá ingresar al sistema *Webmail* de Lexnet.

A continuación el usuario, deberá entrar en la página web del colegio de abogados de residencia, donde aparecerá el enlace directo a Red Abogacía Lexnet.

La Red de Lexnet, le reconocerá como un usuario certificado y le solicitará introducir un PIN (que es el número de la tarjeta que le ha sido dado con el kit de instalación del sistema) que puede equipararse a una clave de cifrado privada que permite el ingreso del usuario al sistema. Subsiguientemente, se abrirá en la

página principal del sistema Lexnet una ventana o menú, donde se aprecian los servicios de informática jurídica de gestión que se ofrecen por el sistema Lexnet.

3.1.2. Presentación de escritos

Para la presentación de escritos al órgano judicial[26] se utilizan mensajes de datos y archivos adjuntos, que contendrán la demanda y los anexos que sean necesarios, teniendo que llenar el abogado presentante por esta vía un formulario que contendrá como menciones obligatorias: el remitente (nombre del abogado, código de abogacía), el destinatario (nombre y código de órgano judicial, del código de la oficina de reparto que es la oficina de registro telemático asociada al órgano judicial destinatario) y asunto como si se tratase de un correo electrónico simple, y que enviará a un destinatario del correo, siendo éste el órgano judicial que considere, ya que el destinatario real de los escritos no es más que la Oficina de Registro Telemático, puesto que esta oficina tiene por función repartir al órgano judicial que corresponda la información. Este acto, implicará el envío de una diligencia de presentación.

La presentación de escritos por el abogado supone de forma implícita el uso de la firma digital, es decir, los datos que ha declarado van a ser firmados digitalmente con su certificado Autoridad de Certificación de Abogacía y serán almacenados con las necesarias medidas de seguridad, para tener certeza de veracidad del escrito.

3.1.3. Envío de comunicaciones judiciales: citaciones y notificaciones

Las oficinas judiciales que han recibido el mensaje de datos que reúne las exigencias contenidas en el punto anterior, hacen el envío –como si se tratara de la remisión de su par el correo electrónico– del mensaje de datos contentivo

26 Véase Red de Abogacía Lexnet (2005). "Manual de Usuario". Documento en línea. Disponible en: http://documentacion.redabogacia.org/docushare/dsweb/Get/Document-25350/Manual+usuario+LexNet++v2.1.pdf. [Consulta: 2009, Febrero 12], p.11.

También podrá darse por notificado quien tuviere mandato expreso para ello, directamente por ante el Tribunal de Sustanciación, Mediación y Ejecución del Trabajo respectivo.

El Tribunal, a solicitud de parte o de oficio, podrá practicar la notificación del demandado por los medios electrónicos de los cuales disponga, siempre y cuando éstos le pertenezcan. A efectos de la certificación de la notificación, se procederá de conformidad con lo establecido en la Ley Sobre Mensajes de Datos y Firmas Electrónicas en todo cuanto le sea aplicable, atendiendo siempre a los principios de inmediatez, brevedad y celeridad de la presente Ley. A todo evento, el Juez dejará constancia en el expediente, que efectivamente se materializó la notificación del demandado. Al día siguiente a la certificación anteriormente referida, comenzará a correr el lapso para la comparecencia de las partes a la audiencia preliminar. Parágrafo Único: La notificación podrá gestionarse por el propio demandante o por su apoderado, mediante cualquier notario público de la jurisdicción del Tribunal.

de la comunicación judicial de las notificaciones y comunicaciones a los usuarios que están registrados en la base de datos de Lexnet, que está conformada por la estructura de los órganos judiciales y de los Colegios Profesionales que residen en el directorio de dicho sistema.

En el supuesto que el usuario de Lexnet sea abogado acreditado con certificado digital proporcionado por la Autoridad de Certificación de Abogacía (ACA) y que forme parte de la base de datos de los usuarios del sistema fuera directamente demandado, la comunicación enviada por el órgano judicial a través de esta vía se convertiría de notificación a una citación por vía de correo electrónico seguro y certificado. De allí que es válido indicar que con el sistema Lexnet, se puede enviar no sólo notificaciones sino también citaciones judiciales electrónicas.

El funcionario judicial que ha generado en el sistema de gestión procesal (*Workflow*) dichas comunicaciones judiciales, deberá hacer click a la aplicación de Lexnet, para que las comunicaciones sean enviadas, de forma múltiple, mecánica y automática, tanto al abogado –usuario registrado– así como al Colegio de Procuradores o abogados.

Paralelamente, el buzón del colegio de procuradores devolverá al órgano judicial correspondiente por medio de correo electrónico un acuse de recibo marcando la fecha del envío, equivaliendo este documento a la diligencia de notificación. De allí que, el sistema de forma automatizada enviará el acuse de recibo para evitar que el destinatario del correo electrónico pueda excusarse de la recepción del mensaje alegando desconocer el recibo de dicha diligencia.

En todo caso el usuario que desee verificar el correo electrónico, deberá hacer click en el enlace o vínculo buzón oficial, en el cual se desplegarán las carpetas que comprenden los ítems de: bandeja de entrada, aceptados, diligencias de presentación, acuses de recibo.

En la bandeja de entrada, se muestran las notificaciones o comunicaciones enviadas por los órganos judiciales, tal como si se tratase del sistema de correo electrónico.

Igualmente en la misma carpeta de bandeja de entrada, el sistema da la información del número total de mensajes y, también, del número de ellos no leídos.

Estos mensajes (escritos, citaciones y notificaciones) una vez depositados a través de los medios electrónicos en los buzones virtuales de los usuarios, se encontrarán accesibles por un período de treinta días pasado ese tiempo, comenzarán a borrarse del sistema.

Ahora bien, cuando se recibe un mensaje (documento notificación o citación), en la bandeja de entrada se va a visualizar la información de cabecera del mismo y se debe hacer click en el link verificarlo para conocer el contenido del mismo.

En la ventana denominada acuse de recibo, el sistema enviará si la operación ha finalizado correctamente, una orden automática en donde se acusa el recibo

del documento con el contenido íntegro del escrito enviado (documento principal y documentos anexos). En el acuse de recibo, se especifica la fecha de recepción del mensaje en el sistema y la fecha de recepción en el buzón electrónico del usuario así como de la sala virtual del colegio de procuradores.

Por tanto, si el destinatario accede a revisar el acto de comunicación y documentos anexos depositados en su buzón virtual, el sistema genera un resguardo electrónico dirigido al remitente, reflejando fecha y hora de la recepción del aviso.

3.2. Ventajas del sistema

El ahorro del papel a través de la utilización del sistema Lexnet, es una de las ventajas más obvias ya que, no es necesario imprimir las comunicaciones judiciales puesto que, el soporte que las contiene es electrónico, y, para comprobar su existencia, sólo se requiere el acuse de recibo marcando la fecha de envío del mensaje de datos y la fecha de recepción en el buzón electrónico del usuario; cosa que es imposible en el sistema de correo certificado con aviso de recibo, donde debe utilizarse el papel no sólo para la compulsa de las copias del libelo de demanda así como para la orden de comparecencia, sino también en el formulario de comprobación de aviso de recibo, situación que genera despilfarro de papel, tinta, firmas y sellos que son necesarios para la citación del demandado por vía de correo electrónico con aviso de recibo y que en caso de no ser verificables anulan lo actuado.

En cuanto al ahorro de tiempo, es de indicar que la autoridad judicial y los funcionarios de la administración de justicia no deben desplazarse para enviar las comunicaciones judiciales fuera de los tribunales, ya que sólo basta que los funcionarios judiciales inviertan unos pocos minutos para ingresar a la plataforma especializada Lexnet, y descargar al sistema la comunicación, en tanto que la para la verificación de las comunicaciones por parte del usuario también existe un ahorro de tiempo, ya que, el usuario podrá obtener la información con tan sólo ingresar al sistema cosa que podría hacer desde la comodidad de su hogar o desde su trabajo, o dentro o fuera de España.

La seguridad de este sistema debe ser considerada como otra ventaja, ya que se garantiza en todo momento la confidencialidad, integridad y autenticidad de la información cosa que es dada gracias al proveedor de certificación de servicios, quien es el ente encargado de asegurar que el mensaje de datos que contiene el correo electrónico seguro y que es enviado por el sistema Lexnet, no ha sido falsificado, ni alterado, y que los datos utilizados para su generación pueden producirse sólo una vez.

4. Futuro de la comunicación judicial de citación en el proceso civil venezolano, realizada por el sistema de Red cerrada de correo electrónico seguro, tomando en consideración el modelo español Lexnet

Es indudable señalar que aún cuando el sistema presenta varias ventajas, es necesario recordar que para usar el sistema Lexnet es indispensable ser abogado y usuario del sistema, y esto sólo es posible en España siempre y cuando se cumplan los requerimientos de inscripción en el Colegio de Procuradores y se obtenga la la acreditación de certificado digital Lexnet y posteriormente la clave para ingreso en esa plataforma.

En caso que el sistema judicial venezolano quisiera implementar un modelo como el sistema Lexnet, debería hacer una inversión tecnológica, que permita crear, e implementar un sistema *Webmail* similar al Lexnet; que responda a los requerimientos, realidades y necesidad de la administración de justicia venezolana, junto a una modificación legislativa como la realizada en España, que permita la posibilidad cierta de la aplicación del modelo de plataforma electrónica que facilitaría la gestión judicial, además, de una preparación previa y profunda tanto para los funcionarios judiciales, como para los usuarios del sistema, que, están acostumbrados a las gestiones judiciales de forma manual y por sistemas tradicionales.

Por tanto, una opción alternativa para la práctica segura de actos comunicacionales judiciales por medios no tradicionales, sería la implantación de un sistema similar a la plataforma Lexnet ya que, permite que los funcionarios judiciales puedan enviar la citación como acto de comunicación, por vía segura así como notificaciones a los demandados.

En este punto es necesario señalar que en materia laboral, existe un antecedente legislativo y práctico, en cuanto a las notificaciones electrónicas al apoderado judicial del demandado, establecida esta figura en el artículo 126 de la Ley Orgánica del Trabajo (2002)[27], permitiendo con ello, que se puedan realizar en el procedimiento laboral, notificación por medios electrónicos de los cuales disponga el demandado, siempre que sea a instancia de parte, o, de oficio.

Todo ello, en función de orientar el proceso laboral bajo la concepción de la humanización de la justicia prevista en la Constitución de la República Bolivariana

27 Artículo 27 Gaceta Oficial de la República Bolivariana de Venezuela N° 37.507 extraordinaria de fecha agosto 13, 2002: Admitida la demanda se ordenará la notificación del demandado, mediante un cartel que indicará el día y la hora acordada para la celebración de la audiencia preliminar, el cual será fijado por el Alguacil, a la puerta de la sede de la empresa, entregándole una copia del mismo al empleador o consignándolo en su secretaría o en su oficina receptora de correspondencia, si la hubiere. El Alguacil dejará constancia en el expediente de haber cumplido con lo prescrito en este artículo y de los datos relativos a la identificación de la persona que recibió la copia del cartel. El día siguiente al de la constancia que ponga el Secretario, en autos, de haber cumplido dicha actuación, comenzará a contarse el lapso de comparecencia del demandado.

de Venezuela, vale decir, implementando mecanismos que conlleven a un procedimiento judicial laboral más eficaz, que dé respuesta a las necesidades judiciales que involucran al colectivo o interés social, debiendo éste mecanismo de notificación prevalecer, frente a las exigencias marcadamente formales del procedimiento ordinario.

Por ello, la administración de justicia civil ordinaria, debe considerar la modernización del sistema judicial venezolano, con la implementación de plataformas electrónicas que se asemejen a Lexnet o que mejoren el sistema en referencia, permitiendo con ello, la electrónificacion del sistema judicial venezolano en lo que respecta a las notificaciones y citaciones a los demandados en procesos civiles ordinarios y la implementación de medios necesarios para poder implementar la informática jurídica de gestión.

V. Consideraciones finales

Con la entrada en vigencia de la Constitución de la República Bolivariana de Venezuela del año 2000, se establecieron las bases necesarias para la implementación de un vuelco legislativo que incluya el uso de las TIC en diversos ámbitos del quehacer diario, y de manera puntual al actuar del Estado en sus diversas operaciones y tareas propias que debe involucrar la informática jurídica y especialmente la informática jurídica de gestión.

Verbigracia de lo anterior, se evidencia en el hecho de que el Estado venezolano a fin de mejorar el acceso a la justicia y acercarla a la ciudadanía colocó en marcha a finales del año 2000, el *Sistema Juris 2000* en los tribunales del trabajo, atendiendo a un modelo organizacional integrado de gestión, documentación y decisión, que agiliza la atención a los ciudadanos, en donde, el Poder Judicial venezolano consiente de consolidar una justicia que responda a los requerimientos de la sociedad venezolana actual, ha implantado el uso de las tecnologías al servicio de la gestión judicial o en otras palabras la informática jurídica de gestión, que permita entre otras cosas instrumentar mecanismos de divulgación de la documentación jurídica, mediante el empleo de las TIC.

Por tanto, la presencia de los medios electrónicos no es una práctica aislada de legislaciones foráneas, sino una realidad en el ordenamiento jurídico venezolano, luego de la entrada en vigencia de la Constitución de la República, que ha permitido el aprovechamiento de las bondades de las TIC, para facilitar y simplificar la vida del ciudadano frente a las exigencias administrativas del Estado y en especial de aquellas que se generan en la gestión judicial para así mejorar el acceso a una justicia transparente, segura y confiable mediante la realización de los actos de comunicación procesal en materia laboral por medios electrónicos que buscan asegurar una tutela judicial efectiva que tiende a la celeridad, y a la ejecución eficaz del acto.

Con todos estos avances legislativos y organizacionales del poder judicial y en especial, el referido al ámbito procesal laboral extraña sobremanera que la

legislación procesal venezolana, no haga pronunciamiento alguno de la inclusión de los medios electrónicos en materia de procedimientos civiles ordinarios como especiales.

De todo lo anterior, se debe colegir que sería descontextualizado pensar que el ordenamiento patrio no está sufriendo una transformación producto de la inclusión de las TI C, ya que sustentado en las leyes promulgadas y los decretos dictados y vigentes que promueven la inclusión de medios tecnológicos y mecanismos de sistematización de los procedimientos administrativos de gestión, se puede pensar en una futura (más no lejana) adaptación del Derecho procesal civil a los avances tecnológicos, que puede ser inspirados por la experiencia legislativa y práctica tomando en consideración el sistema español, así como del modelo procesal laboral venezolano, que constituyen antecedentes para poder incorporar en materia procesal civil venezolana, comunicaciones judiciales a nivel de citaciones y notificaciones realizadas por medios electrónicos como vía de emplazamiento alternativo y de esta manera hacer uso de la tecnología en el campo jurídico con la incorporación de informática jurídica de gestión.

Uso de las Tecnologías de la Información y la Comunicación: protección jurídica a la infancia y adolescencia en Venezuela

Arelys Beatriz Pérez Sánchez*

SUMARIO: I. Introducción. II. Tutela constitucional. III Protección legal de los niños, niñas y adolescentes. IV. Marco jurídico aplicable a la infancia y la adolescencia en Venezuela. V. La pornografía infantil y los delitos informáticos. VI. Uso de las Tecnologías de la Información y Comunicación en el delito de pornografía infantil. VII. Conclusiones.

Resumen

La mayor parte de los países han regulado el uso de las Tecnologías de la Información y la Comunicación (TIC) a efectos de prevenir la comisión de delitos, especialmente la pornografía infantil. En Venezuela destacan la Ley Orgánica para la Protección del Niño y el Adolescente, y la Ley Especial contra Delitos Informáticos. El presente artículo estudia el caso de la difusión y exhibición de material pornográfico de niños y adolescentes, realizadas mediante el uso de las TIC en el Derecho venezolano.

Palabras claves: Niños. Adolescentes. Pornografía infantil. Delito informático.

Abstract

Most countries have regulated the use of Information Technology and Communication (ICT) in order to prevent crime, especially child pornography. In Venezuela the Organic Law for the Protection of Children and Adolescents, and the Special Law against Cybercrime stand out. This paper studies the case of dissemination and exhibition of pornography of children and adolescents by using ICT in Venezuelan Law.

Keywords: Children. Adolescents. Child pornography. Cybercrime.

Recibido: 4/1/2014 • Aceptado: 15/2/2014

* Abogada de la Universidad Católica del Táchira Venezuela. Especialista en Derecho Mercantil de la Universidad de los Andes. Especialista en Planificación Gerencial de la Universidad Nacional Experimental de los Llanos Occidentales Ezequiel Zamora. Doctoranda en Ciencias mención Derecho, en la Universidad Central de Venezuela

I. Introducción

Actualmente la Sociedad de la Información[1], considerada en el marco de los derechos humanos de cuarta generación, ante el acelerado y dinámico uso de la Tecnologías de la Información y la Comunicación (TIC), dadas las necesidades imperantes en tiempo y espacio, universalmente protege el pilar fundamental que lo constituye la familia con sus principios y valores humanos, para alcanzar el respeto, la libertad, la dignidad, la reputación y el honor conforme a la moral, la justicia, el bien común y seguridad jurídica basada en las nomas nacionales e internacionales, orientadas a proteger los derechos humanos.

En Venezuela, con la entrada en vigencia de la Constitución de la República Bolivariana de 1999[2] (CRBV), se inquiere tal como se desprende de su preámbulo, como:

> …fin supremo de refundar la República para establecer una sociedad democrática, participativa y protagónica, multiétnica y pluricultural en un Estado de justicia, federal y descentralizado, que consolide los valores de la libertad, la independencia, la paz, la solidaridad, el bien común, la integridad territorial, la convivencia y el imperio de la ley para esta y las futuras generaciones; asegure el derecho a la vida, al trabajo, a la cultura, a la educación, a la justicia social y a la igualdad sin discriminación ni subordinación alguna; promueva la cooperación pacífica entre las naciones e impulse y consolide la integración latinoamericana de acuerdo con el principio de no intervención y autodeterminación de los pueblos, la garantía universal e indivisible de los derechos humanos, la democratización de la sociedad internacional, el desarme nuclear, el equilibrio ecológico y los bienes jurídicos ambientales como patrimonio común e irrenunciable de la humanidad[3].

Puede afirmase, como lo señala Casal[4] al fijar posición respecto de la Carta Magna: "*no escapa a esta tendencia. Más bien es cabal expresión de la voluntad de asegurar los derechos humanos entendiendo estos en un sentido amplio que abarca a los proclamados internacionalmente y a los consagrados en la Constitución*", por ello del mismo texto constitucional se desprende en su artículo 2[5]:

1 TÉLLEZ VALDÉS, Julio. *Derecho Informático*. México. Mc Graw Hill.p.7. "*aquella que habilita a todas las personas y sin distinciones de ningún tipo para crear, recibir, compartir y utilizar información y conocimientos que permitan promover su desarrollo económico, social, cultural y político*".

2 BREWER CARIAS, Allan R. "*La Constitución de 1999*". Editorial Jurídica Venezolana. Caracas, 2000.

3 *Ibídem*. p. 25.

4 CASAL Jesús María, *Los Derechos Humanos y su Protección.* Estudio sobre derechos humanos y derechos fundamentales, UCAB, Caracas, 2009. Tercera Edición. p. 46.

5 BREWER C., *op.cit*. p. 25.

> Venezuela se constituye en un Estado democrático y social de Derecho y de Justicia, que propugna como valores superiores de su ordenamiento jurídico y de su actuación, la vida, la libertad, la justicia, la igualdad, la solidaridad, la democracia, la responsabilidad social y en general, la preeminencia de los derechos humanos, la ética y el pluralismo político.

Los cuales conlleva en su artículo 3[6]:

> El Estado tiene como fines esenciales la defensa y el desarrollo de la persona y el respeto a su dignidad, el ejercicio democrático de la voluntad popular, la construcción de una sociedad justa y amante de la paz, la promoción de la prosperidad y bienestar del pueblo y la garantía del cumplimiento de los principios, derechos y deberes reconocidos y consagrados en esta Constitución.

Lo que significa que el texto constitucional considera la preeminencia de los derechos humanos como valores superiores en la normativa legal interna, y lo deja sentado cuando menciona la dignidad de las personas y la garantía de sus derechos como principales fines del Estado, que al ser plasmados en su articulado constituyen materia objeto de regulación en el sistema legal del ordenamiento jurídico, para ser objeto de interpretación y aplicación jurídica por los entes competentes para tales efectos.

Con el acceso y uso de las Tecnologías de la Información y la Comunicación (TIC) se crean instrumentos legales que establecen los mecanismos de uso y acceso, tanto el adecuado como el inapropiado que en determinadas circunstancias traspasan los límites legales y sociales permitidos, y se convierten en conductas atípicas que llegan a configurarse como actos delictivos a objeto de ser regulados por el ordenamiento jurídico. La afluencia de todas la personas que interactúan dentro de la Sociedad de la Información hace necesario adoptar medidas de control para prevenir e impedir el uso abusivo de las TIC, tratando de controlar todo tipo de acto ilícito contrario a la dignidad, reputación, privacidad e intimidad de las personas, por atentar contra la moral y las buenas costumbres, como sería el caso de la difusión o exhibición de material pornográfico y la exhibición de pornografía infantil donde se involucren el uso de las TIC, por cuanto sería necesario y primordial garantizar los derechos del niño, niña y adolescente en su más amplia esfera, protegiendo su intimidad, privacidad y reputación.

En este mismo orden puede afirmarse que conforme a Carta Magna indicada supra, se "reconocerá el interés público de la ciencia, la tecnología, el conocimiento"[7], y dentro de ello se destaca la importancia de la estipulación jurídica mediante un texto legal que regule el derecho informático, así como todos los tipos de conductas atípicas y delictuales derivada de hechos punibles

6 *Ibídem*. p 25 y ss.
7 *Ibídem*. p. 63.

como consecuencia de la delincuencia organizada, pedofilia, acoso y abuso sexual infantil, pornografía, trata y explotación a niños, niñas y adolescentes cometido mediante el uso de las TIC. Todo ello, con la finalidad de garantizar los derechos humanos fundamentales y cumplir con las garantías constitucionales en pro de la infancia y la adolescencia, por ello el Estado busca regular, proteger y controlar el uso ilícito de las TIC, y así poder establecer estrategias y acciones adecuadas al uso lícito de las TIC. Desde esta perspectiva nace la importancia y justificación del presente trabajo, desarrollado sobre la base de la normativa legal vigente para la protección de los niños, niñas y adolescente en el sistema jurídico venezolano.

II. Tutela constitucional

El texto constitucional está enmarcado bajo la noción del género, reconociendo a los niños, niñas, adolescentes, jóvenes, adultas y adultos, ancianos y ancianas, personas con discapacidad, como sujetos plenos de obligaciones y derechos en justicia, siendo susceptibles de protección integral, contempla la obligatoriedad del respeto y garantía de los derechos humanos por los órganos del Poder Público, señalando la identidad étnica y cultural, con políticas de inclusión social.

Desde la perspectiva, la Carta Magna del 1999, logra cumplir uno de los principales preceptos, del poder Constituyente en materia de derechos humanos referidos específicamente a la infancia y la adolescencia, que se traduce en reconocer e incorporar expresamente los avances de los últimos cuarenta años en la materia *in comento*, tanto en la doctrina como en los tratados, convenios suscritos y ratificados por la República, y la jurisprudencia internacional. Lo que se manifiesta al desarrollar la Convención sobre los Derechos del Niño y, sobre todo, el paradigma sobre el cual haya su fundamento: basado en la doctrina de la protección integral a la infancia y adolescencia. Así consagra, el artículo 78 del Capítulo V de los Derechos Sociales y de las Familias[8], del Título III ejusdem. Todo se remonta al 20 de noviembre de 1989 cuando la Asamblea General de las Naciones Unidas aprueba, por unanimidad, la Convención Internacional Sobre los Derechos del Niño (CIDN), que representa la incorporación de las concepciones doctrinarias en los sistemas jurídicos.

Considerando que la CIDN transformó las necesidades fundamentales en derechos. Antes, el niño tenía necesidades. Después tiene derechos. La diferencia reside en la exigibilidad de esos derechos, es decir, la Convención diferenció entre la infancia y la Ley. Se cambió el término niño como sujeto tutelado, por el niño como sujeto de derechos, entendiéndose la facultad para demandar, actuar, proponer y asumir responsabilidades. Es decir, se concibe al niño como persona en desarrollo, con derechos y responsabilidades inherentes a todos los seres humanos, todo ello conforme a la nueva forma de convivencia

8 *Ibídem*. p. 51 y SS.

social, que reconoce a los niños y adolescentes como fundamentales a la población que debe recibir del Estado y los adultos toda la atención necesaria para su pleno desarrollo y desenvolvimiento, y que además se les garantice el derecho a participar activamente en todo lo que le sea permitido conforme a derecho, es por lo que vale considerar, que Venezuela ratifica la Convención y la hace Ley de la República el 29 de agosto de 1990 (Gaceta Oficial N° 34.541), asumiendo el compromiso de brindar a los niños y adolescentes protección integral en dos aspectos: protección social mediante un conjunto de actividades dirigidas a las condiciones para el desarrollo de la personalidad, satisfacer básicas y garantizar sus derechos fundamentales y la protección jurídica cuando crea leyes para hacer exigibles los derechos consagrados en la Convención y por la creación de instancias administrativas y judiciales cuando los derechos sean amenazados o violados.

Tomando en cuenta que la Carta Magna, consagra las TIC y su importancia en sus artículos 108 y 110, al establecer que los medios de comunicación social, públicos y privados, deben contribuir a la formación ciudadana, y en tal sentido, señala que el Estado garantizará servicios públicos de radio, televisión y redes de bibliotecas y de informática, con el fin de permitir el acceso universal a la información. Asímismo, los centros educativos deben incorporar el conocimiento y aplicación de las nuevas tecnologías, de sus innovaciones.

Por las razones expresas, el Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación, sus aplicaciones y los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional; aunado a ello garantizará el cumplimiento de los principios éticos y legales que deben regir las actividades de investigación científica, humanística y tecnológica. La ley determinará los modos y medios para dar cumplimiento a esta garantía, es por lo que debe tomar en consideración los casos especiales, como nos corresponde en el presente trabajo, referido a los niños, niñas y adolescentes.

Sobre la base del citado texto constitucional vale considerar, que el Estado enmarca su actuación dentro de los valores superiores del ordenamiento jurídico, mediante el cual toda persona tiene derecho a la protección por parte del Estado a través de los órganos de seguridad ciudadana regulados por ley, frente a situaciones que constituyan amenaza, vulnerabilidad o riesgo para la integridad física de las personas. En tal sentido, los cuerpos de seguridad del Estado respetarán la dignidad y los derechos humanos de todas las personas, conforme a la ley.

Es por lo que el artículo 60 consagra el derecho a la protección del honor, vida privada, intimidad, propia imagen, confidencialidad y reputación de las personas, además, la ley limitará el uso de la informática para garantizar el

honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derecho, siendo de gran importancia los niños niñas y adolescentes. El Estado venezolano tiene como función primordial proteger a las familias como asociación natural de la sociedad y como el espacio fundamental para el desarrollo integral de las personas. También garantizará la protección a la madre y al padre, por cuanto los niños, niñas y adolescentes tienen derecho a vivir, ser criados o criadas y a desarrollarse en el seno de su familia de origen. Igualmente señala en el artículo 78:

> Los niños, niñas y adolescentes son sujetos plenos de derecho y estarán protegidos por la legislación, órganos y tribunales especializados, los cuales respetarán, garantizarán y desarrollarán los contenidos de esta Constitución, la Convención sobre los Derechos del Niño y demás tratados internacionales que en esta materia haya suscrito y ratificado la República. El Estado, las familias y la sociedad asegurarán, con prioridad absoluta, protección integral, para lo cual se tomará en cuenta su interés superior en las decisiones y acciones que les conciernan. El Estado promoverá su incorporación progresiva a la ciudadanía activa, y creará un sistema rector nacional para la protección integral de los niños, niñas y adolescentes.

Por tal motivo, la Constitución en su Título III, Capítulo V, artículo 78, ordena la creación de un Sistema Rector Nacional para la Protección Integral de los Niños, Niñas y Adolescentes, disposición que se ve materializada en el artículo 117 de la Ley Orgánica para la Protección de Niños, Niñas y Adolescentes. También puede señalarse el artículo 79, a los fines de considerar que los jóvenes tienen el derecho y el deber de ser sujetos activos del proceso. Tomando en cuenta que el Estado desarrolla políticas públicas dirigidas a la protección de la infancia y adolescencia en Venezuela, que dan preponderancia al respeto de sus derechos sociales, con el fin de alcanzar mayores niveles en su calidad de vida

III. Protección legal de los niños, niñas y adolescentes

El Estado venezolano desarrolla políticas públicas con enfoque de derechos humanos, en especial las relacionadas con temas como: la salud, la educación, deporte y recreación, integración social y cultural, la seguridad social, el derecho a la vivienda y la protección a la familia, dentro de ella considerándose con especial énfasis a los niños, niñas y adolescentes.

La Ley Orgánica de Protección del Niño y el Adolescente (LOPNNA)[9] fue promulgada con el objeto de garantizar a todos los niños, niñas y adolescentes, en el territorio nacional, el ejercicio, de sus derechos y garantías, a través de la

9 Ley Orgánica de Protección del Niño y el Adolescente Gaceta Oficial Nº5.859 del 10 de diciembre de 2007.

protección integral a la sociedad y a familia. En el marco de este texto, la definición de niño niña y adolescente se desprende de su artículo 2:

> Se entiende por niño o niña toda persona con menos de doce años de edad. Se entiende por adolescente toda persona con doce años o más y menos de dieciocho años de edad. Si existieren dudas acerca de sí una persona es niño o adolescente, niña o adolescente, se le presumirá niño o niña, hasta prueba en contrario. Si existieren dudas acerca de sí una persona es adolescente o mayor de dieciocho años, se le presumirá adolescente, hasta prueba en contrario.

En tal sentido, las disposiciones de esta Ley se aplican por igual a todos los niños, niñas y adolescentes, sin discriminación alguna fundada en motivos de raza, color, sexo, edad, idioma, pensamiento, conciencia, religión, creencias, cultura, opinión política o de otra índole, posición económica, origen social, étnico o nacional, discapacidad, enfermedad, nacimiento o cualquier otra condición de los niños, niñas o adolescentes, de su padre, madre, representante responsable, o de sus familiares. Asimismo reconoce que los niños, niñas y adolecentes con necesidades especiales tienen todos los derechos y garantías consagrados y reconocidos por la Constitución y las leyes, además de los inherentes a su condición, para así asegurarles el pleno desarrollo de su personalidad y el goce de una vida plena y digna. Con programas de asistencia integral, rehabilitación e integración, programas de atención, orientación y asistencia dirigidas a su familia, campañas de difusión, orientación y promoción social dirigidas a la comunidad. También regula el derecho de las minorías, a tener su propia vida cultural, a profesar y practicar su propia religión o creencias y a emplear su propio idioma, especialmente aquellos pertenecientes a minorías étnicas, religiosas, lingüísticas o indígenas.

El citado texto legal consagra las obligaciones generales del Estado de tomar todas las medidas administrativas, legislativas y judiciales para asegurar que todos los niños y adolescentes disfruten plena y efectivamente de sus derechos y garantías; por otra parte establece la corresponsabilidad del Estado, las familias y la sociedad en la defensa y garantía de los derechos de los niños, niñas y adolescentes, para asegurar, con prioridad absoluta, su protección integral, tomando en cuenta el interés superior, en las decisiones y acciones que les conciernan.

Por las razones expuestas, el Estado tiene la obligación garantizar la protección del niño, niña y adolescente contra el abuso y la explotación sexual, la información e imágenes inadecuadas, el honor, reputación, propia imagen, vida privada e intimidad familiar, por cuanto de la misma ley se desprende la prohibición de exponer o divulgar, a través de cualquier medio, su imagen en contra de su voluntad o de su padre, madre, representantes o responsables. En ese mismo orden, se prohíbe exponer o divulgar datos, imágenes o informaciones,

a través de cualquier medio, que lesionen el honor o la reputación de los niños, niñas y adolescentes o que constituyan injerencias arbitrarias o ilegales en su vida privada o intimidad familiar.

Según la LOPNNA, el Estado considera como prioridad absoluta todos los derechos y garantías de los niños, niñas y adolescentes, entre los cuales comprende: a) la formulación y ejecución de todas las políticas públicas, b) asignación privilegiada y preferente en el presupuesto de los recursos públicos para políticas y programas de protección integral, c) precedencia de los niños, niñas y adolescentes en el acceso y la atención a los servicios públicos, y d) primacía de los niños, niñas y adolescentes en la protección y socorro en cualquier circunstancia.

En este mismo orden, el citado texto legal señala en su artículo 8 el interés superior de los niños, niñas y adolescentes al considerar: que es un principio de interpretación y aplicación de esta Ley, siendo de obligatorio cumplimiento en todas las decisiones concernientes a los niños, niñas y adolescentes. Este artículo está dirigido a asegurar el desarrollo integral de los niños, niñas y adolescentes, así como el disfrute pleno y efectivo de sus derechos y garantías. Para determinarlo se debe apreciar: a) la opinión de los niños, niñas y adolescentes, b) la necesidad de equilibrio entre los derechos y garantías y sus deberes, c) entre las exigencias del bien común y los derechos y garantías, d) entre los derechos de las personas y los derechos y garantías, e) la condición específica de los niños, niñas y adolescentes como personas en desarrollo. Por las razones expresas, cuando exista conflicto entre los derechos e intereses frente a otros derechos e intereses legítimos, prevalecerá el interés superior de los niños, niñas y adolescentes.

También gozan de todos los derechos y garantías consagrados en favor de las personas en el ordenamiento jurídico, especialmente aquellos consagrados en la Convención sobre los Derechos del Niño.

IV. Marco jurídico aplicable a la infancia y adolescencia en Venezuela

	Textos Legales	Publicación	Artículos
1	Constitución de la República de Bolivariana de Venezuela	1999. G. O. ExtraordinariaN° 5.453 del 24/03/2000	• Uso TIC: 108,110 • Protección infancia y adolescencia: 55, 60, 75, 78, 79
2	Ley Orgánica para la Protección de Niños, Niñas y Adolescentes	G.O. Nº 5.859 Extraordinaria 10/12/2007	• Prioridad absoluta:7 • Interés superior: 8 • Derechos, garantías y deberes: 10-116 • Sistema rector nacional de protección:117-119 • Delito: actuación, suministro, exhibición: 234-236 • Multa:248-252 • Procedimiento: 450 y SS. • Sistema penal de responsabilidad de adolescentes: 526 y SS. • Garantías: 528 y SS. • Recursos: 607 • Prescripción
3	Ley sobre Procedimientos Especiales en materia de Protección Familiar de Niños, Niñas y Adolescentes	G.O. Nº 39. 57009/12/2010	• Objeto: 1 • Finalidad: 2 • Ämbito de aplicación: 3 • Materia objeto de conciliación: 15 • Mediación: 34 y 35
4	Ley para la Protección de Niños, Niñas y Adolescentes en Salas de uso de Internet, Video, Juegos y otros Multimedias	G.O. Nº 38.529 25/09/2006	Uso adecuado de la información y mecanismos de seguridad: 8 y 10

5	Ley aprobatoria de la Convención sobre los Derechos del Niños	G.O. Nº 34.541 29/08/1990	17 y 34
6	Ley aprobatoria del Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la Venta, Prostitución Infantil y Utilización de los Niños en la Pornografía	G.O. Nº 37.355 02/01/2002	1, 2.c, 3 Nº-1.b, 10 Nº 1.3.
7	Ley para la Protección de las Familias, la Maternidad y la Paternidad	G.O. Nº 38.773 20/09/2007	1 y32
8	Ley Orgánica sobre el Derecho de las Mujeres a una vida libre de violencia	G.O. Nº 38.668 23/04/2007	15 Nº 18, 43 Párrafos 3 y 4, 44, 45, 55, 56, 70, 71
9	Código Penal Venezolano	G.O. Nº 5.768 13/04/2005	374 -382, 387-390
10	Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo	G.O. Nº 39.912 30/04/2012	1, 2, 4, 27, 28. 29.1, 37, 41, · • Pornografía del 46· • Difusión de material pornográfico: 47· • Utilización de niños, niñas o adolescentes en la pornografía: 48 Elaboración de material pornográfico infantil: 49
11	Ley de Proteción de Víctimas, Testigos y demás Sujetos Procesales	G.O. Nº 38.536 04/10/2006	1, 6, 8, 21, 23

12	Ley Especial contra los Delitos Informáticos	G.O. Nº 37.313 30/10/2001	• Objeto 1 • Extraterritorialidad de los delitos 3 • Sanciones principales y accesorias 4 • Responsabilidad de las personas jurídicas 5 • Difusión o Exhibición de material pornográfico 23 • Exhibición pornográfica de niños o adolescentes 24

V. La pornografía infantil y los delitos informáticos

Según el Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía[10], por prostitución infantil se entiende la utilización de un niño en actividades sexuales a cambio de remuneración o de cualquier otra retribución. La pornografía infantil se refiere a toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño, con fines primordialmente sexuales

Tomando como base la Ley de Estados Unidos de América, Sección 2256, la pornografía infantil es cualquier representación visual, incluyendo cualquier fotografía, filmación, video, pintura o una imagen generada por computador, hecha o producida por medios electrónicos o mecánicos, u otro medio, donde haya una conducta sexual explícita, donde la producción visual involucre el uso personas menores de edad en una conducta sexualmente explícita; o donde esa reproducción visual aparentemente involucre a un menor en una conducta sexual explícita; o donde esa representación visual haya sido creada, adaptada o modificada a fin de que un menor identificable esté involucrado; o esa producción visual es anunciada, promocionada, presentada, descrita o distribuida de tal manera que dé la impresión de que ese material contiene un menor en una conducta sexual explícita.

En relación con los delitos informáticos, conviene destacar la definición de Téllez Valdés, al señalar que los delitos informáticos son "*actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico)*

10 http://www2.ohchr.org/spanish/law/crc-sale.htm (Consulta: 30 de agosto de 2013)

o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)"[11].

VI. El uso de las Tecnologías de la Información y Comunicación en el delito de pornografía infantil

De acuerdo con este enfoque, al analizar los elementos que constituyen este delito, se hace necesario señalar el significado de tecnologías de información y los sistemas, según el artículo 2 de la Ley Especial contra Los Delitos Informáticos (LECDI):

> a) "Tecnología de información: rama de la tecnología que se dedica al estudio, aplicación y procesamiento de data, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, así como el desarrollo y uso del *hardware, firmware, software*, cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de data".

Lo cual considera Fuentes[12], como: "*…toda aquella tecnología que facilite el uso de la información de manera automática, a fin de lograr la (obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, entre otras)…*" "*…distribución, intercambio, transmisión o recepción, es decir serían estas las funciones inherentes, que implican o subsumen implícitamente el término tecnología de Información…*". Igualmente, del concepto se desprende la extensión del término para abarcar cualquier bien (tangible e intangible) que permita el cumplimiento de sus funciones.

De acuerdo con este enfoque, considera el citado autor que sistema, según la Ley Especial contra Los Delitos Informáticos[13], en su artículo 2 establece:

> b) Sistema: cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia para cumplir una serie de funciones especificas, así como la combinación de dos o más componentes interrelacionados, organizados en un paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas.

11 TÉLLEZ VALDÉS, Julio: Derecho Informático, op cit.

12 FUENTES PINZÓN, Fernando. Marco Legal de la Informática y La Computación, Venezuela, año 2007, *cit*., p. 274.

13 Ley Especial contra los Delitos Informáticos. Gaceta.Oficial No. 37313, de 30 de octubre de 2001.

Ante lo expuesto anteriormente, deja sentada su posición Fuentes[14], al señalar, que:

> Pues sistema será entonces, todo aquel proceso que permita el trabajo coordinado de un bien (físico o inmaterial) con otros bienes (tangibles o intangibles) basados en la tecnología de la información, siempre y cuando, dicha coordinación permita el cumplimiento de una función específica. Dentro de este concepto se abarcan, tanto a las computadoras como a los sistemas (*software*) operativos, pasando por las redes (*hardware* como programas de computación) que permitan la coordinación de los recursos y procedimientos informáticos.

Dentro de esta idea, en el delito mediante el uso de las TIC entra en juego el objeto material o jurídico protegido; en el caso que nos ocupa, se basa en la protección del interés superior del niño, niña y adolescente en Venezuela, y la acción como elemento constitutivo de este punible, implica el uso de la medios y tecnología informática como instrumento para la ejecución y materialización del delito, para obtener el fin. Esto equivale a que este delito no solo se consuma con el simple uso de la informática, también es necesario materializar la realización de actos de carácter físico y material, tal proceder debe ser culpable, ello equivale a que la acción u omisión debe ser intencional o culposa.

El uso de las TIC en el delito de pornografía infantil en Venezuela se encuentra tipificado en la LECDI, en el artículo 23, el cual prevé las debidas advertencias para que el usuario restrinja el acceso, es decir, la falta de advertencias o avisos preventivos en el uso de material reservado para personas adultas, se considera como un hecho punible del tipo delictual de acción pública que involucre a niños, niñas y adolescentes, en tal sentido es enjuiciable de oficio por las autoridades competentes a tales efectos del Poder Público nacional, estadal o municipal, lo cual implica que el sitio web o el medio por el que se realiza la exhibición, venta o transmisión, difusión de material pornográfico incurre en dicho delito cuando carezca de advertencias o avisos para evitar el acceso de los niños, niñas o adolescentes a dicho material de contenido pornográfico, tal como se desprende del artículo 23:

> Difusión o exhibición de material pornográfico. Todo aquel que por cualquier medio que involucre el uso de tecnologías de la información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

14 FUENTES PINZÓN, Fernando. Marco Legal de la Informática y la Computación, Venezuela, año 2007, *cit.*, pp. 274-275.

de crianza o vigilancia, es decir, la persona que explote comercialmente la actividad sexual del niño, niña o adolescente, en aras de la obtención de un lucro mediante esa actividad, y también hace la salvedad en los casos que las víctimas sean niñas o adolescentes, con competencia para conocer los tribunales especiales.

Empero, en el caso de la acción de provecho consecuencial del delito de explotación sexual, donde se aplica la LECDI, en ella se establecen sanciones para aquellas personas que por cualquier medio que involucre el uso de tecnologías de información difundan, distribuyan, publiquen o comercialicen fotos, videos o cualquier otro soporte mediante los medios informáticos, utilice a la persona o imagen de un niño o adolescente, o en caso que implique su explotación sexual, bien sea con fines exhibicionistas o de pornografía, es decir, la simple exhibición o el fin pornográfico sin fines de lucro, hace que se perfeccione el delito, contemplado en el artículo 24 de la LECDI, el cual establece:

> Exhibición pornográfica de niños o adolescentes. El que por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

Del análisis realizado a la norma *in comento*, puede afirmarse que el sujeto activo del delito se refiere a toda persona; y en caso de la acción criminal, es condición obligatoria que se ejecute mediante el uso de tecnologías de la información; y en lo que respecta al sujeto pasivo del hecho punible, el mismo para que sea calificado, debe tratarse de la persona de un niño(s), niña(s) o adolescente(s), y finalmente el bien jurídico protegido es el interés superior del niño, niña o adolescente en su desarrollo sano psíquico y socialmente (artículo 8 LOPNNA), el cual es prioridad absoluta del Estado venezolano, y conlleva sanción al autor del delito, de pena corporal (prisión de cuatro a ocho años) y pecuniaria (multa de cuatrocientas a ochocientas UT), consideradas como penas concurrentes, y por tratarse de materia especial que involucra a un niño(s), niña(s) o adolescente(s), es materia de orden público y sus delitos son enjuiciables por los órganos del poder público destinados a la administración de justicia en Venezuela.

VII. Conclusiones

Al profundizar en el uso de las TIC y la protección jurídica de la infancia y adolescencia en Venezuela, se concluye que el Estado venezolano ha manifestado a través de sus normas constitucionales y legales, su compromiso en la aplicación de los instrumentos jurídicos nacionales e internacionales, ya sean acuerdos, convenios y protocolos relativos a la protección de los derechos humanos para

Cabe aclarar según el marco normativo regulatorio que se desprende de la CRBV, que en el caso *in comento* el bien jurídico protegido o tutelado lo constituye el interés superior, la prioridad absoluta y el entorno sano del niño, niña o adolescente, consagrado en la LOPNNA, específicamente en los artículos 74, 78 y 79, que establecen la envoltura para los medios que contengan informaciones e imágenes inadecuadas para niños y adolescentes, la prevención contra juegos computarizados y electrónicos nocivos y prohibiciones para la protección de los derechos de información y a un entorno sano, en concordancia con los artículos 55, 60, 74, 75, 78 y 79 de la CRBV, que reconocen a los niños, niñas y adolescentes como sujetos de pleno derecho.

En otro orden de ideas, el acceso de menores de edad a contenidos restringidos, previstos en los artículo 234, 235 y 236 de la LOPNNA, se consideran como normas atenuadas al no tener el carácter de delito, por cuanto sus sanciones oscilan entre uno por ciento (1%) hasta el dos por ciento (2%) de los ingresos brutos causados en el ejercicio fiscal anterior y en otros casos de treinta (30 UT) a seiscientas (600 UT) unidades tributarias, a aquellas personas que vendan, suministren o entreguen a niños, niñas y adolescentes, videos, cassettes y material de difusión de imágenes o sonidos por medios eléctricos, computarizados o electrónicos en contraposición a esta ley, respecto del material restringido o calificado sólo para adultos.

No obstante, es de considerar que el citado texto legal, guarda silencio, es decir, existe una laguna jurídica ante tal esa acción, creando una incertidumbre jurídica en su aplicación, ya que la sanción existente para quien entregue esos contenidos por medios electrónicos o computarizados, de difusión o sonidos eléctricos es solo pecuniaria, en cambio de acuerdo con la LECDI; aquel que haya obviado la colocación de una advertencia respecto al material a ser visto o adquirido, si tendría una sanción privativa de libertad de dos a seis años y pena pecuniaria adicional, que comprende multa de doscientas (200 UT) a trescientas (300 UT) unidades tributarias .

En otro orden de ideas, es de señalar que la LOPNNA regula el delito de explotación sexual de niños, niñas y adolescentes, en el artículo 258, en los siguientes términos:

> Quien fomente, dirija o se lucre de la actividad sexual de un niño, niña o adolescente será penado o penada con prisión de cinco a ocho años.
> Si él o la culpable ejerce sobre la víctima autoridad, responsabilidad de crianza o vigilancia, la prisión será de seis a diez años.
> Si la o las víctimas son niñas o adolescentes, o en la causa concurren víctimas de ambos sexos, conocerán los Tribunales Especiales previstos en la Ley Orgánica sobre el Derecho de las Mujeres a una Vida Libre de Violencia, conforme el procedimiento en ésta establecido.

En tal sentido, el artículo establece que la acción antijurídica está dirigida de manera directa al autor, al director o si es autoridad, quien tiene la responsabilidad

el caso que nos ocupa, referido a la protección de los derechos de los niños, niñas y adolescentes, asumiéndolos como políticas públicas de Estado en cada uno de los organismos que lo conforman y como delitos de acción pública en caso de su violación.

En nuestra legislación informática, a pesar de no establecerse en la LECDI, que sus delitos sean de acción pública o privada, nos queda claro que la mayoría de los punibles allí previstos y contemplados taxativamente, son de acción pública, enjuiciables de oficio, muy especialmente en caso de involucrar como sujetos pasivos a los niños, niñas y adolescentes, por cuanto constituye un precepto constitucional, establecido y desarrollado en la LOPNNA.

Es de reconocer que Venezuela no escapa al incremento de la delincuencia mediante el uso de las TIC, a través de la criminalidad organizada. Ante esta situación, el poder legislativo ha creado las leyes para tratar de combatir esa modalidad del crimen que involucra niño(s), niña(s) o adolescente(s), señaladas en el marco legal donde destacan la LECDI, la LOPNNA, la LOCDOFT, la LOSDMVLV y el Código Penal entre otros, donde se debe tener presente los grados de participación de cada persona que infringe la ley y se le deba aplicar la vía procesal, respecto del procedimiento ordinario establecido entre los artículos 283 al 370 del Código Orgánico Procesal Penal[15].

Al indagar sobre los delitos informáticos en Venezuela está claro que se han incrementado, constituyendo una modalidad delictual muy usual, teniendo como principal característica la particularidad de que ocurren sin la percepción visual o material del colectivo, en tal sentido LOCDOFT, reconoce los delitos informáticos como hechos punibles de criminalidad organizada, aspecto que ciertamente resulta comprensible, traduciéndose ello en una fortaleza en cuanto al tratamiento jurídico e importancia de estos delitos en aras de la consolidación de mayores penas a las previstas en la legislación sustantiva informática interna, y por otra parte, se considera que trasciende la fronteras por cuanto en ella se permite la aplicación de la extraterritorialidad de la norma jurídica.

Es de señalar que el Estado venezolano reconoce que el abuso sexual y la explotación sexual comercial son problemas considerados y declarados por la comunidad internacional como un flagelo muy grave, que perjudica y atenta la dignidad del ser humano, en detrimento progresivo de la sociedad afectando la familia, y muy especialmente al niño, niña y adolescente como sujetos de derecho, por ello ha fortalecido los mecanismos para la implementación de políticas públicas y normas legales dirigidas a la protección integral de la infancia y la adolescencia, con el fin de asegurarle sus derechos fundamentales, y así poder constituir mecanismos de prevención, erradicación del abuso sexual, la explotación sexual, la difusión o exhibición de material pornográfico y de pornografía de niños, niñas y adolescentes.

15 Código Orgánico Procesal Penal. Gaceta Oficial No. 38.536, de 04 de octubre de 2006.

Es de criticar el desequilibrio normativo en cuanto al tratamiento de conductas relacionadas con el tema de la pornografía infantil, especialmente en lo que respecta al tratamiento que otorga la LOPNNA (artículo 235), respecto al acceso de menores de edad a contenidos restringidos, por cuanto es simple una infracción y no un delito, generando su comisión solo una sanción pecuniaria, no consagrando tipificación de penas corporales por estas acciones ilícitas. Empero, la LECDI establece sanción privativa de libertad y además pena pecuniaria accesoria, a toda persona que obvie las advertencias para el material pornográfico o reservado para adultos para ser visto o adquirido por niños, niñas y adolescentes.

Finalmente, es de reconocer que materialmente constituye una conducta más grave la que se encuentra contemplada en la LOPNNA, y en este caso el legislador lo considera como una simple infracción, con la aplicación de una leve sanción pecuniaria; y aquella conducta delictual que se considera penalmente como menos grave prevista en el sentido amplio de la legislación sustantiva, que la constituye la LECDI, y es considerada como un verdadero delito, al cual se le establece una sanción más grave que acarrea pena privativa de libertad (prisión) y pena accesoria (multa).

Comprobantes fiscales digitales y facturación electrónica

José Guadalupe Villegas Castillejos*

SUMARIO: I. Introducción II. ¿Qué son los comprobantes fiscales digitales? III. Requisitos fiscales para emitir comprobantes fiscales digitales. IV. ¿Qué es la facturación electrónica? V. Algunos ejemplos de la migración al nuevo modelo de facturación electrónica. VI. Ventajas y desventajas actuales de la facturación impresa y la electrónica. VII. El valor de los comprobantes fiscales digitales.

Resumen

La recaudación contributiva en México es importante, ya que es una de las bases principales del sustento del mismo, por lo que la incertidumbre y deseo de las autoridades fiscales, es realizar dicha actividad lo mejor posible, en este caso a través de la tecnología, dando como resultado los comprobantes fiscales digitales, y particularmente la facturación electrónica, teniendo como objetivo lograr un mejor control administrativo y sobre todo fiscal de los contribuyentes.

Palabras claves: Comprobantes fiscales. Facturación electrónica. Autoridad. Contribuyente.

Abstract

Effective tax revenue collection is of the utmost importance in sustaining Mexico's economy. Because of the uncertainties that fiscal authorities face; tax collection must be carried out in the technologically most efficient manner possible by producing digital fiscal receipts and, in particular, electronic invoices in order to achieve optimum administrative and –especially– fiscal control of taxpayers.

Key words: Tax Receipts. Electronic Invoices. Authority. Taxpayer.

Recibido: 14/5/2014 • Aceptado: 16/6/2014

* Maestría en Derecho Fiscal y estudiante del Doctorado en Ciencias Jurídicas. Profesor Investigador de tiempo completo en la Carrera de Derecho de la Universidad del Istmo, Campus, Ixtepec.

I. Introducción

Los aspectos históricos, políticos, culturales, científicos y técnicos, pero sobre todo en las actividades comerciales que en mayor parte obedecen a la globalización, han creado necesidades de nuevas tecnologías, mismas que son en ciertos casos indispensables para el cumplimiento o desarrollo de dichas acciones, por lo que México ha optado por la familiarización con éstas, dando como resultado reformas y adiciones a la legislación principalmente en materias civil, mercantil, y fiscal, promoviendo así el comercio electrónico, vigilando siempre el interés, seguridad y certeza jurídica del contribuyente, ya que al no contar físicamente con un documento que avale su operación genera desde un principio cierta inseguridad en el acto.

El encuentro entre las nuevas tecnologías y el Derecho es inevitable creando una realidad en una Sociedad de la Información, siendo imprescindible y urgente la creación de leyes que legalicen y sobre todo respalden las operaciones que realizan las personas a través de la tecnología. Tomando en consideración la grandes necesidades actuales de las nuevas sociedades en construcción.

Es por ello la realización del presente trabajo, que sin ser limitativo se desarrolla sobre la base del tema de los Comprobantes Fiscales Digitales (CFD), así como ejemplificar el tránsito o migración a este nuevo sistema electrónico que tuvo su auge a finales del año 2010 y principios de 2011, tecnologías que son las que respaldan fiscalmente las actividades comerciales de los contribuyentes –personas físicas y morales–, generando mayor eficacia en la Administración Pública, además de proteger jurídica y administrativamente las actuaciones de los sujetos involucrados.

II. ¿Qué son los comprobantes fiscales digitales?

Como bien se señala en líneas que anteceden, de todos los aspectos mencionados, en este caso únicamente se referirá acerca los comprobantes fiscales digitales, por lo que tomando en consideración la legislación en materia fiscal y administrativa, se conceptualizan como aquellos documentos digitales que demuestran fiscalmente las operaciones que realizan los contribuyentes, teniendo en cuenta que dichas actividades pueden materializarse en:

- **Facturas**. Es un documento que refleja la operación realizada entre dos o más personas, ya sea por compraventa, prestación de un servicio, así como la contraprestación pactada.

  > Documento que se expide para hacer constar una venta, en el que aparece la fecha de operación, el nombre del comprador, del vendedor, las condiciones convenidas, la cantidad, descripción, precio e importe total de lo vendido. Algunas veces se hace constar también el número de la factura, el nombre del comisionista

o agente vendedor, la forma del embarque y otros datos adicionales relativos a cada operación[1].

- **Recibos de honorarios**. Los generan los profesionales, artistas, técnicos y/o científicos, por prestar servicios independientes en áreas o temas específicos en los que son expertos.

- **Recibos de arrendamientos**. Es aquel documento que expide la persona física o moral denominado arrendador, a otra denominada arrendatario, por ocupar algún mueble o inmueble como por ejemplo: vehículos, local comercial o casa habitación, etc. Debiendo cumplir este último con todos los requisitos fiscales.

- **Recibos de donativos**. Es aquel documento que expiden las Instituciones autorizadas para recibir donativos, conteniendo los datos del donatario y del donante, cantidad, descripción de los bienes o en su caso, la cantidad donada para el cumplimiento del objeto social de dicha Institución.

- **Notas de cargo**. Se expide cuando no se cuenta con la factura correspondiente, es decir, cuando se hace constar en un documento al deudor que se le ha cargado determinada cantidad en su cuenta.

- **Notas de crédito**. Es un documento que expiden los vendedores para generar un crédito en la cuenta del comprador, cuando existen errores, descuentos, bonificación u otros motivos.

  Es la que se pasa a una persona avisándole haber hecho algún abono en su cuenta. Se registra en contabilidad deduciendo el importe a las ventas, por rebajas o bonificaciones, devoluciones, etc., con abono a clientes[2].

- **Carta de porte**. Es aquel documento que respalda jurídicamente el traslado de mercancías.

  Documento (título de crédito) por el cual una compañía o agencia de transporte terrestre, se compromete a entregar en determinado lugar, las mercancías que haya recibido para su transporte, a cambio de una retribución llamada flete[3].

1 ENRÍQUEZ PALOMEC, Raúl, *Léxico Básico del Contador*, México, D.F., 1990, Editorial Trillas, pág. 57.
2 *Id.*
3 *Id.*

- **Estado de cuenta**. Es el documento el cual sirve para cerciorarse que se encuentran registradas en contabilidad todas las transacciones bancarias. Debiéndose presentar en original y de acuerdo al artículo 29 del Código Fiscal de la Federación de México (CFF).

Respecto al concepto de comprobantes fiscales digitales mencionado al inicio del presente trabajo la legislación menciona el documento digital en el artículo 17-D (cuarto párrafo): Se entiende por documento digital todo mensaje de datos que contiene información o escritura generada, enviada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología[4].

Se retoma el significado anterior del CFF, para aclarar y enriquecer mejor el concepto de comprobante fiscal digital.

Dichas operaciones que realizan los contribuyentes contarán con requisitos indispensables principalmente mencionados en los artículos 29 y 29 A del CFF, así como del Código de Comercio y la Resolución Miscelánea Fiscal, para entonces poder ser tomados en cuenta por las autoridades en el momento de realizar las deducciones correspondientes, principal interés de los comprobantes fiscales digitales. Independientemente de la peculiaridad de cada una de dichas actividades.

III. Requisitos fiscales para emitir comprobantes fiscales digitales

1) Contabilidad en el sistema electrónico. Son sistemas contables, financieros fiscales y administrativos, que ayudan al contribuyente a tener un mejor control en sus operaciones, como por ejemplo, nóminas, pólizas, ingresos, costos, gastos, PTU, vacaciones, aguinaldo, etc., cumpliendo con las bases estipuladas por el artículo 28 fracción I y último párrafo del CFF.

2) Certificado de la Firma Electrónica Avanzada (FIEL). El servicio de Administración Tributaria menciona lo siguiente que: "Es un conjunto de datos que se adjuntan a un mensaje electrónico, cuyo propósito es identificar al emisor del mensaje como autor legítimo de éste, tal y como si se tratara de una firma autógrafa"[5].

El concepto anterior de la FIEL es muy claro y digerible sin embargo, se puede retomar de la doctrina otro, el cual refiere lo siguiente:

4 Código Fiscal de la Federación, México D.F., 2013.

5 http://www.sat.gob.mx/sitio_internet/e_sat/tu_firma/60_11498.html. [Consulta: 2013, agosto 06].

> La firma electrónica es el conjunto de datos en forma electrónica consignados, adjuntados o lógicamente asociados al mensaje de datos por cualquier tecnología, utilizados para: identificar al firmante en relación con el mensaje de datos; indicar que el firmante aprueba la información, y producir los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio[6].

El trámite de la FIEL se realiza ante dicho órgano desconcentrado, el Servicio de Administración Tributaria (SAT) de la Secretaría de Hacienda y Crédito Público, sus reformas y adiciones principales están en el CFF, en el Código de Comercio y en la Resolución Miscelánea Fiscal.

3) Certificado de sello digital. Se utilizarán únicamente para la emisión de los comprobantes fiscales digitales. Estos sellos permiten acreditar la autoría de los comprobantes fiscales digitales que emitan las personas físicas y morales en sus operaciones, avalado por la autoridad administrativa (SAT). Asimismo, los contribuyentes podrán optar por un certificado de sello digital para todos sus establecimientos, o en su caso, tramitar un certificado para cada establecimiento.

4) Solicitud de folios y series. Se realiza mediante el Sistema Integral de Comprobantes Fiscales (SICOFI) una vez que se cuenta con la FIEL, a través de la página de Internet del Servicio de Administración Tributaria. Estos folios y series ayudan al contribuyente a tener certeza jurídica para el proceso de facturación electrónica.

No se omite mencionar, que los folios asignados a los contribuyentes, así como el Código de Barra Bidimensional (CBB), se utilizaron a principios del año 2011, únicamente para la expedición de comprobantes fiscales impresos y tuvieron una vigencia de dos años contados a partir de la fecha de aprobación de la asignación de los mismos, cosa que en la actualidad ya fue suplido por la facturación electrónica.

5) Informe mensual de los comprobantes fiscales emitidos. Por cada factura electrónica emitida se utilizarán folios y series, por lo que el contribuyente está obligado a entregarle un informe mensual al SAT de los mismos, en caso de omitir dicho informe no autorizaran nuevos folios; y

6) Conservar los comprobantes fiscales digitales en medios electrónicos. Este requisito indispensable derivado del artículo 29, fracción V, tercer párrafo del CFF.

6 LEÓN TOVAR, Soyla H., et al, *La Firma Electrónica Avanzada*, México, D.F., 2005, 1ª Edición, Editorial Oxford University Press, pág. Prólogo.

> Para los efectos del artículo 29 fracción V, tercer párrafo, de CFF, los contribuyentes que emitan y reciban CFDI, deberán ser almacenados en medios magnéticos, ópticos de cualquier otra tecnología, en su caso formato electrónico XML.
>
> El SAT considera que se cumple con los requisitos para almacenar los CFDI establecidos en esta regla, cuando los contribuyentes almacenen y conserven los citados comprobantes sujetándose estrictamente a lo dispuesto por la Secretaría de Economía en la Norma Oficial Mexicana No. 151 vigente (NOM-151), publicada en el DOF y mantengan en todo momento a disposición del SAT los elementos necesarios para su verificación y cotejo[7]

El archivo y registro de los comprobantes fiscales digitales, son para el respaldo jurídico-fiscal con lo que cuentan los contribuyentes en caso de controversia, es por ello la mención de la Norma Oficial mexicana número 151 citada en el párrafo que antecede, misma que establece los requisitos a seguir para la conservación de los comprobantes fiscales digitales de manera más detallada.

IV. ¿Qué es la facturación electrónica?

Ahora bien, de los comprobantes fiscales digitales mencionados en líneas que anteceden, el presente trabajo principalmente se inclinará hacia la facturación electrónica, ya que es uno de los documentos que por lo general en el comercio su uso es más relevante, sin quitar o hacer a un lado la importancia de los demás. "*La factura es un documento que expide el vendedor, en el cual aparece la cantidad, descripción y precio del artículo o de los artículos vendidos*"[8].

El concepto anterior se limitó a observar una factura convencional, tomando en cuenta que el concepto es muy general y no considera a la facturación en materia de comprobación, sino más que nada como un documento que se deriva de una compraventa, refiriéndose a que la factura sea de manera impresa, al mencionar que en dicho documento debe aparecer la cantidad, descripción y precio del artículo, pero se debe recordar que las facturas pueden ser con bienes tangibles e intangibles; como por ejemplo: la compra de un bien mueble o la prestación de un servicio, en la que legalmente se debe expedir la factura correspondiente para garantizar la operación realizada, incluso no menciona los requisitos indispensables que lista la legislación para ser un comprobante fiscal, y entonces gozar de los beneficios fiscales que se derivan de los mismos.

7 Servicio de Administración Tributaria, *Primera Resolución de Modificaciones a la Resolución Miscelánea Fiscal para 2010 y sus Anexos 1-A y 20*. http://dof.gob.mx/nota_detalle.php?codigo=5159342&fecha=14/09/2010 [Consulta: 2013, octubre 03].

8 RAMÍREZ VALENZUELA, Alejandro, *Introducción al Derecho Mercantil y Fiscal*, México, D.F., 2004, Editorial Limusa, S.A. de C.V. Grupo Noriega Editores, pág. 89.

En vista de los detalles mencionados con antelación, se dejará por el momento a la facturación impresa, para poder definir a la facturación electrónica de la siguiente manera: es un mecanismo de comprobación y respaldo jurídico-fiscal por medios electrónicos para la generación, transmisión y resguardo de los documentos fiscales de manera digital, siempre observando los requisitos previos plasmados en la legislación del Derecho objetivo mexicano.

Con la reforma a la legislación actual, y las que en su momento se hicieron a finales del año 2010, en específico la que modificó al artículo 29 del CFF y las modificaciones a la Resolución Miscelánea Fiscal para 2010 y sus anexos 1-A y 20, en los que dispusieron que a partir del 1 de enero de 2011, se iniciara de manera paulatina el uso generalizado de la facturación electrónica, para que con ello, los contribuyentes expidieran documentos digitales como comprobantes por las actividades que realicen, independientemente cuál sea ésta.

Las reformas y adiciones a que se refiere el párrafo anterior, en un principio no eran obligatorias ya que eran reflejadas en cuerpos de leyes vigentes en el Derecho, pero es importante recalcar que dejan beneficios u opciones –anteriormente–, sobre todo para los contribuyentes que ya venían usando o generando la facturación electrónica hasta el treinta y uno de diciembre del año 2010, y aún así para los que se integraron o migraron al nuevo modelo de facturación electrónica a partir del primero de enero del año 2011, detalles que se tomarán en cuenta más adelante en el desarrollo del presente trabajo.

V. Algunos ejemplos de la migración al nuevo modelo de facturación electrónica

A manera de ejemplo y como se planteó en un principio, se estructuran los principales casos en los que se empezó a facturar electrónicamente, considerando la migración al nuevo modelo de facturación a partir del año 2011:

Contribuyentes que durante el ejercicio fiscal de 2010 hubieran obtenido ingresos acumulables iguales o menores a $ 4,000,000.00 pesos:

Cuadro 1

Usando comprobantes fiscales impresos o electrónicos antes hasta el 31//12/2010:
1. **Facturación por medios propios** (software o web).- En esta modalidad el contribuyente adquiere, desarrolla o renta un sistema para la emisión de los comprobantes directamente en su computadora, Esquema de facturación electrónica con vigencia indefinida, únicamente los que lo adoptaron durante 2010.Los software no requieren estar autorizados por el SAT, únicamente cumplir con los lineamientos informáticos del Anexo 20;

2. **Facturación por proveedor autorizado** (software o web). Facturación a través de un tercero vigente hasta el primer semestre de 2011, únicamente los que lo adoptaron durante 2010, ya que en caso de superar la cantidad mencionada, es una obligación pasar a comprobantes fiscales digitales a través de Internet en el segundo semestre de 2011;

3. **Facturación en papel por imprenta**. Se podrán seguir utilizando los comprobantes fiscales impresos por medio de un impresor autorizado siempre y cuando hayan sido impresos antes del 01 de enero de 2011.

Fuente: Elaboración propia (2013).

Cuadro 2

Usando comprobantes fiscales impresos o electrónicos a partir del 01//01/2011:
1. **CFDI** Para estos contribuyentes (ingresos menos de $4,000,000.00) lo podrán utilizar de manera opcional;
2. **Facturación en Papel con CBB** Será necesario solicitar la asignación de folios a través del portal SAT utilizando la FIEL. Una vez que han sido autorizados los folios, el SAT generará un archivo electrónico con la imagen de CBB, con vigencia de dos años. Se imprime en la impresora del contribuyente o a través de una imprenta, sin ser necesario que sea impreso por un impresor autorizado por el SAT. No se omite mencionar, que los contribuyentes podrán emitir comprobantes fiscales en papel con CBB en operaciones por cualquier monto.

Fuente: Elaboración propia (2013).

Contribuyentes que durante el ejercicio fiscal de 2010 hubieran obtenido ingresos acumulables mayores a $ 4,000,000.00 pesos:

Cuadro 3

Usando comprobantes fiscales impresos o electrónicos antes hasta el 31//12/2010:
1. **Facturación por medios propios (software o web)**. En esta modalidad el contribuyente adquiere, desarrolla o renta un sistema para la emisión de los comprobantes directamente en su computadora. Esquema de facturación

electrónica con vigencia indefinida, únicamente los que lo adoptaron durante 2010.Los software no requieren estar autorizados por el SAT, únicamente cumplir con los lineamientos informáticos del anexo 20;

2. **Facturación por proveedor autorizado (software o web)**. Facturación a través de un tercero vigente hasta el primer semestre de 2011, únicamente los que lo adoptaron durante 2010, ya que en caso de superar la cantidad mencionada, es una obligación pasar a comprobantes fiscales digitales a través de Internet en el segundo semestre de 2011; y

3. **Facturación en papel por imprenta**. Se podrán seguir utilizando los comprobantes fiscales impresos por medio de un impresor autorizado siempre y cuando hayan sido impresos antes del 01 de enero de 2011.

Fuente: Elaboración propia (2013).

Cuadro 4

Usando comprobantes fiscales impresos o electrónicos a partir del 01//01/2011:
1. **CFDI** Para estos contribuyentes (más de $4,000,000.00) es obligatorio su uso;
2. **Facturación en Papel con CBB** Al igual que en el caso anterior, los contribuyentes podrán emitir comprobantes fiscales en papel con CBB solo en operaciones menores a $2,000.00. **NOTA**.- De acuerdo con las disposiciones de las Reglas de la Resolución Miscelánea Fiscal 201-2011 en la etapa de transición en los meses de enero a marzo de 2011, los contribuyentes obligados a expedir CFDI, podrán expedir comprobantes en papel con dispositivo de seguridad independientemente al monto de la operación.

Fuente: Elaboración propia (2013).

Los cuadros comparativos antes descritos, diferencian dos épocas de facturación electrónica, primeramente tomando en cuenta la facturación hasta el treinta y uno de diciembre del año 2010, y en el segundo caso considerando el nuevo modelo que empieza a partir del primero de enero del año 2011, diferencias y ventajas por la migración al nuevo sistema que el contribuyente por medio de un especialista en la materia, debió analizar en su momento para obtener los mejores beneficios en su aplicación, y no entrar en controversia con la autoridad.

VI. Algunas ventajas y desventajas actuales de la facturación impresa y la electrónica

1. Por lo regular el costo de una factura impresa es de alrededor más de tres pesos o más por un tiraje de más de 100 facturas, esto tomando en cuenta que el papel es más o menos atractivo, ya que si se requiere una factura con un diseño especial, con colores de tinta y logotipos diferentes, el costo se elevaría, aunado al daño ecológico y casi irreparable que se provoca a consecuencia de la impresión de papel.

2. En caso que se tenga que enviar físicamente la factura, se tiene que utilizar mensajería, reflejándose en la contratación del mensajero y el tiempo que tardaría éste en entregarla pudiendo ser local o foránea, la cantidad de facturas –por paquetería–, y la certeza que llegue a su destino, o en su caso la contratación de los servicios de una empresa que se encargue del despacho de las facturas, entre otras cosas.

Con la factura electrónica el costo es considerablemente mucho más bajo y el manejo es más sencillo, sin tener que contratar a personal o a terceros para su manejo, ya que simplemente se envía por correo electrónico, o por medio de una memoria externa.

3. Se debe recordar que el artículo 30 del CFF obliga a conservar la documentación y contabilidad por cinco años, con la finalidad que la autoridad pueda verificar en su momento las operaciones de los contribuyentes. Por lo que con la factura impresa el contribuyente debe contar con un almacén físico en un área de su empresa totalmente acondicionado para el caso, y además contratar gente cuidadosa que se encargue del mismo y sobre todo para el manejo de las facturas, ya que, en caso de pérdida o extravío de alguna habrían muchos problemas y generarían gastos y tiempo al contribuyente, y más aún si se quema o roban el almacén.

En el caso de la factura electrónica, el almacén es virtual, puesto que la base de datos se podrá tener en una computadora o bien realizar algunas copias como respaldo en caso de pérdida o robo de la misma, y archivarla en otras computadoras o memorias. De igual forma se puede conservar la base de datos en Internet y la información estaría segura. Incluso existen en la red páginas gratuitas para realizar este tipo de almacenamiento a través de la web. En caso de robo total de los archivos guardados en formato electrónico, se podría pedir una copia de los mismos que se enviaron a los clientes con antelación, teniendo dichos archivos el carácter de original, ya que en los documentos digitales una copia es igual que el original, y no hay diferencia entre ambos.

4. Si se pierde una factura impresa se tendría que recurrir a un trámite administrativo como por ejemplo: la realización de un protocolo de certificación a una copia y entregársela al cliente o incluso jurídico para reponerla.

En caso de la factura electrónica se le vuelve a enviar al cliente, y si éste lo requiere se le envía de manera impresa por medio del formato PDF como lo establece la legislación fiscal.

> Portable Document Format, PDF (Formato de Documento Portable) formato gráfico creado por la empresa Adobe que reproduce cualquier tipo de documento en forma digital idéntica, facsímil, permitiendo así la distribución electrónica de los mismos a través de la red en forma de ficheros PDF. El programa gratuito Acrobat Reader, de Adobe, permite la visualización de los mismos[9].

Tomando en consideración lo antes expuesto, seguramente la mayoría de los contribuyentes confiarán por mucho los trámites con la facturación electrónica, independientemente que ya sea obligatorio en todo México. Además de darse cuenta que este mecanismo ayuda a mejorar los trámites, además de agilizarlos, añadiéndole que su costo es aún más atractivo, en comparación con los costos que genera la facturación impresa, dejando a un lado el temor al cambio con la tecnología, incertidumbre que se dejará atrás con la familiarización y aplicación de las nuevas tecnologías.

VII. El valor de los comprobantes fiscales digitales

El Derecho busca la igualdad, legalidad, seguridad y equidad, entre otros principios. Es una protección con la que cuenta principalmente el gobernado frente a la autoridad, por lo que todas las operaciones deben estar siempre respaldadas jurídicamente debido a las consecuencias que originen dichas actividades, es por ello la importancia del valor que la legislación le ha otorgado a los documentos electrónicos, para evitar controversias y sobre todo pérdidas en las inversiones y obligaciones de los contribuyentes.

En materia jurídica, fiscal, administrativa, laboral, mercantil, civil, etc., y en caso de duda o inconformidad respecto a las obligaciones para con la autoridad o entre particulares, se debe recurrir a un proceso –de cualquier materia– para demostrar que las actuaciones fueron apegadas a derecho, y para darle legitimidad a los documentos, y es ahí, en el momento procesal en donde se debe demostrar, a la luz de las leyes los hechos, a través de diversos medios de pruebas y de documentación fehaciente que los avale. "*El proceso es la solución heterocompositiva, es decir, la solución imparcial, a cargo de un órgano de autoridad del Estado, el juzgador, que interviene a instancia*

9 TÉLLEZ VALDÉS, Julio, *Derecho Informático*, México, D.F., 2004, Tercera Edición, Editorial McGRAW-HILL/INTERAMERICANA EDITORES, S.A. DE C.V., págs. 489 y 490.

de una de las partes y cuya autoridad deriva del imperio del propio Estado y de la fuerza de la Ley"[10].

Parte indispensable de un proceso en materia jurídica, sin lugar a dudas son las pruebas, ya que a través de ellas el juzgador podrá conocer fehacientemente la historia narrada por los sujetos involucrados. "*Los medios de prueba son los elementos necesarios para la consecución de un fin. En la materia probatoria los medios de prueba están constituidos por los elementos del conocimiento que llevan la finalidad de producir una convicción en el juzgador*"[11].

De acuerdo con lo anterior y de conformidad con el Derecho, durante el proceso para argumentar un dicho, principalmente se utiliza las siguientes pruebas: la documental, confesional, testimonial, pericial, inspección judicial y la presuncional legal y humana, demostrando la razón.

A continuación y respecto a las diversas pruebas referidas por la legislación actual, lo siguiente se inclinará hacia las pruebas documentales. "*El documento es la representación material idónea para poner de manifiesto la existencia de un hecho o acto jurídico (acontecimiento independiente de la voluntad humana, contrato, testamento, sentencia, etc.), susceptible a servir, en caso necesario, como elemento probatorio*"[12].

Un concepto amplío dejando abiertas muchas opciones por cual decidir como por ejemplo: los documentos impresos, las películas, fotografías, discos, etc.

Sin lugar a dudas la prueba documental es una de las más certeras y verosímiles, con las que se puede convencer a las autoridades de nuestras operaciones y actividades, ya que se ven reflejadas de manera palpable en un documento, sin mencionar que, en los documentos impresos se pueden manifestar las voluntades por medio de las firmas autógrafas de los que en ellos intervienen, o en su caso, con las huellas dactilares.

Lo anterior, refleja una ventaja enorme en los documentos impresos, pero entonces los documentos electrónicos de qué manera pueden ser tan confiables como los impresos, si su esencia es esa, el de no ser impresos. Lo idóneo, es trabajar sobre los medios de prueba de los documentos electrónicos, y crear en ellos la seguridad y garantía de legalidad.

Al principio del presente trabajo se hizo referencia del concepto de documento digital, sin embargo, para mayor abundamiento, se refiere lo siguiente:

> Técnicamente el documento electrónico es un conjunto de impulsos eléctricos que recaen en un soporte de computadora, y que sometidos a un adecuado

10 OVALLE FAVELA, José, *Teoría General del Proceso*, México, D.F., 2001, Quinta Edición, Editorial Oxford University Press México, S.A. de C.V., pág. 30.

11 ARELLANO GARCÍA, Carlos, *Práctica Forense Mercantil*, México, D.F., 2009, Primera Edición, Editorial Porrúa, S.A. DE C.V., pág. 352.

12 DE PINA VARA, Rafael, *Diccionario de Derecho*, México, D.F., 1965, Editorial Porrúa, S.A., pág. 116.

> proceso, permiten su traducción al lenguaje natural a través de una pantalla o una impresora.
>
> Cabe aclarar que lo que se lee en la pantalla o lo impreso no son el documento electrónico original sino copias, ya que el original no se podrá utilizar directamente, debido a que su contenido no puede ser aprehendido por nuestros sentidos[13].

Los procesos tecnológicos y los procesos legislativos son totalmente diferentes y actualmente unos avanzan mucho más rápido que los otros, razón por la cual el documento electrónico tiene muchos cuestionamientos y desconfianza, basados en la discrepancia entre los desarrollos tecnológicos y las leyes.

Sin embargo, en varias legislaciones se contemplan los requisitos de los documentos digitales, y sobre todo los procedimientos a seguir en caso de controversia, como por ejemplo: El CFF, el Código de Comercio, Código Federal de Procedimientos Civiles, entre otras; inclusive en la Ley Federal de Procedimiento Contencioso Administrativo, ya contempla los juicios en línea, mismo que se le conoce como: "*Substanciación y resolución del juicio contencioso administrativo federal en todas sus etapas, así como de los procedimientos previstos en el artículo 58 de esta Ley, a través del Sistema de Justicia en Línea*"[14].

Siendo el juicio en línea una realidad jurídica en la actualidad de México.

> Artículo 210-A.- Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.
>
> Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta.
>
> Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta[15].

Es así, que la legislación de manera escueta, pero confiable, protege a los documentos digitales, por lo que se debe empezar aplicar lo que se tiene, y

13 TÉLLEZ VALDÉS, Julio, *Derecho Informático*, México, D.F., 2004, Tercera Edición, Editorial McGRAW-HILL/INTERAMERICANA EDITORES, S.A. DE C.V., pág. 247.

14 *Ley Federal de Procedimiento Contencioso Administrativo*, México, D.F., Art. 1-A fracción XIII.

15 Código Federal de Procedimientos Civiles, México, D.F.

avanzar a la par con la tecnología. A veces se escucha hablar de documentos electrónicos y más aún cuando se trata del pago con el carácter de contribuyente –pago de contribuciones–, al instante se piensa en inseguridad, probabilidad de ser alterados, la duda de que si son auténticos, que si la autoridad lo va tratar como un documento totalmente válido, etc., entre muchas cosas más. Pensamientos quizá un poco extremos pero realmente sucede.

Los comprobantes fiscales digitales jurídicamente son válidos, toda vez, que como bien se menciona, antes diversas legislaciones le dan ese carácter de legitimidad, además que al igual como los comprobantes fiscales impresos pueden ser signados, los digitales constan de una firma electrónica avanzada, firma digital, sello digital, con lo cual autentica al mismo.

Por ello es que, los comprobantes fiscales digitales en la legislación fiscal vigente los adopta como totalmente válidos y exigibles. Tal es el caso que aproximadamente desde el año 2005 se han venido aplicando, por lo que no se debe tener inseguridad alguna al momento de presentarlos, eso sí, cumpliendo con los requisitos establecidos. Por ello y por su gran relevancia en el impacto social, que con el nuevo modelo de los comprobantes fiscales digitales plasmados en el CFF y sobre todo en materia de facturación electrónica les otorga certeza jurídica. Considerando que en lo que se debe trabajar es en la simplicidad para poder realizarlos de manera que se cumplan con los requisitos previamente establecidos y de forma puntual. Los comprobantes fiscales digitales eran solo un proyecto para muchos en años anteriores, pero en la actualidad son una realidad y una exigencia para todos, además de ser utilizados por las autoridades y los contribuyentes de forma rutinaria.

El acto administrativo electrónico en Venezuela

Mónica Rivera Cajas*

SUMARIO: I. Aspectos preliminares: Modernización de la función administrativa en Venezuela a través del uso de medios electrónicos. II. Definición clásica de acto administrativo y de acto administrativo electrónico. III. Tratamiento legal y jurisprudencial del acto administrativo electrónico en Venezuela. 1. Marco legal 2. Jurisprudencia del Tribunal Supremo. IV. Validez del acto administrativo electrónico en Venezuela. V. Conclusiones.

Resumen

La presente investigación estudia el uso de las Tecnologías de Información y la Comunicación en la Administración Pública en Venezuela. Al ser el acto administrativo electrónico una de sus principales manifestaciones, resulta relevante analizar el contexto legal y jurisprudencial que afecta el reconocimiento de la validez jurídica de este tipo de actos.

Palabras claves: Acto administrativo electrónico. Tecnologías de la Información y la Comunicación. Medios electrónicos.

Abstract

This research studies the use of Information Technology and Communication in the Public Administration in Venezuela. As the electronic administrative act is one of its main manifestations, it is relevant to analyze legislation and case law that affects the legal standing of that kind of acts.

Keywords: Electronic Administrative Act. Information Technology and Communication. Electronic Means.

Recibido: 15/7/2014 • Aceptado: 16/8/2014

* Abogada egresada de la Universidad Católica Andrés Bello (UCAB). Especialista en Derecho Laboral (UCAB), Especialista en Derecho Procesal (UCAB) y cursante del Postgrado de Derecho Administrativo (UCAB). mrivera@sidor.com / monicarivera1970@hotmail.com

I. Aspectos preliminares: modernización de la función administrativa en Venezuela a través del uso de medios electrónicos

Con el objetivo de lograr la simplificación de los trámites administrativos y la debida eliminación de los que se consideren innecesarios, la Administración Pública debe garantizar el cabal cumplimiento de los principios que rigen su actividad, tales como: economía, celeridad, simplicidad administrativa, rendición de cuentas, eficacia, eficiencia, proporcionalidad, oportunidad, objetividad, imparcialidad, participación, honestidad, accesibilidad, uniformidad, modernidad, transparencia, buena fe y responsabilidad en su ejercicio.

En este sentido, los órganos y entes de la Administración Pública deben considerar la implementación de tecnologías, la utilización de medios electrónicos e informáticos para la consecución de sus fines fundamentales, destacándose que la misma se encuentra al servicio de las personas para la atención de sus requerimientos y satisfacción de sus necesidades. A tales efectos, la Administración Pública debe garantizar los derechos de las personas vinculados con ésta, así como le corresponde velar por el progreso de sus procedimientos y servicios de conformidad con los lineamientos y políticas del Estado.

Los beneficios que involucran las nuevas formas de comunicación y transmisión de información, así como la transferencia y almacenamiento de documentos, estimulan a que se considere la incorporación de las Tecnologías de la Información y las Comunicaciones (TIC), en especial el uso de los recursos informáticos y electrónicos al ámbito de las actividades de la Administración Pública, y especialmente a los procedimientos administrativos, todo ello en el marco del desarrollo del gobierno electrónico en Venezuela, por lo que son obvias las ventajas que implica su aplicación a las relaciones entre la Administración Pública y los particulares, quienes podrán realizar innumerables gestiones, incluso sin necesidad de movilizarse de un lugar a otro, lo que se traduce en ahorro de tiempo y costo, mayor eficacia y eficiencia por la reducción de los trámites, lo que implica mayor seguridad y facilidad en las diligencias que se realicen ante la Administración.

El ordenamiento jurídico venezolano contiene normas de rango constitucional y legal, cuyo objeto se orienta a regular el hecho informático y/o electrónico aplicado a las actividades gubernamentales, estableciendo las bases para propiciar el desarrollo y la consolidación de la Administración Pública electrónica, y en consecuencia, del gobierno electrónico. A partir de la entrada en vigencia de la Constitución de la República Bolivariana de Venezuela de 1999 (CRBV), se dio impulso al nacimiento y desarrollo de normativas para construir un marco legal actualizado, dirigido a preparar un entorno propicio para la aplicación de los servicios informáticos y/o electrónicos en el campo de la actividad administrativa de los entes u órganos del Estado, constituyéndose en un medio para que el Estado emita respuestas oportunas a las nuevas exigencias de los

ciudadanos, se reduzcan los trámites excesivos, la duplicación de esfuerzos y predomine la celeridad y oportunidad necesarias.

En este contexto, la Constitución de la República Bolivariana de Venezuela en su artículo 110, reconoce como de interés público la ciencia, la tecnología, el conocimiento, la innovación y los servicios de la información, como medios vitales para lograr el desarrollo económico, social y político del país. Asimismo, conviene resaltar lo establecido en los artículos 5, 10 y 151 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública (LOPA), su orientación a la simplificación de los trámites administrativos, incorporando tecnologías y empleando cualquier medio electrónico o informático para el cumplimiento de los fines de la Administración Pública. Vale resaltar que en los epígrafes subsiguientes se desarrollará el resto de la normativa que regula la materia en el contexto nacional.

Una de las manifestaciones de la implementación de los mecanismos informáticos y electrónicos, se concreta en tres experiencias de gran trascendencia en el país, como han sido la de CADIVI (Comisión de Administración de Divisas, la cual fue suprimida por la asunción inmediata y progresiva de sus competencias por el Centro Nacional de Comercio Exterior - CENCOEX- a través del Decreto N° 904, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 40.393, de fecha 14 abril de 2014), la del SENIAT (Servicio Nacional Integrado de Administración Tributaria) y la del SAIME (Servicio Administrativo de Identificación, Migración y Extranjería), órganos adscritos a los distintos Ministerios con competencia en la materia. Estos órganos en su actividad administrativa utilizan constantemente las tecnologías de información en las solicitudes, en el intercambio electrónico de datos e información, con la finalidad de mejorar su gestión pública y los servicios que prestan a los particulares, cumpliendo con los recaudos y requisitos determinados en el ordenamiento jurídico administrativo.

Por otra parte, es necesario mencionar que los principios que rigen el procedimiento administrativo no se modifican con la implementación de la tecnología, sino que ésta se adecua a ellos perfeccionándolos, y de acuerdo con lo previsto en el artículo 30 de la Ley Orgánica de Procedimientos Administrativos (LOPA), la actividad administrativa debe desarrollarse conforme a los principios de economía, eficacia, celeridad e imparcialidad, e igualmente debe considerarse el principio de interpretación progresiva del derecho.

Ante los avances en la incorporación de TIC en los órganos y entes de la Administración Pública, resulta interesante ahondar en la problemática legal en torno a la validez del acto administrativo expedido por medios electrónicos, según las disposiciones que regulan la materia y obviamente de conformidad con las normas que sustentan la actuación administrativa, así como analizar el tratamiento que la jurisprudencia del Tribunal Supremo de Justicia le ha dado en nuestro país.

En este contexto, se pretende profundizar en aspectos como la incidencia de la modernización de la función administrativa a través del uso de medios electrónicos, en la definición clásica de acto administrativo y de acto administrativo electrónico, en el tratamiento legal y jurisprudencial del acto administrativo electrónico en nuestra Nación y finalmente, desarrollar el tema de la validez del acto administrativo electrónico en Venezuela.

Por último, no podemos dejar de considerar que de conformidad con el artículo 2 de la CRBV, nos encontramos en presencia de un Estado democrático y social de Derecho y de Justicia, y de acuerdo con el artículo 141 *ejusdem*, la Administración Pública se encuentra al servicio de los ciudadanos, sometida a los principios que la informan, estando subordinada al ordenamiento jurídico, por lo que la Administración y los particulares pueden relacionarse desde una perspectiva jurídica a través de TIC, siempre en cumplimiento de las formalidades de ley.

II. Definición clásica de acto administrativo y de acto administrativo electrónico

La definición legal del acto administrativo, en nuestra legislación, se encuentra en el artículo 7 de la Ley Orgánica de Procedimientos Administrativos (LOPA) como: "*toda declaración de carácter general o particular emitida de acuerdo con las formalidades y requisitos establecidos en la Ley, por los órganos de la Administración Pública*".

Algunos doctrinarios en la materia, manifiestan que la definición legal de acto administrativo señalada, excluye como tal, la declaración emanada de los entes de la Administración Pública, y en este sentido León, M. lo precisa como: "*toda actuación con destinatario general o particular, producida con base a un poder legal de derecho público, por los órganos y entes de la Administración Pública*"[1].

Asimismo, García, E. y Fernández, T. lo definen como: "*la declaración de voluntad, de juicio, de conocimiento o de deseo realizada por la Administración en ejercicio de una potestad administrativa distinta de la potestad reglamentaria*"[2]. Las definiciones señaladas desarrollan un concepto de acto administrativo, desde el punto de vista orgánico, sin embargo, el mismo

1 LEÓN, M. (2011). *Estudios acerca de la Ley Orgánica de la Administración Pública de 2008: El concepto de acto administrativo y su aplicación a las misiones. 100 años de la enseñanza del Derecho Administrativo en Venezuela 1909-2009.* Caracas. Editorial Funeda, p. 822.

2 GARCÍA, E. y FERNÁNDEZ T. (1993). *Curso de Derecho Administrativo*. Madrid, Editorial Thomson-Civitas, p. 550.

puede conceptualizarse en atención al criterio orgánico, formal, material y mixto, tal como lo señala Pesci-Feltri[3].

Ahora bien, con base en los otros criterios referidos, se puede señalar el del administrativista venezolano Allan Brewer-Carías, que combina los criterios orgánico, formal y el funcional (o material), y define el acto administrativo así:

> …manifestación de voluntad de carácter sublegal –criterio formal-, realizada por los órganos del Poder Ejecutivo (criterio orgánico), actuando en ejercicio de la función administrativa, de la función legislativa y de la función jurisdiccional –criterio funcional-, por los órganos del Poder Legislativo, actuando en ejercicio de la función administrativa y de carácter sublegal (criterio formal y funcional), y por los órganos del Poder Judicial actuando en ejercicio de la función administrativa y de la función legislativa (criterio funcional), con el objeto de producir efectos jurídicos determinados que son la creación de una situación jurídica individual o general, o la aplicación a un sujeto de derecho de una situación jurídica general[4].

Otra definición de acto administrativo que luce oportuno citar es la de Ramón Parada:

> …aquel dictado por una Administración Pública u otro poder público en el ejercicio de potestades administrativas y mediante el que impone su voluntad sobre los derechos, libertades o intereses de otros sujetos públicos o privados, bajo el control de la Jurisdicción Contencioso-administrativa[5].

De este contexto conceptual, se desprende la existencia de actos administrativos emanados de órganos que ejecutan otras funciones del Poder Público, siendo determinante para su encuadramiento en tal categoría –de acto administrativo–, que resulten del ejercicio de una potestad administrativa, sin ser relevante quién dicta el acto, por lo que en Venezuela se acoge el criterio funcional, siendo factible que los órganos del Poder Judicial o del Poder Legislativo dicten actos administrativos, siempre considerando que por encontrarnos en un Estado de Derecho, debe ser conforme al principio de legalidad, que informa el ordenamiento jurídico, como manifestación directa del sometimiento del poder a la ley.

3 PESCI-FELTRI, F. (2011). *Algunas notas sobre la evolución doctrinal de la noción de acto administrativo en el Derecho Administrativo Venezolano. 100 años de la enseñanza del Derecho Administrativo en Venezuela 1909-2009.* Caracas. Editorial Funeda.

4 BREWER, A. (1997). *Sobre la importancia para el Derecho Administrativo de la noción de acto administrativo y de sus efectos. Los efectos y la ejecución de los actos administrativos*. Caracas. Editorial Funeda.

5 PARADA, R. (1996). *Derecho Administrativo*. *Parte General*. Madrid. Editorial Marcial Pons, p. 95.

Por otra parte, de acuerdo con lo señalado en la definición legal de acto administrativo, éste debe cumplir con las formalidades y requisitos previstos en la Ley, desarrollados en el artículo 18 de la LOPA, y de los cuales se colige que su forma escrita es el modo de producción más frecuente, mediante el cual se manifiesta la declaración de voluntad, de juicio, de conocimiento o de deseo de la Administración Pública. Como resulta evidente, esta forma escrita viene impuesta en la mayor parte de los actos por razones de seguridad, además debido a que los actos deben motivarse, notificarse, firmarse y en general recorrer el camino reglado del procedimiento administrativo.

En relación con el acto administrativo, se debe acentuar que la regla general consiste en que está rodeado de formalidades para su formación e instrumentación, a los fines de exteriorizar la voluntad administrativa que contiene.

El artículo 18 de la LOPA establece expresamente los ocho (8) requisitos que debe cumplir el acto administrativo, tales como identificación del organismo al que pertenece el órgano que dicta el acto, identificación del órgano que lo emite, determinación del lugar y fecha, identificación del destinatario, la motivación –expresión concisa de los hechos, razones alegadas y los supuestos legales–, la decisión, la competencia para dictarlo, el sello de la oficina y la firma autógrafa del funcionario que lo emita.

En este sentido, vale mencionar lo señalado en un trabajo presentado por la autora Abreu, Gigliolla:

> el vigente régimen legal del procedimiento administrativo ordinario está enmarcado en un sistema jurídico esencialmente formalista, en el cual se prevé una serie de requisitos, lapsos y trámites que necesariamente deben cumplirse para otorgarle validez tanto al procedimiento como al acto administrativo, todo ello prescrito en la LOPA, a lo largo de su contenido. Precisamente, es en este formalismo donde incide la incursión de las NTIC, cuyos resultados se reflejan favorablemente en los restantes principios procesales, con una notoria reducción de tiempo en el Principio de Celeridad, una consecuente reducción de costasen el Principio de Economía Procesal, lo que redunda en la optimización del Principio de Eficacia y Transparencia[6].

Ahora, si bien las formalidades de este tipo, señaladas anteriormente, son relevantes para el logro del objetivo de concretar el otorgamiento de validez jurídica a los procedimientos y actos administrativos, cónsonos con las directrices previstas en la CRBV se debería evitar el excesivo formalismo que implica un obstáculo para la fluidez de los procedimientos y el cumplimiento de los objetivos y fines, y que a su vez, causan mayores gastos y costos tanto para los particulares

6 ABREU Gigliolla. (2010). "Hacia el procedimiento administrativo electrónico venezolano en el contexto de la Administración Pública electrónica". 1er Congreso ON LINE del Observatorio para la CiberSociedad, UCV, fecha de la consulta: 05 de mayo de 2014. Disponible en htpp:// www.cibersociedad.net

como para la Administración Pública, lo que no tendría sustento suficiente en la actualidad, ya que la moderna sociedad cuenta con los medios e instrumentos tecnológicos necesarios para facilitar la actividad administrativa del Estado.

Algunos autores como García, E. y Fernández, T. definen el acto administrativo electrónico como "*una declaración de voluntad, de juicio o de conocimiento de rango sublegal, realizada y emitida por la Administración Pública mediante el uso de medios técnicos electrónicos o informáticos en el ejercicio de una potestad administrativa*"[7].

Efectuando un análisis comparativo de las definiciones de acto administrativo tradicional y acto administrativo electrónico, se colige que contienen elementos de fondo equivalentes, ya que su principal diferencia radica en el medio o soporte material de su emisión o transmisión, y una muestra específica de ello, es que para su validez jurídica y consecución de sus efectos jurídicos, deben cumplirse los requisitos de competencia del sujeto que emite el acto, el objeto del acto, la motivación y su finalidad. En este orden, los cambios que se producen por el uso de los medios tienen su mayor incidencia en los elementos de forma del acto administrativo, más aún considerando que la LOPA causó intensas transformaciones jurídicas dentro de la Administración Pública, sustituyendo el informalismo por el formalismo, exigiéndolo como principio que se manifiesta tanto en el establecimiento de requisitos en la actuación de la Administración en sus trámites, como en las formas del acto administrativo.

En este ámbito resulta necesario mencionar, que conforme a la definición legal de acto administrativo (artículo 7 de la LOPA), su característica esencial radica en su sometimiento al principio de legalidad, tanto en su aspecto formal como sustancial:

A. En su aspecto formal: se refiere a que el acto administrativo como tal, debe obedecer a alguna de las categorías determinadas en la Ley y encuadrar en ésta conforme a las características que lo informan. Igualmente, debe responder a los requisitos previstos en el artículo 18 de la LOPA señalados *ut supra*.

B. En su aspecto sustancial: se alude a que el acto administrativo esté caracterizado por una serie de requisitos o elementos intrínsecos previstos en la Ley, tales como la competencia reconocida como el ámbito legítimo de actuación de los órganos y entes de la Administración, establecida expresamente en la ley, el objeto relacionado con su contenido, y su motivación correspondiente a sus fundamentos de hecho y de derecho.

7 GARCÍA, E. y FERNÁNDEZ T. (1993). *Curso de Derecho Administrativo*. Madrid, Editorial Thomson-Civitas, p. 520.

Igualmente, pudiese señalarse otro aspecto de importancia, el teleológico relacionado con la finalidad del acto, que debe estar entrelazada con la intención del legislador.

Tal como se mencionó anteriormente, la LOPA despliega como una de sus características la formalidad, en cuanto a que la Administración en su actuar, se apegue estrictamente a las prescripciones de dicha normativa legal y, en particular, a las formalidades y requisitos procedimentales que ella consagra, de conformidad con su artículo 1, referido al ámbito de su aplicación. Es por ello, que en la implementación de las TIC se mantendría la aplicación del formalismo señalado, aunque resulta inevitable que su puesta en práctica tropiece con ciertos requisitos procedimentales, los cuales deben ser replanteados, ya que en este punto, se evidencia realmente un "formalismo relajado", lo que implica que su cumplimiento no es radicalmente estricto. A tales efectos, se pueden señalar a priori algunas manifestaciones de esta flexibilidad en la materia tratada, tales como la determinación del momento de inicio del cómputo del lapso para ejercer el recurso respectivo, luego de la notificación del acto administrativo a través de un medio electrónico; las formalidades que deben considerarse para materializar las notificaciones de un acto administrativo; la determinación de los pasos a cumplir para iniciar un procedimiento administrativo; el acceso a un expediente administrativo o el medio que ha de servir de soporte a un acto administrativo y el método para atribuirle la debida autoría al mismo, todo ello cumpliendo con los requisitos legales con que debe contar un acto administrativo para su validez.

En este sentido se ha pronunciado la doctrina nacional estableciendo que:

> ...el procedimiento administrativo debe realizarse mediante una serie de formalidades para que tenga validez. Seis de esas formalidades deben modificarse necesariamente para poder ser desarrollado mediante el uso de TIC. Estas son: el sistema de comunicación por el cual han de manifestarse la Administración y los particulares, el medio que ha de servir de soporte para ese sistema de comunicación, el método para atribuir esa manifestación, el modo, el tiempo y el lugar para intercomunicarse[8].

III. Tratamiento legal y jurisprudencial del acto administrativo electrónico en Venezuela

1. Marco legal

El ordenamiento jurídico venezolano ha avanzado hacia la actualización en el campo de las TIC, y posee un conjunto de normas que ha sido desarrollado con mayor precisión, teniendo como marco la Constitución de de 1999, que tal

8 AMONI, G. (2010). *Memorias. XIV Congreso Iberoamericano de Derecho e Informática*. Monterrey. Nueva León, México, p. 18.

como se mencionó, en su artículo 110 establece el reconocimiento por parte del Estado venezolano del interés público de la ciencia, la tecnología, el conocimiento, la innovación y los servicios de información, por ser instrumentos fundamentales para el desarrollo económico, social y político del país.

En el año 2001 entró en vigencia el Decreto con Fuerza de Ley N° 1.204 de Mensajes de Datos y Firmas Electrónicas, publicado en la Gaceta Oficial N° 37.148 de fecha 28 de febrero de 2001, adoptando un marco normativo que sirve de fundamento legal para el desarrollo tecnológico sobre seguridad en materia de comunicaciones y negocios electrónicos, orientados a otorgar valor jurídico a los mensajes de datos y constituirse en sustento para los mecanismos necesarios para que la firma electrónica tenga la misma eficacia que la firma autógrafa, cumpliendo inexorablemente los requisitos establecidos en este decreto.

Es por ello que su artículo 1° prevé que este Decreto-Ley tiene por objeto:

> …otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.

Por lo que el mencionado Decreto-Ley le otorga validez a una serie de mecanismos electrónicos desarrollados en su texto para el cumplimiento de ciertos formalismos, que le otorgan pleno valor jurídico a las actuaciones que no sean desarrolladas por escrito en papel, cumpliendo los requisitos establecidos en este. Y de acuerdo con lo explanado en su exposición de motivos, se destacan los principios que informan este instrumento normativo, tales como:

A. Eficacia probatoria: con fines de seguridad jurídica se otorga a los mensajes de datos y firmas electrónicas el mismo valor probatorio que la ley consagra a los instrumentos escritos, y en cuanto a su incorporación a un proceso judicial se regularán como prueba libre.

B. Tecnología neutra: por cuanto no se direcciona hacia una determinada tecnología para las firmas y certificados electrónicos.

C. Se respetan las formas documentales: por lo que la utilización de la firma electrónica es voluntaria, ni se pretende modificar las formas solemnes de otros actos jurídicos, lo que se busca es que el mensaje de datos no carezcan de validez por su firma electrónica o su soporte material.

D. Se respetan las firmas electrónicas: las firmas de este tipo preexistentes en relaciones contractuales previas, se excluirán de las regulaciones de este decreto-ley.

E. Otorgamiento y reconocimiento jurídico de los mensajes de datos y firmas electrónicas y su buen funcionamiento.

F. La no discriminación del mensaje de datos firmado electrónicamente.
G. Permisibilidad en la elección de las partes para optar en la modalidad de sus transacciones.
H. Responsabilidad.

Posteriormente, el Decreto N° 2.479 del 27 de junio de 2003, ordena la creación de la Comisión Presidencial para la conformación de la red del Estado, con la finalidad de facilitar la comunicación e interacción de los órganos y entes de la Administración Pública.

Y un año más tarde, se publica el Decreto N° 3.390 en la Gaceta Oficial N° 38.095 de fecha 28 de diciembre de 2004, donde se establece que la Administración Pública Nacional empleará prioritariamente Software Libre desarrollado con estándares abiertos, en sus sistemas, proyectos y servicios informáticos, por lo tanto, con el objeto de lograr este cometido todos los órganos y entes de la misma, iniciarán los procesos de migración gradual y progresiva de éstos hacia el Software Libre.

La LOPA, publicada en la Gaceta Oficial N° 5.890 de fecha 15 de julio de 2008, tal como se mencionó *ut supra*, establece los principios, lineamientos y bases que rigen la organización y el funcionamiento de la Administración Pública nacional. También regula los compromisos de gestión, los mecanismos para promover la participación y el control sobre las políticas y resultados públicos; y establece las normas básicas sobre los archivos y registros públicos. En este sentido, sus artículos 5, 10 y 151 dejan ver su orientación a la simplificación de los trámites administrativos, incorporando tecnologías de información y comunicación para el cumplimiento de los cometidos de la Administración Pública.

En fecha cercana a la publicación de la LOAP, entra en vigencia el Decreto con Rango y Fuerza de Ley de Simplificación de Trámites Administrativos, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 38.984 Extraordinaria, del 31 de julio de 2008, con la finalidad de lograr una verdadera optimización para la elaboración de planes uniformes de simplificación de trámites administrativos aplicables a toda la Administración Pública, para racionalizar los trámites que realizan las personas ante esta, y lograr eficacia, eficiencia, utilidad y obtener mayor celeridad, reducir gastos operativos, obtener ahorros presupuestarios y mejorar las relaciones de las personas con la Administración.

Esta ley prevé en su artículo 2, como mecanismo para simplificar y mejorar los trámites administrativos, rediseñar el trámite utilizando al máximo los elementos tecnológicos, y en su artículo 44 establece que cada órgano o ente de la Administración Pública diseñará un sistema de información centralizada de fácil acceso que sirva de apoyo a los servicios de atención al público y deberán habilitar sistemas de transmisión electrónica de datos, con la finalidad de que las personas interesadas envíen o reciban información de sus actuaciones

frente a la Administración y que la misma pueda ser compartida con otros entes u órganos.

En el año 2010, se publica la Ley Especial contra Delitos Informáticos, en la Gaceta Oficial N° 37.313 de fecha 30 de octubre de 2010, que tiene como objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra los mismos o de los cometidos mediante el uso de dichas tecnologías.

Ese mismo año, se da a conocer la Ley de Reforma de la Ley Orgánica de Ciencia, Tecnología e Innovación, publicada en la Gaceta Oficial N° 39.575 de fecha 16 de diciembre de 2010, que en sus artículos 10 y 18 señala que la autoridad nacional con competencia en materia de ciencia, tecnología e innovación, actuará como coordinador e integrador de los sujetos regulados por la misma, en las acciones de su competencia, en articulación con los órganos y entes de la Administración Pública y ejercerá la dirección en el área de tecnologías de información.

Luego, el Decreto N° 9.051 con Rango, Valor y Fuerza de Ley Sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos Entre los Órganos y Entes del Estado (Ley de Interoperabilidad), publicado en la Gaceta Oficial N° 39.945 del 15 de junio de 2012, el cual entró en vigencia dos (02) años después de su publicación en la Gaceta Oficial respectiva, es decir, el 15 de junio del presente año y cuyos objetivos primordiales se basan en el establecimiento de un estándar de interoperabilidad entre los órganos y entes del Estado, a través del desarrollo de las condiciones necesarias para la adopción de planes y proyectos que garanticen el acceso e intercambio electrónico de datos, información y documentos entre éstos, la promoción del desarrollo de sistemas de información interoperables adecuados para lograr la satisfacción de las necesidades de los ciudadanos, el mantenimiento de una Plataforma Nacional de Servicios de Información Interoperables, la creación y desarrollo de un modelo nacional para el intercambio, publicación e interpretación de información y documentos, que permita el establecimiento de políticas, lineamientos y estrategias públicas adecuadas, que garantice un adecuado nivel de interoperabilidad en los sistemas de información utilizados por los órganos y entes del Estado, todo lo cual permitirá contribuir con la mejora del funcionamiento interno de los órganos y entes del Estado, y con la ordenación, coordinación, cooperación y racionalización de la acción pública de éstos, y contribuirá con los principios administrativos de celeridad, eficacia y eficiencia mediante la simplificación de los trámites que realizan los ciudadanos ante los órganos y entes del Estado, todo ello enmarcado en los objetivos estratégicos de la Nación.

El artículo 5 de este decreto establece que la interoperabilidad –concebida como la capacidad de los órganos y entes del Estado de intercambiar por medios electrónicos datos, información y documentos de acceso público–, se fundamenta en los principios de coordinación, cooperación, responsabilidad, eficiencia,

legalidad, privacidad, adecuación tecnológica, conservación, reutilización, integridad, continuidad y seguridad. Igualmente, prevé la posibilidad para los ciudadanos, en forma individual o colectiva, de presentar física o electrónicamente ante las Oficinas de Atención al Ciudadano de los órganos y entes del Estado; peticiones, reclamos o denuncias en la prestación de servicios públicos o por la irregularidad de la actuación de los funcionarios públicos, reconociendo de esta manera el derecho de petición a través de medios electrónicos.

En este marco conceptual, este instrumento jurídico reconoce el carácter de interés público de la interoperabilidad, como instrumento para garantizar el desarrollo de servicios públicos integrados y la simplificación de los trámites administrativos que sus órganos y entes llevan a cabo, de acuerdo con los requerimientos de los ciudadanos, en pro del interés general, y establece expresamente, entre otros:

a) Prohibición de exigir consignación de información en físico de documentos que contengan datos de autoría o información que pueda ser objeto de intercambios electrónicos (artículo 46).
b) La sustanciación electrónica de los expedientes administrativos (artículo 49).
c) La firma electrónica en las actuaciones administrativas (artículo 50), por lo que los funcionarios públicos podrán sustituir las firmas autógrafas por firmas electrónicas, cuando la sustanciación de las actuaciones administrativas se realice total o parcialmente por medios electrónicos.
d) La digitalización de los archivos públicos, cumpliendo con la normativa aplicable y la firma electrónica respectiva, lo que implicará un reconocimiento de que su contenido es válido (artículo 51).
e) La obligación de conformar un repositorio digital, donde se puedan recuperar los documentos electrónicos emitidos por ese órgano o ente del Estado (artículo 52).
f) Cuando la ley exija que un documento o información debe ser presentado por escrito, este requisito se cumplirá cuando el mensaje de dato se presente impreso y se identifique con el código del repositorio digital (artículo 53).
g) El documento señalado en el literal anterior, será validado por el funcionario público, mediante la consulta que realice en el repositorio digital, constatando que es copia fiel y exacta del original (artículo 54).

Posteriormente, fue dictada la Ley de Infogobierno, publicada en la Gaceta Oficial N° 40.274 del 27 de octubre de 2013, que establece el carácter de obligatoriedad del uso de las Tecnologías de Información en el ejercicio de las competencias del Poder Público, con la finalidad de establecer los principios, bases y lineamientos que regirán el uso de estas, a fin de optimizar la gestión y

los servicios que se prestan a los ciudadanos, así como de promover el desarrollo nacional que garantice la soberanía tecnológica, la seguridad y defensa de la Nación.

De conformidad con su disposición final tercera, este instrumento legal contará con un plazo de diez (10) meses para su entrada en vigencia a partir de su publicación en Gaceta Oficial –previsto para el mes de agosto de 2014–, por lo que se resalta que a partir de dicho momento quedará derogado el Decreto Presidencial N° 3.390, que establece el uso prioritario de Software Libre en la Administración Pública Nacional; así como el capítulo I "Del Comité Nacional de la Interoperabilidad" del Título III denominado "De la Organización Pública para la Interoperabilidad" (artículos 14 al 17) relativos a dicho Comité, sus atribuciones y funcionamiento, y el Título V "Régimen Sancionatorio" (artículos 62 al 65) referidos a la responsabilidad de los funcionarios públicos, infracciones, inhabilitación, del Decreto con Rango, Valor y Fuerza de la Ley Sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado (Ley de Interoperabilidad).

El artículo 6 de esta nueva ley establece la obligatoriedad para el Poder Público del uso de las técnicas de información en su gestión, en sus relaciones entre órganos y entes del Estado y en sus relaciones con las personas y con el Poder Popular, de conformidad a las prescripciones previstas en dicho instrumento legal. Por otra parte, prevé que todo programa informático que se desarrolle, adquiera o implemente en el Poder Público deberá ser software libre y con estándares abiertos, salvo las excepciones expresamente establecidas en la ley y previa autorización del ente competente.

Por lo tanto, estos últimos decretos, en vigencia a partir del segundo semestre de 2014, amplían el sustento legal para la consolidación del gobierno electrónico en Venezuela, la consecuente validez del acto administrativo electrónico y el establecimiento de una plataforma para la propuesta de un modelo de procedimiento administrativo electrónico, el cual pudiese tratarse como una serie de actos y diligencias que regulan la tramitación de los asuntos ante la Administración Pública, a través de la utilización de los nuevos mecanismos o técnicas de información y comunicación. Pero debe considerarse que si bien en la actualidad no existe una regulación normativa integral o completa que regule un procedimiento administrativo tendiente a facilitar el uso de los medios técnicos electrónicos, podría asomarse como solución definitiva la creación o la reforma de la normativa sustantiva y adjetiva que lo regule, pero a pesar de ello, se puede afirmar con claridad que en el marco regulatorio señalado, es posible la emisión de actos electrónicos válidos.

2. Jurisprudencia del Tribunal Supremo

En este contexto resulta importante analizar la jurisprudencia del Tribunal Supremo de Justicia que ha desarrollado el tratamiento de los mensajes de

datos obtenidos por correo electrónico y lo relativo a los requisitos de fondo y de forma que deben contener los actos administrativos, es decir, en cuanto a la utilización de la nuevas tecnologías para el cumplimiento de los fines de la Administración Pública.

A este respecto, la Sala Político Administrativa donde ha sostenido el mismo criterio del tema en cuestión, se puede señalar la sentencia N° 1.011 del 08 de julio de 2009, sentencia N° 1.437 del 08 de octubre de 2009, sentencia N° 100 del 03 de febrero de 2010 y sentencia N° 01801 del 15 de diciembre de 2011, las mismas versan sobre pretensiones de nulidad interpuestas contra actos emanados de la Comisión de Administración de Divisas (CADIVI), donde esta negaba la venta de divisas solicitadas y se había alegado el incumplimiento de los requisitos de forma y de fondo del acto administrativo, establecidos expresamente en la LOPA.

En estos fallos se desarrolla la temática de los mensajes de datos a través de correos electrónicos como resultado de la consulta efectuada a través del Sistema Automatizado de la Comisión de Administración de Divisas (CADIVI), y la Sala Político Administrativa del Tribunal Supremo de Justicia en este sentido, ratifica el criterio de que dichos mensajes de datos *no deben contener de acuerdo a la normativa aplicable, los requisitos de forma y de fondo de los actos administrativos*, por lo que la legalidad de dichos mensajes no puede impugnarse alegando el argumento de que no cumplen con esos requerimientos.

En las decisiones mencionadas, la Sala analizó la normativa aplicable a este tipo de mensajes transmitidos a través de medios electrónicos, tales como el Decreto con Rango y Fuerza de Ley de Simplificación de Trámites Administrativos, así como el Decreto con Fuerza de Ley N° 1.204 de Mensajes de Datos y Firmas Electrónicas y concluyó estableciendo que no puede atribuírsele a todo tipo de información contenida en un mensaje de datos del sistema tecnológico utilizado por los órganos o entes de la Administración Pública, los vicios de ilegalidad por no cumplir con los requisitos o formalidades de un acto administrativo.

En este sentido, se cita lo establecido por la Sala Político Administrativa del Tribunal Supremo de Justicia de fecha 03 de febrero de 2010, en la Sentencia N° 100:

> (…) la negativa de la autorización para la adquisición de divisas se encuentra contenida en un medio electrónico; por lo tanto, resulta imprescindible determinar en el caso concreto la exigibilidad del cumplimiento de los requisitos de forma y de fondo establecidos en la Ley Orgánica de Procedimientos Administrativos en este tipo de medios, a fin de verificar la legalidad del acto; para lo cual es necesario hacer las siguientes consideraciones:
>
> (…) el Decreto con Fuerza de Ley N° 1.204 dio a los mensajes de datos y firmas electrónicas la eficacia probatoria que la Ley otorga a los documentos escritos y, cuando la información electrónica se reproduzca en formato impreso, su valor será el atribuido a las copias o reproducciones fotostáticas. No obstante

> lo anterior, debe resaltarse que el mismo instrumento normativo establece expresamente la necesidad del cumplimiento de las formalidades que respecto a determinados actos o negocios jurídicos exige el ordenamiento jurídico; toda vez que el espíritu de dicho Decreto, como se señala en su Exposición de Motivos, no fue alterar las restantes formas de los diversos actos jurídicos, registrales y notariales, sino que se propone que un mensaje de datos firmado electrónicamente, no carezca de validez jurídica únicamente por la naturaleza de su soporte y de su firma.
>
> En efecto, de la lectura del instrumento jurídico bajo análisis se evidencia que la normativa especial que regula el uso de los medios electrónicos no pretende sustituir o excluir el cumplimiento de los requisitos y formalidades que deben reunir ciertos actos para producir efectos jurídicos, entre los que tienen que incluirse aquellos que emanan de la Administración, sino regular los nuevos mecanismos tecnológicos que el Estado pone al alcance de los ciudadanos para aumentar la eficiencia de la gestión pública.
>
> (…) No obstante, evidencia la Sala que la mencionada Providencia no establece como obligación que el acto administrativo formal a enviarse como mensaje de datos a través de correo electrónico –en este caso la negativa de la autorización– deba transcribirse y transmitirse íntegramente en su forma original (…) estima la Sala que la legalidad de dicho mensaje no puede impugnarse bajo el argumento de no reunir los requisitos de forma y de fondo de todo acto administrativo; razón por la cual la Sala debe desechar el vicio denunciado.
>
> Aunado a lo anterior, advierte la Sala que luego de conocer el "status" de su solicitud por cualquier medio –por ejemplo: a través de correo electrónico, consulta en el sistema automatizado de la Comisión de Administración de Divisas o a través del Operador Bancario–, los particulares tienen el derecho de acudir ante la Administración para solicitar la entrega del acto administrativo dictado y, en caso de considerarlo necesario, ejercer los recursos pertinentes con la exposición de los alegatos y defensas que consideren pertinentes.

Del extracto de la sentencia transcrita, se colige que conforme a la normativa que regula la materia de la utilización de los medios electrónicos, y en este caso en especial lo referido a las solicitudes de divisas ante la Comisión de Administración de Divisas (CADIVI), no resulta obligatorio el cumplimiento de los requisitos de forma y de fondo de los actos administrativos previstos en la LOPA para el mensaje de datos recibido por los particulares por esa vía electrónica, y en caso de que estos consideren que se vean afectados o vulnerados sus derechos, deben acudir y exigir a la Administración Pública la entrega del texto íntegro del acto contentivo de la declaración respectiva, a efectos de tener conocimiento de los motivos e interponer los recursos respectivos en caso de ameritarlo.

Ante esto, la Sala Político Administrativa concluye que hay requisitos de validez del acto administrativo tradicional que no pueden trasladarse al formato electrónico, y el mensaje de datos recibido a través del correo electrónico es una simple notificación o medio de comunicación del acto administrativo formal,

que debe ser dictado en papel (escrito) y cursar en un expediente administrativo, y que para que el particular pueda acceder a este y conocerlo en su integridad debe solicitarlo directamente ante el órgano que lo dictó, lo cual fue recogido en la tesis de especialización del profesor Amoni Reverón[9].

En esta situación, pudiesen surgir dudas respecto al momento en que comienzan a correr los lapsos para la impugnación o interposición del recurso correspondiente ante un acto administrativo de esta categoría, por la eventual vulneración de algún derecho del particular; en la determinación del momento en que este se encuentra notificado del respectivo acto administrativo, bien sea desde que recibe el mensaje de datos a través del correo electrónico o desde que acude al órgano o ente de la Administración Pública que emite el acto y le entrega el mismo. Resultaría factible que el criterio que garantizaría el derecho a la defensa y al debido proceso, se corresponde con el de considerar que el particular se encuentra notificado del acto administrativo una vez que conoce los motivos que fundamentan el mismo, es decir, para estos casos, desde el momento en que acude a la Administración y le es entregado dicho acto.

IV. Validez del acto administrativo electrónico en Venezuela

En la LOPA se establecen los requisitos de fondo y de forma para la validez del acto administrativo. Según los diversos sectores de la doctrina, los requisitos de fondo se subdividen en subjetivos tales como la competencia (artículos 3, 6, 12, 15, 16, 17, 18.7, 19.4) y quién lo dicta en ejercicio de la potestad administrativa[10]. Y en objetivos, constituidos por el objeto (artículos 19.3, 62, 88, 89), la causa (artículos 9, 12, 18.5, 58, 69), el contenido, el fin (artículos 3, 12) y los motivos[11].

Los requisitos de forma están constituidos por el procedimiento administrativo caracterizado por la formalidad y los requisitos establecidos en el artículo 18 de la LOPA, la motivación y la forma de exteriorización.

A su vez, resulta necesario destacar que de acuerdo con la jurisprudencia de la Sala Político Administrativa del máximo Tribunal, se ha venido manejando el criterio de que necesariamente no deben cumplirse para los actos administrativos electrónicos los requisitos de forma del acto administrativo tradicional. Y en este sentido, la doctrina ha establecido que deben considerarse tres (3) aspectos primordiales para determinar que en nuestro país los actos administrativos electrónicos tienen validez jurídica y pleno valor probatorio, por lo que debemos profundizar en el sistema de comunicación, en el soporte material

9 AMONI REVERÓN, Gustavo. (2011). "Las Tecnologías de Información y Comunicación en las diversas formas de la actividad administrativa". Trabajo Especial de Grado no publicado. Universidad Católica Andrés Bello. Caracas.

10 GARCÍA, E. y FERNÁNDEZ, T. (2004). *Curso de Derecho Administrativo*. Madrid, Editorial Thomson-Civitas, p. 555.

11 *Ibídem* , p. 557-558.

del acto como tal y en el método para atribuir la autoría de dicho acto administrativo[12].

Tal como se ha señalado anteriormente, en la publicación del autor venezolano Gustavo Amoni, se desarrollan los aspectos citados, así en referencia al sistema de comunicación, de acuerdo con la LOPA, priva el sistema escrito, cuyo fin es garantizar la seguridad jurídica a través de la integridad del acto, donde se determina con claridad el órgano o ente que lo emite, a quién va dirigido y su contenido, e igualmente se establecen las circunstancias de lugar y tiempo en que se dicta.

Ahora bien, con la entrada en vigencia del Decreto con Fuerza de Ley N° 1.204 de Mensajes de Datos y Firmas Electrónicas, se introduce la innovación de otorgarle valor jurídico y eficacia probatoria a la firma electrónica, al mensaje de datos y a toda información inteligible en formato electrónico en igualdad a la que la ley le otorga a los documentos escritos. En este Decreto, en su artículo 7° se determinan dos (02) requisitos para otorgar la validez mencionada al mensaje de datos, en primer término, que dicho mensaje se conserve en su integridad y se mantenga inalterable, y por último, cuando la información contenida en éste se encuentre disponible o accesible.

El mencionado autor señala, con respecto al medio que ha de servir de soporte a las actuaciones electrónicas, tanto el artículo 7 como el 8 del Decreto con Fuerza de Ley N° 1.204 de Mensajes de Datos y Firmas Electrónicas, establecen sobre la constancia por escrito del mensaje de datos, que dicho presupuesto se considerará cumplido si la información contenida en el mismo es accesible y permite su consulta posterior. Así cuando la ley requiera que ciertos actos se materialicen por escrito y sean accesibles, se debe cumplir con los siguientes requisitos previstos en el mencionado artículo 8:

> (…)
> 1. Que la información que contengan pueda ser consultada posteriormente.
> 2. Que conserven el formato en que se generó, archivó o recibió o en algún formato que sea demostrable que reproduce con exactitud la información generada o recibida.
> 3. Que se conserve todo dato que permita determinar el origen y el destino del Mensaje de Datos, la fecha y la hora en que fue enviado o recibido.

Por lo tanto, de las disposiciones señaladas se colige que la materialización de los requisitos señalados, permiten que la información contenida en un mensaje de datos, almacenada o intercambiada, tenga validez probatoria y eficacia, por otra parte, el mencionado instrumento legal otorga valor jurídico al mensaje de datos, independientemente de su soporte material.

12 AMONI, G. (2010). *Memorias. XIV Congreso Iberoamericano de Derecho e Informática*. Monterrey. Nueva León, México, p. 18-25.

Por último, el citado autor expresa sobre el elemento referido al método para atribuir la autoría a ese acto, específicamente representado por la firma y el sello electrónico, que la LOPA en el numeral 8° del artículo 18 prevé como requisito del acto administrativo tradicional el sello de la oficina y la firma autógrafa de los funcionarios que lo suscriban.

Sobre este tema, el artículo 2 del Decreto con Fuerza de Ley N° 1.204 de Mensajes de Datos y Firmas Electrónicas, define la firma electrónica como la "*información creada o utilizada por el Signatario, asociada al Mensaje de Datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado*". Y de conformidad con el artículo 6 *ejusdem*, cuando legalmente se exija la firma autógrafa para determinados actos, dicha exigencia será saldada cuando el mensaje de datos tenga vinculada o asociada una firma electrónica.

No obstante lo anterior, el artículo 50 de la Ley de Interoperabilidad consagra específicamente la firma electrónica en las actuaciones administrativas, determinando que los funcionarios públicos podrán sustituir por firmas electrónicas, la utilización de las firmas autógrafas, cuando la sustanciación de las actuaciones administrativas se realice total o parcialmente bajo medios electrónicos.

Del artículo 16 del Decreto con Fuerza de Ley N° 1.204 de Mensajes de Datos y Firmas Electrónicas se desprende que para la validez y eficacia de la firma electrónica equiparable a la firma autógrafa, esta debe cumplir con los siguientes requisitos: "*(…) 1. Garantizar que los datos utilizados para su generación puedan producirse sólo una vez, y asegurar, razonablemente, su confidencialidad. 2. Ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente a cada momento. 3. No alterar la integridad del Mensaje de Datos*". A tales efectos, legalmente se establece que la firma electrónica que no cumpla con los señalados requisitos no tendrá el mismo valor jurídico que la firma autógrafa y sólo podrá ser valorada conforme a las reglas de la sana crítica.

Por otra parte, el mencionado instrumento legal tasa expresamente el valor probatorio de la firma certificada (artículo 18), la cual debe ser debidamente certificada por un proveedor de servicios de certificación. Sobre este punto, la Ley de Infogobierno establece que el Estado debe garantizar el principio de seguridad en sus actuaciones electrónicas, y en este sentido, prevé la utilización de la firma electrónica certificada, por lo que a partir de la entrada en vigencia de esta Ley (el 17 de agosto de 2014, 10 meses después de su publicación), sólo tendrá valor este tipo de firma.

En cuanto al sello, como otro de los elementos para atribuir la autoría de un determinado acto administrativo, es decir, para la determinación del órgano o ente de donde emana un determinado acto, según lo señalado por el mencionado autor, éste no se constituye en un requisito esencial, por lo que no se trata de un requisito invalidante, criterio igualmente sustentado en las decisiones a tales efectos, emitidas por la Sala Político Administrativa del Tribunal Supremo de

Justicia, en algunos fallos donde ha ratificado el criterio señalado, tales como: Sentencia N° 799 del 11 de junio de 2002, Sentencia N° 1275 del 23 de octubre de 2002, Sentencia 4925 del 14 de julio de 2005, Sentencia N° 581 del 07 de marzo de 2006 y Sentencia N° 2043 del 10 de agosto de 2006.

En definitiva, es necesario destacar que la implementación de las TIC, en la emisión de los actos administrativos electrónicos, solo pueden modificar en cierta manera sus requisitos de forma, más no los requisitos de fondo imprescindibles en su formación y validez, por lo que desde mi punto de vista la importancia radica en que el acto administrativo electrónico cumpla su finalidad u objetivo.

V. Conclusiones

El marco jurídico desarrollado en nuestro país, destinado a regular la eficacia y validez del acto administrativo electrónico, a partir de la Constitución de la República Bolivariana de Venezuela, ha aportado un gran avance en la consolidación del gobierno electrónico.

Es importante señalar, que para lograr una correcta apreciación de los documentos electrónicos como medios probatorios en plataformas tecnológicas, resulta necesario que los jueces y administradores amplíen sus criterios sobre la base de los adelantos de la tecnología informática, pues de nada servirá que las partes utilicen los avances jurídicos, de la ciencia y de la tecnología como medios de prueba, si los funcionarios públicos encargados de la resolución de las controversias, se cierran a apreciarlos en todo su valor probatorio, por desconocimiento o desconfianza. Es por ello, que la firma, sea autógrafa o electrónica en un documento, lo califica de veraz, al demostrar el consentimiento de quien la suscribe y su autoría.

Con la implementación de las TIC, los actos administrativos solo se verán afectados en sus elementos de forma, mas no en los elementos de fondo, por lo que el régimen legal del acto administrativo electrónico, así como la adjudicación de su validez se ha ido incorporando paulatinamente en el ámbito normativo venezolano.

Por otra parte, resulta indudable que las formalidades y requisitos de procedencia y tramitación de los procedimientos administrativos se verán afectados por los cambios tecnológicos, por lo tanto, es viable considerar una reforma o la implementación de una nueva ley, que regule el procedimiento administrativo electrónico adaptado a las nuevas necesidades informáticas. Las TIC tienen un valor estratégico fundamental en el diseño del procedimiento administrativo electrónico, debido a los beneficios o ventajas que conllevan su utilización, tales como mayor celeridad en las actuaciones, economía, transparencia, eficacia y eficiencia en las tramitaciones y decisiones y ahorro de tiempo por parte de los ciudadanos y la Administración Pública.

Por último, la migración a un sistema de esta naturaleza generará mayor confianza y transparencia en la Administración Pública por parte de los

administrados y gracias a las TIC, se obtendrá una mejor coordinación e interoperabilidad entre los diversos órganos y entes de la Administración Pública y se optimizará el nivel de calidad en la prestación de los servicios públicos y de las demás actividades administrativas.

El documento electrónico en el ámbito laboral y su uso como medio de prueba

Sulmer Paola Ramírez*

SUMARIO: I. El documento electrónico. 1. El documento en papel frente al soporte electrónico. 2. Autenticidad del documento electrónico. 3. El documento electrónico en el ámbito laboral. 4. Principios rectores en la interpretación de los documentos electrónicos. 4.1. Principio de neutralidad tecnológica. 4.2. Principio de equivalencia funcional. 4.3. Principio de libertad contractual. 4.4. Principio de inalteración del Derecho preexistente de obligaciones y contratos. 4.5. Principio de buena fe. II. El documento electrónico como medio de prueba. 1. Admisión. 2. Promoción. 2.1. Reglas generales 2.2. Promoción del documento electrónico en los procedimientos regidos por el Código de Procedimiento Civil 2.3. Promoción del documento electrónico en los procedimientos regidos por la Ley Orgánica Procesal del Trabajo. 3. Valor jurídico del documento electrónico.

Resumen

Las Tecnologías de la Información y las Comunicaciones permiten la expresión de la voluntad en soportes electrónicos. En la actualidad, uso de estos instrumentos como medios de prueba es posible. En este trabajo se estudian los principios que rigen la interpretación del documento electrónico y su uso como medio probatorio en los contratos y obligaciones laborales. Tomando en cuenta la especial naturaleza de estos documentos, se analiza la forma de promoción, evacuación, control, contradicción y valor jurídico probatorio de los documentos electrónicos de acuerdo con lo establecido en el Código de Procedimiento Civil y en la legislación laboral venezolana.

Palabras clave: Mensajes de datos. Firma electrónica. Documento electrónico. Medios de prueba. Derecho laboral.

Recibido: 22/7/2014 • Aceptado: 25/8/2014

* Abogada, Especialista en Derecho del Trabajo y Seguridad Social UCAT. Especialista en Derecho Administrativo UCAT. Especialista en Negocios con América Latina IDEC Universidad Pompeu Fabra Barcelona España. Doctoranda del Doctorado en Ciencias Mención Derecho UCV. Profesora de la Universidad Católica del Táchira y asesora de empresas públicas y privadas. sulmerp@yahoo.com

Abstract

Information Technologies and Communications allow expression of will in electronic media. Nowadays, the use of electronic documents as evidence is possible. This paper studies the principles governing the interpretation of the electronic documents, and its use as evidence in labor obligations and contracts. According to the special nature of these documents, filing, examination, control, contradiction, and legal probative value are analyzed regarding to the provisions of Venezuelan Procedure Code and Labor Law.

Keywords: Data messages. Electronic Signature. Electronic Document. Evidence. Labor Law.

I. El documento electrónico

1. El documento en papel frente al soporte electrónico

La palabra documento tiene su origen en el vocablo griego "dek" que corresponde al verbo latino "docere" que significa instruir, que a su vez es el origen del término "documentum" que significa lo que se enseña. En un sentido amplio, al conjugar el verbo latino "docere" y el griego "dekomai" se obtiene como significado: poner en conocimiento a alguien sobre una determinada situación o cosa[1]. Por su parte el Diccionario de la Real Academia Española define el documento como: "*Diploma, carta, relación u otro escrito que ilustra acerca de algún hecho, principalmente de los históricos*" y como: "*Escrito en que constan datos fidedignos o susceptibles de ser empleados como tales para probar algo*"[2].

Para Carnelutti, el documento "*es una cosa que hace conocer un hecho*"[3]. Mientras que para Jorge Cardoso Isaza, por documento se entiende "*cualquier cosa que siendo susceptible de ser percibida por la vista el oído, o por ambos, sirve por sí misma para ilustrar o comprobar, por vía de representación, la existencia de un hecho cualquiera o la exteriorización de un acto humano*"[4].

1 RICO CARRILLO, M.: *Comercio electrónico Internet y Derecho*, Legis, Bogotá 2005, p. 95.

2 Disponible en: http://lema.rae.es/drae/

3 CARNELUTTI citado por CARRASCOSA LÓPEZ V., POZO ARRANZ M. A., RODRÍGUEZ DE CASTRO E. P.: *La contratación informática: el nuevo horizonte contractual*. Editorial Comares Tercera Edición 2000, p. 56.

4 CARDOSO ISASA, Jorge citado por CUBILLOS VELANDIA, R. y RINCÓN CÁRDENAS, E.: *Introducción jurídica al comercio electrónico*, Bogotá: Ediciones Jurídicas Gustavo Ibañez Ltda. 2002, p. 224-225.

La amplia definición de la palabra documento, da cabida a la diversidad de soportes que pueden contener la información que desea hacerse del conocimiento de alguien mediante el documento, sin que exista la obligatoria vinculación con el papel como soporte, lo que está en sintonía con lo señalado por Álvarez Cienfuegos al indicar que "*El documento, como objeto corporal que refleja una realidad fáctica con trascendencia jurídica, no puede identificarse ni con el papel como soporte, ni con la escritura como unidad de significación*"[5], permitiéndose así entre otros, el uso de los medios electrónicos ya sea para manifestar la voluntad de los declarantes, para contener las respectivas declaraciones y/o para comunicar las mismas, lo que permite hablar entonces del documento electrónico.

Las Tecnologías de la Información y la Comunicación (TIC) han permitido que además del uso del papel como soporte tradicional, se empleen los soportes electrónicos que se denominan memorias. La norma (ISO 110113) define la memoria (*storage*) como la unidad funcional capaz de recibir, conservar y restituir datos[6]. Existen gran variedad de sistemas de soporte electrónico según su fiabilidad, posibilidad de regrabación, acceso secuencial o directo, entre otras características, por lo que generalmente se estudia el tipo de sistema a emplear según el fin perseguido.

Davara Rodríguez[7], señala que el documento electrónico, informático y telemático es un documento con las mismas características, en principio y en cuanto su validez jurídica, que cualquier otro de los que tradicionalmente se aceptan en soporte papel.

Carlos Barriuso señala que el denominado documento electrónico, está constituido por: "*Las declaraciones de voluntad con efectos de creación, modificación o extinción de derechos y obligaciones, por medio de la electrónica, la informática y telemática*"[8].

En Venezuela, la Sala de Casación Civil del Tribunal Supremo de Justicia, en sentencia dictada el 24 de octubre de 2007, caso: Distribuidora Industrial de Materiales C.A. contra Rockwell Automation de Venezuela C.A., dejó sentado que:

> …el documento electrónico debe entenderse como cualquier tipo de documento generado por medios electrónicos, incluyendo en esta categoría los sistemas electrónicos de pago, la red de internet, los documentos informáticos y telemáticos, entre otros.

5 ALVAREZ CIENFUEGOS SUÁREZ, A. citado por RICO CARRILLO, M.: *Comercio electrónico Internet y Derecho, op. cit*, p. 94.

6 BARRIUSO RUIZ, C.: *La contratación electrónica*. Madrid: Editorial Dykinson, S. L. 1998, p. 224.

7 DAVARA RODRÍGUEZ, citado por RICO CARRILLO, M. *Comercio electrónico Internet y Derecho, op. cit.* p. 97.

8 BARRIUSO RUIZ, C.: *La contratación electrónica, op. cit.* P. 319.

En relación a los criterios de seguridad, que permitirán al documento electrónico constituirse en documento, Y. Poullet[9] señaló, que el mismo:

> -Debe ser inalterable
> -debe ser legible gracias a un procedimiento apropiado
> -debe ser identificado respecto al lugar (nombre y dirección) y al tiempo (fecha de redacción, de envío y de recepción);
> -debe ser estable, lo que plantea el problema del soporte físico y los métodos de rejuvenecimiento del soporte.

En Venezuela, siguiendo la orientación de la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) sobre Firma Electrónica, la Ley de Mensaje de Datos y Firmas Electrónicas (LMDFE), da cabida al documento electrónico, al señalar en su artículo 4 que "*Los Mensajes de Datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos…*", entendiéndose por mensaje de datos según lo establecido en el artículo 2 del referido texto legal, "*Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio*".

Cabe destacar que los documentos electrónicos son igualmente documentos escritos, y lo que hace la diferencia con el documento tradicional es su soporte, mientras que éste último está contenido por regla general en soporte papel, el documento electrónico tiene un soporte electrónico, pero ambos son documentos escritos, realidad que no implica que sean obligatoriamente manuscritos, pudiendo admitirse pacíficamente, como lo señaló J. Rouanet citado por Carlos Barriuso Ruiz[10], "*…que la electrónica deba ser considera escritura, a todos los efectos, y que por tanto, el documento electrónico pertenece a la categoría de los documentos en sentido jurídico*".

Para Giannantonio[11], no hay inconveniente en considerar el documento electrónico como documento escrito ya que:

> 1. Contiene un mensaje (texto alfanúmero o diseño gráfico)
> 2. En lenguaje convencional (el de los bits)
> 3. Sobre soporte (cinta o disco)
> 4. y destinado a durar en el tiempo

En plena sintonía con lo expuesto, el legislador venezolano en atención al posible requerimiento legal que una información conste por escrito, estableció

9 Y. PULLET citado por CARRASCOSA LÓPEZ, V., POZO ARRANZ M. A., RODRÍGUEZ DE CASTRO E. P.: *"La contratación informática…, op. cit.* p. 59.

10 BARRIUSO RUIZ, C. *La contratación electrónica, op. cit,* p. 226.

11 GIANNANTONIO citado por CARRASCOSA LÓPEZ, V., POZO ARRANZ, M. A., RODRÍGUEZ DE CASTRO, E. P.: *La contratación informática…, op. cit*. p. 59.

en el artículo 8 de la LMDFE que dicho requisito quedará satisfecho con relación a un mensaje de datos, si la información que éste contiene es accesible para su ulterior consulta, lo que se logra con el cumplimiento de las siguientes condiciones:

> 1. Que la información que contengan pueda ser consultada posteriormente.
> 2. Que conserven el formato en que se generó, archivó o recibió o en algún formato que sea demostrable que reproduce con exactitud la información generada o recibida.
> 3. Que se conserve todo dato que permita determinar el origen y el destino del Mensaje de Datos, la fecha y la hora en que fue enviado o recibido.
> Toda persona podrá recurrir a los servicios de un tercero para dar cumplimiento a los requisitos señalados en este artículo[12].

2. Autenticidad del documento electrónico

La autenticidad de un documento se refiere principalmente a la necesidad de identificar a su autor y a certificar que éste aprueba su contenido. Al tratarse de un documento electrónico, la firma electrónica es considerada el elemento idóneo para satisfacer este requisito.

En el marco de la LMDFE, el artículo 6 establece que para aquellos actos o negocios jurídicos, en que la ley exija como requisito que el documento deba contener la firma autógrafa, dicho requisito, al tratarse de un mensaje de datos quedará satisfecho al tener asociado una firma electrónica.

Esta norma proviene del artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico que dispone que cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos *"… si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos"*. Este principio es incorporado también en la Ley Modelo sobre Firmas Electrónicas. En el ámbito de esta norma, el artículo 6 establece que cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos si se utiliza una firma electrónica fiable y apropiada para los fines que se generó o comunicó el mensaje.

Para la generación de la firma electrónica con efectos equivalentes a la firma manuscrita, la LMDFE exige determinados requisitos, que en la actualidad son satisfechos mediante la emisión de los certificados electrónicos por parte de los proveedores de servicios de certificación electrónica.

Un certificado electrónico es un documento electrónico emitido por un proveedor de servicios de certificación que atribuye certeza y validez a la firma electrónica. El proveedor de servicios de certificación electrónica, es un tercero que por excelencia va a prestar los servicios para la conservación y consulta

12 Condiciones contenidas en el artículo 8 de la Ley de Mensaje de Datos y Firmas Electrónicas.

posterior de la información contenida en un documento electrónico, y es quien, entre otras actividades, está facultado para emitir un certificado electrónico que garantiza la autoría de la firma electrónica que certifica, así como la integridad del mensaje de datos.

3. El documento electrónico en el ámbito laboral

El documento electrónico laboral, es un instrumento emitido o recibido en forma conjunta o separada por las autoridades administrativas y/o judiciales del trabajo, por el trabajador, o por el patrono, que contiene información inteligible en formato electrónico relacionada en forma directa o indirecta con el cumplimiento o incumplimiento de los derechos y obligaciones de las partes de una relación de trabajo subordinada. Hay una suerte de contenido y continente entre el documento electrónico laboral y el documento electrónico, ya que el primero, se encuentra contenido dentro del documento electrónico, por lo que no todo documento electrónico será un documento electrónico laboral, pero si todo documento electrónico laboral será un documento electrónico. Los aspectos característicos del documento electrónico laboral son los siguientes:

1) Sujetos. El documento electrónico laboral, para ser considerado como tal, debe ser emitido o recibido en forma conjunta o separada, por las autoridades administrativas y/o judiciales del trabajo, el trabajador, el patrono.

2) Contenido. Toda información inteligible en formato electrónico relacionada en forma directa o indirecta con el cumplimiento o incumplimiento de los derechos y obligaciones inherentes a las partes de una relación de trabajo subordinada, vale decir, trabajador y patrono.

3) Forma. La forma del documento electrónico laboral es de un mensaje de datos[13] en formato electrónico.

4) Firma. El documento electrónico laboral, puede tener asociado a él, una información creada o utilizada por su signatario, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado, esta información es la firma electrónica de la autoridad administrativa y/o judicial del trabajo, del patrono o del trabajador.

En las relaciones de trabajo, tanto el trabajador como el patrono pueden emplear documentos electrónicos en el cumplimiento de sus obligaciones, lo que en la práctica se traduce por vía de ejemplo, en la notificación de riesgos laborales efectuada por el empleador a su trabajador mediante un documento electrónico, o en el cumplimiento de una determinada tarea que el trabajador

13 Mensaje de datos, que es entendido como toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio, de conformidad con lo establecido en el artículo 2 de la Ley de Mensaje de Datos y Firmas Electrónicas patria.

informe a su patrono a través de un mensaje de datos, prácticas que cada vez son más comunes, gracias a que responden a principios de eficiencia, eficacia, conservación del planeta por la disminución del uso de hojas de papel, disminución de costos, entre otras tantas razones.

El documento electrónico laboral, tiene la misma naturaleza del documento electrónico en general, basada en su forma inteligible en formato electrónico. Al igual que sucede con los documentos laborales emitidos en papel, cuando se trata de documentos electrónicos laborales pueden existir documentos privados, emanados del trabajador o del patrono, documentos oficiales electrónicos (emanados de autoridades administrativas o judiciales) o documentos públicos, autorizados por los funcionarios encargados de dar fe pública a los actos que se celebran en su presencia, como el caso de los notarios y registradores. Sobre este punto, es necesario mencionar que el ordenamiento jurídico venezolano admite el documento público electrónico, toda vez que la Ley de Registro Público y Notariado (LRPN) permite que el proceso registral y notarial se desarrolle íntegramente a partir de un documento electrónico y establece que la firma electrónica de los registradores y notarios tendrá la misma validez y eficacia probatoria que la ley otorga a la firma manuscrita.

4. Principios rectores en la interpretación de los documentos electrónicos

Los documentos electrónicos, forman parte de las modificaciones derivadas del uso de las TIC en las actividades desarrolladas por los seres humanos, siendo posible, gracias a ellas, el cotidiano intercambio de información entre ciudadanos sujetos a iguales o diferentes jurisdicciones, lo que ha hecho necesaria la aplicación de principios que traten de armonizar y contribuyan al desarrollo de la normativa legal que regule estas nuevas formas documentales y sus consecuencias en el mundo jurídico, siendo éste el objeto del Derecho del comercio electrónico.

Aunque los principios que se señalan a continuación provienen de la Ley Modelo de la CNUDMI sobre Comercio Electrónico, son aplicables a la interpretación de los documentos electrónicos en general, siendo por ello también aplicables al documento electrónico laboral individual y al documento electrónico bilateral conocido como contrato electrónico laboral, por lo que su enfoque será en sentido general, con las aclaratorias y salvedades propias del documento electrónico laboral. Dentro de los principios, creados como reglas básicas de aplicación general, adoptados por diferentes países en sus distintas legislaciones, que sirven de base para la interpretación de los documentos electrónicos, y por ende de los documentos electrónicos laborales, se encuentran los siguientes:

4.1. Principio de neutralidad tecnológica

Este principio implica el respeto al uso de cualquier tecnología, impidiendo que se favorezcan unas tecnologías sobre otras, lo que responde a la velocidad de desarrollo e innovación de las TIC, que traería como consecuencia la no vigencia de la norma o acuerdo que establezca una determinada tecnología para ser usada.

El legislador venezolano, en respeto al principio de neutralidad tecnológica, utiliza el termino firma electrónica en lugar de firma digital, aceptando que la firma electrónica contiene a la firma digital que está basada en una tecnología de dígitos (unos y ceros) propias del sistema binario, que es utilizado por las computadoras gracias a los dos niveles de voltajes que manejan, en el que uno (1) representa encendido y cero (0) representa apagado.

Con el avance propio de las TIC, el sistema binario dejará de ser utilizado trayendo como consecuencia el desuso de la firma digital, en contraposición con el uso de la firma electrónica que permite además del sistema binario, emplear cualquier otra tecnología capaz de producir una firma electrónica.

El principio de neutralidad tecnológica en el campo de las relaciones de trabajo subordinado, implica que los patronos son libres de emplear la tecnología que deseen en sus procesos productivos, así como también en las comunicaciones que internamente fluyan entre las partes del contrato de trabajo y con terceros, pudiendo las mismas contenerse en documentos electrónicos, siempre que se respeten las leyes, buenas costumbres y el orden público.

Dependiendo de la actividad productiva del patrono, de las características de sus trabajadores y de los recursos económicos con los que cuente, el empleador utilizará una determinada tecnología en lugar de otra. Por vía de ejemplo, se puede contextualizar lo señalado, planteando el caso de una empresa que emplee a personas con discapacidad visual lo que implicaría que la tecnología por ellos requerida deba estar adecuada para el uso de personas con esta discapacidad, siendo por ello menester la aplicación de la tiflotecnología[14], pudiendo optar por el Sistema Jaws[15] o el Windows-Eyes[16] entre otros.

Cabe destacar, que el empleador ante una inspección de los órganos administrativos laborales, puede basarse en el principio de neutralidad tecnológica

14 La tiflotecnología es una tecnología de apoyo, entendida como el conjunto de teorías y de técnicas que permiten el aprovechamiento práctico de los conocimientos tecnológicos aplicados a personas ciegas o con baja visión.

15 EL Sistema Jaws, de Freedom Scientific, es un software que permite escuchar por intermedio de las bocinas o altavoces de la computadora cada paso que se da sobre el teclado y las opciones para continuar.

16 El Windows-Eyes Desarrollado por GWMicro, Windows-Eyes provee, es competencia directa del Sistema Jaws, siendo también un lector de pantalla para el sistema operativo Windows de Microsoft que utiliza una voz sintetizada y líneas de Braille dinámicas, acceso casi completo a Windows y sus aplicaciones.

para defenderse en contra del requerimiento realizado por dicho organismos o por cualquier ente estadal, de utilizar una determinada tecnología en su empresa ya sea en los procesos productivos o en el soporte de los documentos empleados para su comunicación con los trabajadores, socios o terceros.

4.2. Principio de equivalencia funcional

Este principio permite equiparar los efectos que producen los documentos que se plasman en soporte papel y son firmados en forma autógrafa por su autor, con los efectos derivados de sus homólogos, los documentos electrónicos, que tienen un soporte y firma electrónica.

El principio de equivalencia funcional da protagonismo al objetivo que persigue el declarante o los declarantes al firmar un documento, sin discriminar su soporte ni la forma de la firma, debiendo tener en cuenta para el análisis del mismo, los requisitos de fiabilidad, rastreabilidad e inalterabilidad de forma, en virtud de la naturaleza de los documentos electrónicos[17].

La exigencia que los documentos deban constar por escrito sobre papel, ha sido un obstáculo jurídico para el empleo masivo de las TIC, en diversos campos del Derecho, entre ellos el Derecho laboral, pero la búsqueda de aplicación del principio de equivalencia funcional, hizo que se analizaran de una parte, la naturaleza de las exigencias legales sobre la escritura de un documento, y de otra, las razones por las cuales se solicita la presentación de un escrito[18], logrando que se establecieran las pautas tecnológico-jurídicas mínimas que deben cumplir los mensajes de datos para que cumplan el requisito de escritura, centrándose en el concepto básico *"que la información se reproduce y se lee"*[19].

La LMDFE acoge la equivalencia funcional en sus artículos 4 y 16 al otorgarle respectivamente al mensaje de datos, la misma eficacia probatoria que la ley otorga al documento escrito y a la firma electrónica, que permita vincular al signatario con el mensaje de datos y atribuir la autoría de éste, la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa.

Gracias al principio de equivalencia funcional, en las relaciones de trabajo subordinado, tanto el trabajador como el patrono pueden emplear documentos electrónicos en el cumplimiento de sus obligaciones, sin que esto sea óbice para considerar que efectivamente han cumplido con las mismas. Más aún cuando la citada LMDFE establece en su articulado los requisitos que deben cumplir los mensajes de datos, cuando una determinada ley requiera que la información

17 CUBILLOS VELANDIA, R. y RINCÓN CÁRDENAS, E.: *Introducción jurídica al comercio electrónico*, *op cit*, p. 229.

18 Razones generalmente vinculadas al ámbito probatorio.

19 Grupo de Estudios en Internet, Comercio Electrónico & Telecomunicaciones e Informática. GECTI "Comercio Electrónico" Universidad de Los Andes. Editorial Legis, 2005. p. 148.

sea presentada o conservada en su forma original[20], o cuando la ley requiera que la información conste por escrito.

Partiendo de lo anteriormente expuesto, y con un objetivo ilustrativo, el patrono cumpliendo con lo establecido en la ya citada LMDFE, a través de mensajes de datos, podrá consultar a los trabajadores y trabajadoras y a sus organizaciones, y al Comité de Seguridad y Salud Laboral de la empresa, antes de que se ejecuten, las medidas que prevean cambios en la organización del trabajo que puedan afectar a un grupo, o la totalidad de los trabajadores, o decisiones importantes de seguridad e higiene y medio ambiente de trabajo, dando de esta forma cumplimiento al deber impuesto en el numeral 2 del artículo 56 de la Ley Orgánica de Prevención, Condiciones y Medio Ambiente de Trabajo, en lo adelante LOPCYMAT, referido como ejemplo en este caso.

Existen obligaciones de cada una de las partes en las cuales la ley exige la escritura como requisito, tal es el caso de la norma contenida en el numeral 3 del artículo 56 de la LOPCYMAT, que establece como un deber del empleador:

> 3. Informar por escrito a los trabajadores y trabajadoras de los principios de la prevención de las condiciones inseguras o insalubres, tanto al ingresar al trabajo como al producirse un cambio en el proceso laboral o una modificación del puesto de trabajo e instruirlos y capacitarlos respecto a la promoción de la salud y la seguridad, la prevención de accidentes y enfermedades profesionales así como también en lo que se refiere a uso de dispositivos personales de seguridad y protección.(Subrayado propio)

Aplicando el principio de equivalencia funcional, y las normas contenidas en la LMDFE, el patrono podrá cumplir con el referido deber a través de un documento electrónico, vale decir, mensaje de datos en soporte electrónico, y quedará satisfecho el requisito exigido de escritura, siempre que la información que esté contenida en dicho mensaje sea accesible para su ulterior consulta, debiéndose conservar el formato en que se generó, archivó o recibió, o en algún formato que sea demostrable que reproduce con exactitud la información generada o recibida, además de ser conservado igualmente todo dato que permita determinar el origen y el destino del referido mensaje, así como la fecha y la hora en que fue enviado o recibido, condiciones que pueden cumplirse contratando los servicios de un tercero o por un sistema creado por el mismo patrono[21].

20 Requisito que según lo establecido en el artículo 7 de la Ley de Mensaje de Datos y Firmas Electrónicas, quedará satisfecho con relación a un mensaje de datos, si la información allí contenida está disponible y ha conservado su integridad.

21 En virtud que la LDMFE en su artículo 8 al respecto señala que*: "…Toda persona podrá recurrir a los servicios de un tercero para dar cumplimiento a los requisitos señalados en este artículo*" de forma tal, que es una facultad del patrono acudir al tercero o no, lo importante es el cumplimiento de las condiciones exigidas para la escritura y ulterior consulta del mensaje de datos.

El tema de la autoría del documento electrónico, que en su homólogo en papel es resuelto con mayor simplicidad gracias a la firma autógrafa generalmente en él contenida, ha limitado igualmente el uso más frecuente de las TIC en el Derecho, abordando específicamente el caso del Derecho laboral, debido a la complejidad del uso de la firma electrónica.

La firma electrónica que permite vincular al signatario con el mensaje de datos y atribuir la autoría de éste, tiene la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa, según lo dispone el artículo 16 de la LMDFE. El caso es que en materia laboral la carga de la prueba recae por principio general sobre el patrono, quien deberá probar que efectivamente fue él quien cumplió con las obligaciones que le han sido impuestas por la legislación laboral; y en el caso de la utilización de una firma electrónica, deberá demostrar el acuerdo que sobre la firma de los documentos electrónicos haya llegado con sus trabajadores, o en su defecto, demostrar el cumplimiento de los requisitos exigidos en el artículo 16 de la LMDFE que se refieren a los siguientes aspectos:

- Garantizar que los datos utilizados para la generación de la firma electrónica puedan producirse sólo una vez, y asegurar, razonablemente, su confidencialidad.
- Ofrecer seguridad suficiente de que no pueda ser falsificada la firma electrónica con la tecnología existente en cada momento.
- No alterar la integridad del mensaje de datos, vale decir, del documento electrónico que contiene el cumplimiento de los deberes que hayan acatado con el uso del mismo.

El problema es que en la actualidad y de acuerdo con las previsiones de la LMDFE, el cumplimiento de estos requisitos se presume cuando se utiliza una firma electrónica basada en un certificado electrónico expedido por un proveedor de servicios de certificación acreditado, lo que viene a complicar más el tema de la carga de la prueba, por la complejidad que este tipo de firma representa en la práctica.

De no cumplir el patrono con lo anteriormente señalado, la firma electrónica asociada al mensaje de datos, no se le podrá otorgar la validez y eficacia probatoria atribuida por ley a la firma autógrafa pero podrá constituir un elemento de convicción valorable conforme a las reglas de la sana crítica, según lo establecido en el artículo 17 de la LMDFE. Cabe destacar, que si un Proveedor de Servicios de Certificación Electrónica, certifica en forma debida la firma electrónica del patrono, ésta producirá los mismos efectos de validez y eficacia otorgados a la firma autógrafa, solo deberá evaluar el empleador, los beneficios de dicha certificación con las posibilidad económicas de la empresa.

4.3. Principio de libertad contractual

La libertad contractual, como principio de interpretación de los documentos electrónicos, está basada en la autonomía de la voluntad de los declarantes,

quienes deciden libremente emplear en sus negocios jurídicos medios electrónicos, ya sea para manifestar su voluntad, para conservar su declaración, para ejecutar lo pactado, o para verificar el cumplimiento de cualquier aspecto que haya sido acordado.

La LMDFE recoge este principio en su articulado, citando entre otras normas el contenido del artículo 15, relativo a la formación de los contratos, en el que se establece la posibilidad de las partes de acordar que la oferta y aceptación se realicen por medio de mensajes de datos, de forma tal, que son los declarantes quienes deciden en principio la forma y soporte que quieran darle a sus manifestaciones de voluntad, siendo una opción el uso del documento y la firma electrónica.

Asimismo, son las partes de un negocio jurídico quienes pueden acordar el procedimiento para establecer cuándo el mensaje de datos proviene efectivamente del emisor, o cuándo se tendrá por emitido un mensaje de datos, o pactar sobre su lugar de emisión y de recepción o sobre los mecanismos del acuse de recibo[22], entre otros aspectos.

En materia de relaciones de trabajo subordinado, perteneciente al Derecho del trabajo, el principio de libertad contractual encuentra ciertas limitaciones que se enfocan principalmente más que en la forma que se le pueda dar a una declaración de voluntad, vale decir, si se usa o no el documento en soporte electrónico, en el contenido de tal declaración. La restricción viene dada por el contenido, ya que las normas del Derecho del trabajo son de orden público sin poder ser relajadas por las partes, en donde existen una serie de principios que deben ser respetados, como la irrenunciabilidad de los derechos del trabajador, según la cual, independientemente de la manifestación de su libre voluntad -en soporte papel o electrónico- acerca de renunciar a un derecho consagrado en la legislación laboral, se entiende nula por mandato legal dicha manifestación.

El principio de libertad contractual puede encontrar su máximo esplendor en los acuerdos realizados entre trabajador y patrono relativos a las condiciones de la relación de trabajo, o a los derechos y deberes inherentes a la misma, pudiendo elegir que las comunicaciones se realicen mediante el uso de las TIC o en soporte papel. De elegir la primera opción, un ejemplo de ello sería la asignación de tareas vía correo electrónico y el reporte del cumplimiento de las mismas por parte del trabajador a través de la misma vía o por mensaje de texto, por citar un ejemplo de soporte electrónico de información. Resulta de capital importancia resaltar, que en forma tácita o expresa, ambas partes deben haber consentido el uso de los medios electrónicos para la comunicación, tanto de las tareas como de sus resultados.

El contrato de trabajo, que por regla general es el primer acuerdo al que llegan trabajadores y patronos, puede igualmente, en ejercicio del principio de

22 Manifestaciones del principio de libertad contractual, establecidas en los artículos del 9 al 14 de la Ley de Mensaje de Datos y Firmas Electrónicas.

libertad contractual, ser realizado a través de medios electrónicos, hablándose en este caso del contrato electrónico laboral, figura que será desarrollada más adelante en este trabajo.

4.4. Principio de inalteración del Derecho preexistente de obligaciones y contratos

Este principio indica que lo acordado en un documento electrónico no puede sufrir modificación alguna que esté basada solo en el medio que se utilizó como soporte de las declaraciones de voluntad de las partes, en otras palabras, los medios electrónicos son simplemente nuevas formas de representación de la voluntad de los contratantes, sin que esto sea óbice para el cumplimiento de sus deberes y derechos.

En un documento electrónico unilateral, o bilateral como el contrato electrónico, el principio de autonomía de la voluntad de las partes, que a su vez se traduce en libertad contractual, es el que faculta a los contratantes o al declarante a utilizar los medios electrónicos como forma para la celebración del negocio jurídico, no pudiendo luego excusarse del cumplimiento de sus obligaciones solo por la elección que hizo del referido medio.

El mismo grado de responsabilidad se deriva para el patrono y el trabajador de la celebración de un contrato de trabajo en soporte papel, que del contrato de trabajo celebrado por medios electrónicos. Igual ocurre con las órdenes que sobre la ejecución de la labor encomendada dé el patrono a su trabajador vía correo electrónico, las mismas deben ser acatadas sin decir que por ser por correo electrónico y no en soporte papel, no tenía valor alguno.

El principio de inalteración del Derecho preexistente, lo establece la LMDFE venezolana en su Exposición de Motivos, al indicar que dicha ley no pretende alterar el funcionamiento de los negocios jurídicos, sino otorgar validez a los mensajes de datos y a las firmas electrónicas.

4.5. Principio de buena fe

El vocablo buena fe provienen del latín, "bona fides" definida por el diccionario de la Real Academia Española como: "*Criterio de conducta al que ha de adaptarse el comportamiento honesto de los sujetos de derecho" y "En las relaciones bilaterales, comportamiento adecuado a las expectativas de la otra parte"*[23].

En Derecho es un principio general, que hace referencia a la observancia de una conducta de honradez, de respeto y lealtad por parte del declarante o de los declarantes en un acto jurídico. Este principio está recogido en el artículo 1.160 del CC venezolano al señalar *"Los contratos deben ejecutarse de buena*

23 Disponible en: http://lema.rae.es/drae/(Consulta: 15 de julio de 2014.)

fe y obligan no solamente a cumplir lo expresado en ellos, sino a todas las consecuencias que se derivan de los mismos contratos, según la equidad, el uso o la Ley".

En cuanto a la buena fe y el uso de las TIC en el campo del Derecho, incluyendo el Derecho del trabajo, debido a lo novedoso del documento electrónico laboral y la firma electrónica,

> …es fundamental y adquiere especial significado ante el desconocimiento y la desconfianza generada en el medio por su reciente aparición y complejidad técnica, por lo tanto la buena fe debe ser respetada en grado superior mientras las circunstancias del parcial desconocimiento y desconfianza persistan[24]

El principio de buena fe, aplicado a la interpretación de los documentos electrónicos laborales, trae consigo la presunción, salvo prueba en contrario, que la información en ellos contenida corresponde a la expresión de la voluntad tanto del patrono como del trabajador, quienes en su elaboración actuaron con honradez y con el firme propósito de cumplir las conductas a que se comprometieron, siendo traducidas éstas en derechos y obligaciones para cada una de las partes.

II. El documento electrónico como medio de prueba

Los distintos actos del ser humano, pueden estar soportados en documentos electrónicos, por ello es de vital importancia su estudio como medio de prueba. En el campo de las relaciones de trabajo subordinadas, el documento electrónico puede servir como medio de prueba del cumplimiento o incumplimiento de las obligaciones que la relación de trabajo impone tanto al trabajador como al patrono.

La "prueba" en su acepción común, es la acción y el efecto de probar, mientras que "probar" es entendido como "*justificar, manifestar y hacer patente la certeza de un hecho o la verdad de algo con razones, instrumentos o testigos*"[25].

Gracias al principio de libertad contractual, adminiculado con el principio de inalteración del Derecho preexistente de obligaciones y contratos, en forma conjunta y/o separada, las partes de un contrato pueden decidir que el cumplimiento de las manifestaciones de voluntad y sus prestaciones estén recogidas en mensajes de datos, pudiendo o no asociar a éstos sus firmas electrónicas, asimismo, pueden acordar que dichos mensajes, entendidos como documentos electrónicos, sirvan para probar entre ellos lo allí contenido.

24 ILLESCAS ORTIZ, citado por RICO CARRILLO, M. *Comercio electrónico Internet y Derecho, op. cit*. p. 73.

25 Tomado del Diccionario de la Lengua Española, disponible en: http://lema.rae.es/drae/ (Consulta: 15 de julio de 2014.)

En las relaciones de trabajo subordinado, el patrono y/o el trabajador, pueden decidir, en forma conjunta o separada, el uso del documento electrónico laboral para ejecutar el cumplimiento de las obligaciones inherentes a la relación de trabajo, siendo en este caso, el documento electrónico un medio de prueba empleado en forma privada, *extra liten*, que se regirá por las reglas de valoración probatoria que hayan sido previamente establecidas por las partes. De no llegar a acuerdos satisfactorios sobre los hechos que se desean probar, las partes están en plena libertad de acudir a los órganos administrativos y/o judiciales en busca de la tutela judicial efectiva.

Eduardo J. Couture, señala que los hechos y actos jurídicos son objeto de afirmación y negación en el proceso[26], afirmación que comparte quien escribe y partiendo de la misma, surge la siguiente inquietud: ¿Los documentos electrónicos son medios de prueba de hechos y actos jurídicos que hayan sido objeto de afirmación o negación en los procesos?

En aras de resolver la interrogante planteada, se analizará la admisión del documento electrónico como medio de prueba, su forma de promoción y finalmente su valor jurídico. Este análisis se fundamenta en la naturaleza del documento electrónico, vale decir, su forma inteligible en soporte electrónico, por lo que se hablará del documento electrónico en general, abarcando de este modo al documento electrónico laboral[27]:

1. Admisión

La LMDFE, además de atribuirle al mensaje de datos la misma eficacia probatoria que la ley le otorga a los documentos escritos sobre la base del principio de equivalencia funcional que fue ya desarrollado en el punto anterior, reconoce al mensaje de datos como un medio de prueba, estableciendo que su promoción, control, contradicción y evacuación, se realizará conforme a lo previsto para las pruebas libres en el Código de Procedimiento Civil (CPC).

La libertad de prueba, consagrada en el CPC, permite a las partes, a fin de demostrar sus pretensiones, valerse de cualquier medio de prueba que no esté prohibido en forma expresa por la ley. La norma procesal establece que estos medios se promoverán y evacuarán aplicando por analogía las disposiciones relativas a los medios de prueba semejantes contemplados en el CC y en su defecto en la forma que señale el juez[28]. Esta libertad de prueba desarrolla el principio constitucional contenido en el artículo 49 de la Constitución de la

26 COUTURE, E. *Fundamentos del Derecho procesal civil*. Buenos Aires: Ediciones Depalma, tercera edición, 1993, p. 217.

27 Que como se señaló anteriormente, es un documento electrónico que contiene información relacionada en forma directa o indirecta las obligaciones inherentes a la relación de trabajo subordinado, y emana en forma conjunta o separada del patrono, el trabajador o la autoridad administrativa y/o judicial laboral.

28 Principio de Libertad Probatoria consagrado en el artículo 395 del CPC venezolano.

República Bolivariana de Venezuela, según el cual, toda persona tiene derecho a utilizar los medios adecuados para ejercer su defensa.

La Sala de Casación Civil del Tribunal Supremo de Justicia[29], ha catalogado al documento electrónico como un medio atípico o prueba libre, "*por ser aquél instrumento que proviene de cualquier medio de informática o que haya sido formado o realizado por éste*" catalogándolo también

> …como el conjunto de datos magnéticos grabados en un soporte informático susceptible de ser reproducidos que puede fungir como objeto de prueba y su reproducción, independientemente de su denominación, debe ser considerada otro documento que actúa como medio para su traslado al expediente.

La Ley Orgánica Procesal del Trabajo, al igual que su homóloga en materia civil, admite la prueba libre, señalando que las partes pueden valerse de cualquier medio de prueba no prohibido expresamente por la ley y que consideren conducente a la demostración de sus pretensiones. En cuanto a la promoción y evacuación de dichos medios de prueba, indica que se realizará en la forma contemplada en la Ley Orgánica en cuestión, y de no ser posible, se aplicarán por analogía, las disposiciones relativas a los medios de pruebas semejantes contemplados en el CPC, CC o en su defecto, en la forma que señale el Juez del Trabajo[30].

De lo anteriormente expuesto, se evidencia en forma clara que los documentos electrónicos si pueden ser admitidos en los respectivos procedimientos como medios de prueba, pero es importante destacar que se deben cumplir ciertas condiciones de admisibilidad, tal y como lo señala Rico Carrillo[31], destacando entre otras:

- La posibilidad de identificación de los declarantes y las operaciones realizadas por cada uno de ellos durante la elaboración del documento electrónico.
- La calidad de los sistemas utilizados para la elaboración y almacenamiento del documento, entre los que destacan el hardware y el software.
- La legibilidad del documento electrónico, que implica su posibilidad de lectura y comprensión, empleando para ello el lenguaje de los bits que a pesar de ser diferente al alfanumérico, puede ser de acceso del hombre con el uso de la informática y el adecuado software.
- La veracidad de la información. El mensaje de datos enviado por el emisor debe ser exacto al recibido por el destinatario, siendo importante conservar su integridad y disponibilidad, requisitos establecidos el artículo 7 de la LMDFE.

29 Sentencia de la Sala de Casación Civil del Tribunal Supremo de Justicia de Venezuela, de 05 de octubre de 2011, expediente N° 2011-000237. Disponible en: http://www.tsj.gov.ve/decisiones/scc/Octubre/RC.000460-51011-2011-11-237.html(Consulta: 15 de julio de 2014.)

30 Principio consagrado en el artículo 70 de la LOPT de Venezuela.

31 RICO CARRILLO, M. *Comercio electrónico Internet y Derecho, op. cit.* p. 105-106.

- La atribución a una persona determinada de la autoría de un mensaje de datos (autenticidad del mensaje), circunstancia acreditable mediante el uso de la firma electrónica.
- La fiabilidad de los sistemas empleados para la autenticación del documento electrónico.

A los efectos de determinar cuándo un documento electrónico se reputa original y cuando no, la LMDFE sigue la tesis de la inalterabilidad del mensaje de datos, según la cual, en materia electrónica para ser catalogado como original, se debe tener en cuenta la conservación íntegra del mensaje de datos[32], tal y como se señala en el artículo 7 de la LMDFE al establecer:

> Cuando la ley requiera que la información sea presentada o conservada en su forma original, ese requisito quedará satisfecho con relación a un Mensaje de Datos si se ha conservado su integridad y cuando la información contenida en dicho Mensaje de Datos esté disponible. A tales efectos, se considerará que un Mensaje de Datos permanece íntegro, si se mantiene inalterable desde que se generó, salvo algún cambio de forma propio del proceso de comunicación, archivo o presentación.

La tesis de inalterabilidad, seguida por la LMDFE de Venezuela, se contrapone a la tesis basada en un criterio cronológico, según el cual, será el original del documento, aquel que primero se generó, tal como sucede en el caso de los documentos emitidos en papel. Si bien el sellado de tiempo permitiría satisfacer la exigencia cronológica, en el entendido que se trata de una herramienta informática que permite determinar el momento, lugar, fecha de emisión y/o envío de un documento[33], en la actualidad es el criterio de inalterabilidad el que determina la condición de documento original cuando se trata de un soporte electrónico.

En cuanto a la tesis basada en un criterio tecnológico (integridad o inalterabilidad), se destaca que el documento original se produce en la memoria RAM como soporte de los lenguajes binarios y codificados que usa el sistema, pero debido a que dicha memoria se borra en ausencia de la energía eléctrica, para evitar esa volatilidad y desmaterialización es necesario que se grave en otro soporte indeleble[34], el cual se considerará documento original siempre que permanezca inalterable. En atención a esta circunstancia, la mayoría de las legislaciones, siguiendo los principios de la Ley Modelo de Comercio Electrónico de la CNUDMI, adoptan el criterio de la integridad (inalterabilidad) para garantizar la condición de original de un documento electrónico, lo cual permite la existencia de multiplicidad de "originales", a diferencia de lo que sucede con el documento en papel.

32 *Ibid*., p. 108.
33 RICO CARRILLO, M.: *Comercio electrónico Internet y Derecho, op. cit.* p. 108.
34 BARRIUSO RUIZ, C. *La contratación electrónica, op. cit*, p. 307.

En cuanto a la exigencia del documento original, es necesario destacar que al tratarse de un documento electrónico, a efectos de analizar la integridad del mensaje, el original es el soporte electrónico (intangible por naturaleza) y sobre este soporte es que debe recaer el objeto de la prueba, toda vez que por disposición de la propia LMDFE, (artículo 4) dispone en forma expresa que la información contenida en un mensaje de datos, reproducida en formato impreso, tendrá la misma eficacia probatoria atribuida en la ley a las copias o reproducciones fotostáticas.

En una relación de trabajo subordinada, por vía de ejemplo, el patrono y los trabajadores pueden acordar que las instrucciones de la ejecución de una determinada labor y el reporte de dichas tareas, sea realizado en mensaje de datos, pactando asimismo las condiciones que deben imperar para la elaboración de dicho mensaje, entre otras, el medio a ser empleado, los tiempos de emisión y recepción, el opcional acuse de recibo entre otros aspectos, creando así un medio de prueba a ser utilizado en principio entre ellos, y de ser necesario, ante los respectivos órganos administrativos y/o judiciales.

2. Promoción

2.1. Reglas generales

Entre los declarantes de un documento electrónico bilateral, su promoción privada como medio de prueba, quedará supeditada a las reglas que sobre la promoción de dicho documento hayan establecido las partes en ejercicio del principios de libertad contractual, que los faculta para fijar sus propias pautas y procedimientos, fundamentados en los principios de equivalencia funcional, inalteración del Derecho preexistente de obligaciones y contratos, y el principio de buena fe.

En el supuesto de procedimientos administrativos o judiciales, evidenciada como ha quedado en el anterior punto, la posibilidad de admitir en un procedimiento el documento electrónico como medio de prueba de lo afirmado o negado por las partes, es importante analizar la forma de promoción, aspecto que se encuentra regido por lo establecido para la promoción de las pruebas libres, según el mandato del artículo 4 de la LMDFE, en concatenación con lo establecido según el caso, en el artículo 395 del CPC y el artículo 70 de la Ley Orgánica Procesal del Trabajo.

Resulta de capital importancia el auto de admisión del documento electrónico como medio de prueba, ya que será en la oportunidad en que se incorporen los documentos electrónicos promovidos a las actuaciones judiciales cuando el administrador de justicia, que en materia laboral será el juez laboral en sede judicial o los inspectores o directores en sedes administrativas, fijen si la evacuación del documento electrónico se va a realizar aplicando la forma de un

medio semejante, o mediante una forma autónoma establecida por dicha autoridad.

Cabe destacar el criterio sostenido por la Sala de Casación Civil del Tribunal Supremo de Justicia, según el cual dispuso que *"…era evidente que los mensaje de datos son un medio de prueba atípico, cuyo soporte original está contenido en la base de datos de un PC (personal computer) o en el servidor de la empresa y es sobre esto que debe recaer la prueba"*[35]. Este criterio es conforme con las previsiones de la LMDFE que sólo consideran original al soporte electrónico.

2.2. Promoción del documento electrónico en los procedimientos regidos por el Código de Procedimiento Civil

Este punto analiza la promoción del documento electrónico que tiene su certificado electrónico, mediante el cual se garantiza la autoría de la firma electrónica que certifica y la integridad del mensaje de datos.

En aquellos casos en que el documento electrónico cumpla con los requisitos exigidos en la LMDFE, para que se le otorgue el mismo valor probatorio que a los documentos escritos y a la firma electrónica la misma validez y eficacia probatoria que a la firma autógrafa, su promoción será como prueba documental, debiendo ser incorporado al proceso en su soporte electrónico, rigiéndose principalmente en materia civil por lo establecido en el artículo 430 del CPC. Se destacan en cuanto a la promoción del documento electrónico, los siguientes aspectos:

a. Oportunidad de incorporación

En el procedimiento ordinario establecido en el CPC, el documento electrónico, según el interés de la parte promovente, podrá, como todo documento privado, ser acompañado junto con el libelo de la demanda, si el actor lo considera un instrumento en que se fundamente su pretensión[36], o junto con el escrito de contestación a la demanda o ser promovido en el escrito de pruebas presentado en la oportunidad establecida para la promoción de las mismas[37].

La naturaleza propia del documento electrónico representa algunas particularidades para su incorporación a las actas del expediente, en virtud que su soporte, como es sabido, es electrónico, mientras que las actas del expediente tienen soporte papel, y se rigen por el principio de la escritura y formación del expediente según el cual *"Los actos del Tribunal y de las partes se realizarán*

35 Sala de Casación Civil del Tribunal Supremo de Justicia: sentencia dictada el 24 de octubre de 2007, en el caso Distribuidora Industrial de Materiales C.A. contra Rockwell Automation de Venezuela C.A.

36 De conformidad con lo establecido en el ordinal 6° del artículo 340 del CPC venezolano.

37 Según lo establecido en el artículo 396 del CPC venezolano.

por escrito. De todo asunto se formará expediente separado con un número de orden, fecha de su iniciación, el nombre de las partes y su objeto"[38].

El requisito de escritura de las actas del expediente, queda satisfecho respecto al documento electrónico, cuando éste se incorpore en su soporte original (electrónico) y siempre que la información que éste contiene sea accesible para su ulterior consulta, en los términos establecidos en el artículo 8 de la LMDFE. Es importante recordar que la impresión en papel del documento solo tiene los efectos probatorios de atribuidos por la legislación a una copia fotostática.

La satisfacción del requisito de escritura del documento electrónico no es el único aspecto a considerar. La efectiva forma de incorporación a las actas del expediente de dicho documento es lo que quizás desde un punto de vista práctico en la actualidad, representa un aspecto que supera la simpleza teórica. Una copia certificada del documento electrónico emanada de funcionario público que de fe pública del mismo, o una inspección judicial previa a la presentación del libelo de demanda, y que haya sido solicitada con el auxilio de perito capacitado en TIC, con el fin que quede levantada en acta la existencia del documento electrónico y su certificado, pudiera acompañarse junto con el libelo de demanda, en el supuesto que dicho documento quiera ser producido con constancia del original del mensaje de datos y sea el instrumento en que se funde la pretensión del demandante. Forma de incorporación al expediente, también aplicable en los casos que la misma se produzca junto con el escrito de contestación de la demanda.

En el caso que el actor desee producir junto con el libelo de demanda, en lugar de la constancia del original del mensaje de datos, una copia o reproducción fotostática del instrumento electrónico en que se funde su pretensión, la incorporación de éste a las actas del expediente se podrá realizar con el formato impreso de la información contenida en dicho documento electrónico.

También, a tenor de lo establecido en el artículo 434 del CPC, puede el actor indicar en el libelo de demanda el lugar donde se encuentre el documento electrónico, con la obligación de producirlo dentro del lapso de promoción de pruebas, pudiéndose valer en esta oportunidad, de la promoción de una inspección judicial, con auxilio del perito capacitado en TIC, con el objeto de dejar constancia de la existencia del documento electrónico y su certificado, en otras palabras, dejar constancia del contenido íntegro del mensaje de datos, de la autoría del mismo, de la fecha en que fue elaborado y en su caso enviado y/o recibido, entre otros particulares. Esta forma de promoción del mensaje de datos, permite el control de la prueba por las otras partes del proceso.

En el supuesto de la promoción del documento electrónico en la oportunidad establecida para la promoción de las pruebas en el expediente, se puede promover igualmente como prueba documental, promoviendo asimismo la

38 Principio establecido en el artículo 25 del CPC.

mencionada inspección judicial dirigida al lugar donde se encuentre el documento electrónico[39] con el auxilio del perito capacitado en TIC, en los términos antes señalados. Adicionalmente se puede solicitar prueba de informes dirigida al Proveedor de Servicios de Certificación Electrónica que proporcionó el certificado electrónico promovido, entre otros medios de prueba. Permitiendo al igual que en el supuesto anterior, el ejercicio del control de la prueba por las partes en el proceso.

b. Control y contradicción

1) Reconocimiento del documento electrónico producido junto con el libelo de demanda. Incorporada a las actas del expediente la constancia del original del mensaje de datos del documento electrónico[40] como instrumento fundamental de la pretensión producido, junto con el libelo de demanda, corresponde a la parte contra quien se produjo dicho instrumento privado como emanado de ella o de algún causante suyo, manifestar formalmente en el acto de contestación de la demanda, si lo reconoce o lo niega, de conformidad con el artículo 444 del CPC.

2) Reconocimiento producido con posterioridad a la presentación del libelo de demanda. Incorporada a las actas del expediente, la constancia del original del mensaje de datos del documento electrónico con posterioridad al momento de presentación del libelo de demanda, que podría ser por regla general, en la oportunidad de contestar la demanda, o en el lapso fijado para la promoción de pruebas, corresponde a la parte contra quien se produjo dicho documento como emanado de ella o de un causante suyo, manifestar formalmente dentro de los cinco días siguientes a aquel en que ha sido producido, si lo reconoce o lo niega de conformidad con el artículo 444 del CPC.

Cabe destacar, que si la parte contra la que se produjo el documento electrónico como emanado de ella guarda silencio, dará por reconocido dicho documento.

39 Que puede ser el computador personal, o cualquier otro instrumento telemático e informático.

40 Documento electrónico con certificado electrónico en el que el mensaje de datos tiene el mismo valor probatorio otorgado a los documentos escritos y la firma electrónica tiene otorgada la misma validez y eficacia probatoria que la firma autógrafa, de conformidad con lo establecido en la LMDFE (artículos: 4, 16, 18).

c. La carga de la prueba

Al ser desconocido un documento privado, corresponde a la parte que produjo el documento, probar su autenticidad[41]. El CPC, en materia de desconocimiento (distinto a lo que ocurre con la tacha de documento privado) contempla solo la posibilidad de probar la autenticidad de la firma, guardando silencio por lo que respecta a la integridad del contenido del documento privado, que en materia de documento electrónico seria la integridad del mensaje de datos.

Carnelutti ha definido la autenticidad como la correspondencia entre el autor aparente y el autor real del documento, dependiendo ésta de la seguridad con que se rodee el proceso de elaboración y emisión de un documento[42].

Es importante hacer la acotación, que la referida autenticidad de la firma, es diferente al carácter auténtico de un instrumento, ya que la primera hace referencia a la correspondencia entre la persona que aparece como firmando un documento y la persona que efectivamente lo firmó, mientras que un documento público o auténtico, es aquel que ha sido autorizado con las solemnidades legales por un Registrador, por un Juez u otro funcionario o empleado público que tenga facultad para darle fe pública, en el lugar donde el instrumento se haya autorizad, según lo establecido en el artículo 1357 del Código Civil (CC) patrio.

Para probar la autenticidad de la firma, el artículo 445 del CPC, establece la posibilidad de promover la prueba de cotejo y de no ser posible ésta, se podrá promover la prueba de testigos.

En Venezuela, la Superintendencia de Servicios de Certificación Electrónica con el objeto de garantizar la confidencialidad, integridad, autenticidad y control en el uso de documentos electrónicos creó la Autoridad de Certificación de Estampado de Tiempo[43].

d. Prueba de cotejo

De ser elegido el cotejo por el promovente del documento electrónico, éste deberá indicar el instrumento indubitado con el cual deba hacerse dicho cotejo, que será practicado por expertos, en este caso informáticos o expertos en TIC. Para la práctica del cotejo, se considerarán indubitados según lo establecido en el artículo 448 del CPC:

41 Según lo establecido en el artículo 445 del CPC.

42 CARNELUTTI, citado por CARRASCOSA LÓPEZ, V., POZO ARRANZ Ma., RODRÍGUEZ DE CASTRO E. P.: *La contratación informática…, op. cit.* p. 72.

43 Mediante providencia número 003-11 de fecha 06 de julio de 2011, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela número 39.717 de fecha 20 de julio de 2011.

- Los instrumentos que las partes reconozcan como tales, que en materia de documento electrónico, puede hacer referencia a negocios jurídicos previos entre las partes, en los que se haya utilizado la misma firma electrónica, y que haya quedado reconocida.
- Los instrumentos firmados ante un Registrador u otro funcionario público. En este caso, el promovente puede indicar como documento indubitado la misma firma promovida pero a la que se le ha otorgado fe pública por un Notario Público patrio, en los términos establecidos en el numeral 18 del artículo 74 de la Ley de Registro Público y Notaría.
- Los instrumentos privados reconocidos por la persona a quien se atribuya el que se trate de comprobar, supuesto que puede ser verificado indicando un documento electrónico existente al que se le haya asociado la misma firma objeto de prueba, pero que en ese caso la persona que está siendo vinculada con el mensaje de datos, reconoció la misma firma electrónica que dio origen al cotejo por haber sido negada
- La parte reconocida o no negada del instrumento que se trate de comprobar, esto en el caso que se haya desconocido la autenticidad de la firma electrónica debido a alteraciones en la fase de memorización, elaboración o transmisión del documento electrónico[44].

e. Tacha

En materia de tacha del documento electrónico, hay que distinguir entre el documento electrónico público, que ha sido otorgado por un funcionario púbico con tal competencia y el documento electrónico privado.

1) Tacha del documento electrónico con fe pública. A tenor de lo establecido en el artículo 1.357 del CC, el documento público o auténtico es el que ha sido autorizado con las solemnidades legales por un Registrador, por un Juez u otro funcionario o empleado público que tenga facultad para darle fe pública, en el lugar donde el instrumento se haya autorizado.

Al respecto, es importante destacar que de conformidad con lo establecido en la LRPN, la firma electrónica de los Registradores y Notarios tendrá la misma validez y eficacia probatoria que la ley le otorga a la firma manuscrita.

Los notarios y registradores patrios, podrán en el cumplimiento de sus funciones registrales y notariales, y de las formalidades y solemnidades de los actos o negocios jurídicos, aplicar los mecanismos y la utilización de los medios electrónicos consagrados en la ley. Destacándose que por mandato legal:

- El proceso registral y notarial podrá ser llevado a cabo íntegramente a partir de un documento electrónico.

44 Causas de falta de autenticidad del documento electrónico, señaladas por CARRASCOSA LÓPEZ, V., POZO ARRANZ, M. A., RODRÍGUEZ DE CASTRO, E. P.: *La contratación informática… op. cit.* p. 72.

- La publicidad registral reside en las bases de datos del sistema automatizado de los Registros, en la documentación archivada que de ellas emanen y en las certificaciones que se expidan.
- Los asientos e información registrales contenidos y emanados oficialmente del sistema registral surtirán todos los efectos jurídicos que corresponden a los documentos públicos.
- El Registrador expedirá certificaciones sobre todos los actos y derechos inscritos, su descripción, propietarios, gravámenes, cargas legales y demás datos.

En relación con los notarios, en la LRPN, en su artículo 69, los define como funcionarios de la Dirección Nacional de Registros y del Notariado que tienen la potestad de dar fe pública de los hechos o actos jurídicos ocurridos en su presencia física o a través de medios electrónicos, indicando en este último caso los instrumentos mediante los cuales le otorga presunción de certeza al acto.

Los notarios son competentes en el ámbito de su jurisdicción para dar fe pública de todos los actos, hechos y declaraciones que autoricen con tal carácter, pudiendo entre otros, dar fe pública de:

- Documentos, contratos y demás negocios jurídicos, unilaterales, bilaterales y plurilaterales
- Constancias de cualquier hecho o acta a través de inspección extrajudicial.
- Transcripciones en acta o por cualquier medio de reproducción o de grabación del contenido de archivos públicos o de documentos privados, siempre y cuando no esté expresamente prohibido en el primer caso o lo autorice el dueño o depositario del documento en el segundo caso.
- Transacciones que ocurran en medios electrónicos.
- Autenticar firmas autógrafas, electrónicas y huellas digitales.

Asimismo, por mandato legal, los notarios son competentes para expedir copias certificadas o simples de los documentos y demás asientos que reposen en su oficina, siempre que las copias se soliciten con indicación de la clase de actos o de sus otorgantes, circunstancias éstas que se harán constar en la correspondiente nota de certificación. También podrán expedir copias de documentos originales por procedimientos electrónicos, fotostáticos u otros semejantes de reproducción.

Dicho lo anterior, resta determinar las causales y el procedimiento para tacha del documento electrónico con fe pública

De lo expuesto se desprende que existe la posibilidad legal de dar fe pública a documentos electrónicos, de forma tal que podrán existir documentos electrónicos con fe pública, siendo procedente para su tacha, en cuanto sean aplicables, los supuestos de tacha contenidos en el artículo 1380 del CC, según las cuales puede tacharse un instrumento público o que tenga apariencia de tal por cualquiera de las siguientes causales:

- *"1º Que no ha habido la intervención del funcionario público que aparezca autorizándolo, sino que la firma de éste fue falsificada"*: en este caso, en el campo del documento electrónico, puede tratarse de la asociación al mensaje de datos de otra firma electrónica distinta a la otorgada al funcionario público para que diera la respectiva fe pública.
- *"2º Que aun cuando sea auténtica la firma del funcionario público, la del que apareciere como otorgante del acto fue falsificada*": pudiendo operar en este sentido el mismo supuesto del caso anterior, vale decir, que se haya asociado al mensaje de datos otra firma electrónica distinta a la del otorgante del acto.
- *"3º Que es falsa la comparecencia del otorgante ante el funcionario, certificada por éste, sea que el funcionario haya procedido maliciosamente o que se le haya sorprendido en cuanto a la identidad del otorgante"*: en este caso, es importante señalar que dentro del ejercicio de las competencias del funcionario público, éste debe verificar la identificación del otorgante del documento electrónico, lo que incluye la respectiva verificación del certificado electrónico que utiliza, ya que se puede dar el caso de la utilización de documentos, firmas y certificados electrónicos pertenecientes a otras personas.
- *"4º Que aun siendo auténtica la firma del funcionario público y cierta la comparecencia del otorgante ante aquél, el primero atribuya al segundo declaraciones que éste no ha hecho; pero esta causal no podrá alegarse por el otorgante que haya firmado el acta, ni respecto de él"*: operaría en el mismo sentido en caso del documento electrónico.
- *"5º Que aun siendo ciertas las firmas del funcionario y del otorgante, se hubiesen hecho, con posterioridad al otorgamiento, alteraciones materiales en el cuerpo de la escritura capaces de modificar su sentido o alcance. Esta causal puede alegarse aun respecto de los instrumentos que sólo aparezcan suscritos por el funcionario público que tenga la facultad de autorizarlos"*: este supuesto ataca directamente al documento electrónico cuando este es objeto de alteración, circunstancia que se acredita a través de una experticia sobre el soporte electrónico.
- *"6º Que aun siendo ciertas las firmas del funcionario y los otorgantes, el primero hubiese hecho constar falsamente y en fraude de la Ley o perjuicio de terceros, que el acto se efectuó en fecha o lugar diferentes de los de su verdadera realización"*: en materia del documento electrónico esta causal está directamente relacionada con el certificado electrónico y el servicio de certificación electrónica y la certificación de estampado de tiempo, que son los encargados de garantizar la autoría de la firma electrónica que certifica, así como la integridad del mensaje de satos, y de determinar el momento, lugar, fecha de emisión y/o envío de un documento.

En el campo laboral, la fe pública de un documento electrónico, puede verificarse mediante el uso de la firma electrónica otorgada para el ejercicio de

sus funciones a los Inspectores del Trabajo, Directores del Instituto Nacional de Prevención, Salud y Seguridad Laborales INPSASEL, Jueces del Trabajo, entre otras autoridades laborales. En este caso, debe tratarse de una firma electrónica basada en un certificado expedido por un proveedor de servicios de certificación acreditado ante la Superintendencia de Servicios de Certificación Electrónica.

En cuanto al procedimiento, el CPC patrio en su artículo 438, establece la posibilidad de proponer en juicio civil la tacha de falsedad, ya sea como objeto principal de la causa, ya incidentalmente en el curso de ella. Propuesta la tacha de falsedad de un documento electrónico con fe pública, el procedimiento aplicable es el establecido en el CPC en el artículo 440 y siguientes.

2) Tacha del documento electrónico privado. El documento electrónico que no tenga asociado a él la firma electrónica de un funcionario público que en ejercicio de sus competencias le haya otorgado la fe pública, podrá ser tachado formalmente con acción principal o incidental, como cualquier documento privado, siempre que se verifiquen alguna de las siguientes causales establecidas en el artículo 1.381 del CC:

- *"1º Cuando haya habido falsificación de firmas"*: en este caso, en el campo del documento electrónico, al igual que en el caso de documento electrónico con fe pública, puede tratarse de la asociación al mensaje de datos de otra firma electrónica distinta o de una firma electrónica o certificado electrónico alterada que traiga como consecuencia su falsedad.
- *"2º Cuando la escritura misma se hubiere extendido maliciosamente, y sin conocimiento de quien aparezca como otorgante, encima de una firma en blanco suya*": este supuesto puede ser verificado cuando se asocia a un mensaje de datos una firma electrónica sin el conocimiento del propietario de la misma.
- *"3º Cuando en el cuerpo de la escritura se hubiesen hecho alteraciones materiales capaces de variar el sentido de lo que firmó el otorgante"*: lo que se puede deber a la actuación maliciosa de algún interesado o a alteraciones en la fase de memorización, elaboración o transmisión del documento electrónico.

Es de destacar que en todos los casos, es necesaria la promoción de una prueba pericial a efectos de determinar la manipulación, alteración o falsificación del documento electrónico, circunstancias que sólo puede detectar un experto informático.

En cuanto al procedimiento de tacha, el CPC establece en su artículo 443, la posibilidad de tachar instrumentos privados, aplicable igualmente a los documentos electrónicos privados, indicando que dicha tacha deberá efectuarse en el acto de reconocimiento, o en el acto de contestación de la demanda, o en

el quinto día después de producidos en juicio, si antes no se los hubiese presentado para el reconocimiento, o en apoyo de la demanda, a menos que la tacha verse sobre el reconocimiento mismo. Este procedimiento de tacha por mandato legal, observará en cuanto le son aplicables las mismas normas contenidas en los artículos 440 y siguientes del citado código.

2.3 Promoción del documento electrónico en los procedimientos regidos por la Ley Orgánica Procesal del Trabajo

Este punto analiza la promoción del documento electrónico laboral que tiene su certificado electrónico, que como ya se dijo anteriormente, garantiza la autoría de la firma electrónica que certifica y la integridad del mensaje de datos, y dada su naturaleza de documento privado en materia laboral se rige principalmente por el contenido del artículo 78 y siguientes de la Ley Orgánica Procesal del Trabajo (LOPT), normas que regulan los documentos privados como medios de prueba, destacando entre otros aspectos, los siguientes:

a. Oportunidad de incorporación

En el procedimiento ordinario establecido en la LOPT, el documento electrónico laboral según el interés de la parte promovente, podrá, como todo documento privado, ser acompañado junto con el libelo de la demanda, o promovido en la audiencia preliminar que es la única oportunidad que tienen ambas partes de promover pruebas, no pudiendo promover pruebas por regla general en otra oportunidad posterior, a tenor de lo establecido en el artículo 73 de la LOPT.

1) Incorporación del documento electrónico laboral junto con el libelo de demanda. El documento electrónico laboral público, privado, reconocido o tenido legalmente por reconocido, producido en el proceso en original[45] acompañando al libelo de demanda, se incorporará al expediente junto con el escrito libelar, para ello puede el demandante presentar una copia certificada del documento electrónico emanada de funcionario público que de fe pública del mismo, o las resultas de una inspección judicial previa a la presentación del libelo de demanda, y que haya sido solicitada con el auxilio de un perito capacitado en TIC con el fin que quede levantada en acta la existencia del documento electrónico y su certificado, o las resultas de una inspección extrajudicial que con el mismo objetivo sea

45 Se considera que el documento electrónico laboral es presentado o conservado en su forma original, siempre que el mensaje de datos, vale decir, documento electrónico laboral en este caso, haya sido conservado en su integridad, debiendo estar disponible la información contenida en dicho mensaje de datos, de conformidad con lo establecido en el artículo 7 de la LMDFE de Venezuela.

practica por notario público en ejercicio de las competencias atribuidas en la LRPN patria.

- El documento electrónico laboral que haya sido acompañado al libelo de demanda en formato impreso, se incorporará al expediente junto con el escrito libelar y tendrá el valor de una simple copia fotostática, según lo dispuesto en la LMDFE.
- El documento electrónico laboral público, privado, reconocido o tenido legalmente por reconocido, que no haya sido producido en el proceso en original, y se haya acompañado al libelo de demanda, se incorporará al expediente junto con el escrito libelar, para ello puede el demandante tomar las medidas señaladas en este punto para el documento electrónico laboral público, privado, reconocido o tenido legalmente por reconocido, producido en el proceso en original.

2) Incorporación del documento electrónico laboral en la audiencia preliminar. El documento electrónico laboral que haya sido promovido en la audiencia preliminar, se incorporará a las actas del expediente por el juez de sustanciación, mediación y ejecución, una vez finalizada la audiencia preliminar, a los fines de su admisión y evacuación ante el juez de juicio. Dicha incorporación, dada la naturaleza del documento electrónico laboral, basada en su forma inteligible en formato electrónico, pueda darse, entre otras formas de la siguiente manera:

- Mediante la incorporación a las actas del expediente de una copia certificada del documento electrónico emanada de funcionario público que de fe pública del mismo, siempre que la misma haya sido promovida en la debida oportunidad. La copia certificada para que tenga el valor de original habrá de producirse en formato electrónico.
- A través de las resultas de una inspección judicial previa a la instalación de la audiencia preliminar, y que haya sido solicitada con el auxilio de un perito capacitado en TIC, con el fin que quede levantada en acta la existencia del documento electrónico laboral, la firma electrónica y su certificado, de ser el caso.
- Consignando las resultas de una inspección extrajudicial practicada por notario público, antes de la audiencia preliminar, con el objetivo de dejar constancia en acta de la existencia según corresponda, del documento electrónico laboral, la firma electrónica y su certificado.
- Mediante las resultas de la inspección judicial, que promovida en la debida oportunidad, sea evacuada en la audiencia de juicio con el auxilio de perito capacitado en TIC que pueda dejar constancia según corresponda, de la existencia del documento electrónico laboral, la firma electrónica y su certificado electrónico, en aras de probar la integridad del mensaje de datos promovido y la autoría del mismo.

- A través de la evacuación de la prueba de informes debidamente promovida, dirigida según el caso, a oficinas públicas, bancos, asociaciones gremiales, sociedades civiles o mercantiles e instituciones similares, con el fin que rindan informe sobre la existencia del documento electrónico, señalado en el proceso, su integridad, la firma electrónica que tenga asociada y su certificado electrónico según sea el caso[46].
- Mediante la evacuación de la prueba de exhibición promovida en la audiencia preliminar, de conformidad con lo establecido en el artículo 82 de la LOPT, evacuación que dada la naturaleza inteligible en soporte electrónico del mensaje de datos, puede ser realizada en presencia del juez y con el auxilio de perito capacitado en TIC.
- Mediante la consignación del formato impreso del documento electrónico laboral, cuyo valor en este caso será de una simple fotocopia.

b. La carga de la prueba

En materia de Derecho laboral, por regla general, la carga de la prueba corresponde a quien afirme hechos que configuren su pretensión o a quien los contradiga, alegando nuevos hechos, pero el patrono siempre tiene la carga de la prueba de las causas del despido y del pago liberatorio de las obligaciones inherentes a la relación de trabajo, mientras que el trabajador cuando le corresponda probar la relación de trabajo, gozará de la presunción de su existencia, siendo carga del patrono, desvirtuar dicha presunción.

c. Admisión como medio de prueba

La respuesta sobre la admisión o negativa de admisión del documento electrónico laboral como medio de prueba, será providenciada por el juez de juicio dentro de los cinco (5) días hábiles siguientes al recibo del expediente[47]. Dada la naturaleza del documento electrónico laboral, el juez al admitirlo como medio de prueba, debe indicar con claridad si para su evacuación va a aplicar la forma de evacuación de un medio semejante, o va a establecer una forma autónoma de evacuación del citado documento electrónico laboral.

d. Control y contradicción

1) Reconocimiento del documento electrónico laboral. El reconocimiento del documento electrónico laboral, opera:

46 Esto de conformidad con lo establecido en el artículo 81 de la LOPT.
47 De conformidad con lo establecido en el artículo 75 de la LOPT.

- Cuando la parte contra quien se produzca en la audiencia preliminar un documento electrónico como emanado de ella, o de algún causante suyo, lo reconoce formalmente.
- En el supuesto que la parte contra quien se haya producido un documento electrónico laboral, guarde silencio acerca del formal desconocimiento o reconocimiento de dicho instrumento
- Por interpretación en contrario del contenido del artículo 78 de la LOPT, quedará reconocido el documento electrónico laboral privado, producido en original o en copias o reproducciones fotostáticas o por cualquier otro medio mecánico, claramente inteligible, si la parte contra quien obra dicho documento, no lo impugnase.

En el supuesto de ser impugnado el documento electrónico laboral, la mencionada ley adjetiva del trabajo, no establece en forma expresa procedimiento alguno, por lo que corresponde al juez laboral como rector del proceso, indicar el modo y el lapso para que cada una de las partes actúe en defensa de su pretensión con respecto al documento impugnado. Ello no obsta para que en ejercicio del derecho de la defensa, el debido proceso y el derecho a petición, las partes soliciten al juez lo que consideren respecto a sus afirmaciones o negaciones.

2) Desconocimiento de la firma electrónica en el procedimiento laboral ordinario. El desconocimiento de la firma electrónica asociada al mensaje de datos por la parte contra quien se produjo el documento electrónico, implica para la parte que produjo el mismo la carga de probar su autenticidad. A este efecto, puede promover la prueba de cotejo, debiendo señalar uno o varios de los documentos indubitados indicados en el artículo 90 de la LOPT, que son los mismos documentos indubitados contemplados en el artículo 448 del CPC, que fueron analizados anteriormente, al abordar el reconocimiento del documento electrónico en aquellos procedimientos regidos por el CPC, siendo lo allí señalado aplicable a la prueba de cotejo para probar la autenticidad del documento electrónico según lo establecido en el citado artículo 90 de la ley adjetiva del trabajo.

e. Tacha

La tacha de falsedad de los documentos electrónicos laborales públicos y los privados, reconocidos o tenidos legalmente por reconocidos, se puede proponer incidentalmente en el curso de un procedimiento laboral, específicamente en la audiencia de juicio, con fundamento en los motivos señalados en el artículo 83 de la LOPT. Dichos motivos son idénticos a los establecidos en el artículo 1.380 del CC, como causales de tacha de instrumento público o que tenga apariencia de tal. Al tratar la tacha de instrumento público en los procedimientos regidos por el CPC, se analizaron cada una de dichas

causales, siendo aplicable lo allí señalado a la tacha del documento electrónico laboral normada en el citado artículo 83 de la ley adjetiva laboral.

3. Valor jurídico del documento electrónico

Existen principalmente tres criterios fundamentales para la valoración de las pruebas: el criterio de la prueba tasada, que supone para el juez una imposición legal de manera abstracta y preestablecida del valor que debe atribuir a cada medio probatorio; el criterio de la prueba libre, en la que el juez valora cada prueba según su convicción, y el criterio de la prueba mixta, que supone se adopte el criterio de la prueba legal para determinados medios probatorios como los documentos públicos y para los restantes medios de prueba se aplique la libre apreciación, conforme a la regla de la sana critica[48].

Para Eduardo J. Couture[49], las reglas de la sana crítica, son ante todo las reglas del correcto entendimiento humano, interfiriendo en ellas las reglas de la lógica con las reglas de la experiencia del juez, quien no es libre de razonar en forma discrecional y arbitraria, sino mediante la lógica y la experiencia sin excesivas abstracciones del orden intelectual y sin olvidar los preceptos llamados por los filósofos higiene mental, que buscan asegurar el más certero y eficaz razonamiento.

Hernando Devis Echandía[50], señala que la sana crítica consiste en la libertad de apreciar las pruebas, de acuerdo con la lógica y las reglas de experiencia, que sean aplicables a cada caso según el criterio personal del juez.

Bello Tabares[51], considera que el operador de justicia, mediante el uso de la sana crítica como sistema de valoración, al momento de apreciar y valorar una prueba realiza una actividad silogística, donde la premisa menor estará constituida por el medio de prueba traído de oficio o aportado por las partes al proceso, mientras que la premisa mayor estará constituida por las máximas de experiencia del juzgador, y la conclusión será la existencia o inexistencia del hecho controvertido, que es el tema de la prueba.

El sistema de valoración de pruebas documentales, ordenado para los procedimientos regidos por el CPC, es el de la prueba mixta, que según lo establecido en el artículo 507 de dicho Código, ordena al juez, a menos que exista una regla legal expresa para valorar el mérito de la prueba, apreciarla según las reglas de la sana crítica.

48 CARRASCOSA LÓPEZ, V., POZO ARRANZ, M. A., RODRÍGUEZ DE CASTRO, E. P.: *La contratación informática…, op. cit*. p. 62.

49 COUTURE, E.: *Fundamentos del derecho procesal civil*, *op. cit.* p. 270-271.

50 Hernando DEVIS ECHANDÍA, citado por BELLO TABARES, H. E., "Ley Orgánica Procesal del Trabajo" *Ensayos Volumen II*, Caracas: Tribunal Supremo de Justicia. Serie Normativa N° 4. 2004. P. 799-800.

51 BELLO TABARES, H.: "Ley Orgánica Procesal del Trabajo". *op. cit*. p. 800.

Por su parte, el sistema de valoración de pruebas acogido por el legislador venezolano en la LOPT, es el de sana crítica que se asemeja al sistema de la libre convicción pero razonada, lo que implica que el operador de justicia, no puede decidir en forma arbitraria ni caprichosa lo que considere, sino que se ve obligado a emplear la lógica y las máximas de experiencia en su razonamiento para la toma de la respectiva decisión, sin obviar lo establecido para determinada pruebas en la ley, como sería el caso de los documentos públicos, reconocidos o tenidos legalmente por reconocidos. Adicionalmente a ello, si llegase a tener dudas sobre la valoración de una prueba, por mandato legal[52] debe optar por la valoración que resulte más favorable para el trabajador.

La sana crítica también está contemplada como elemento de valoración probatoria en la LMDFE, a tal respecto cabe citar el artículo 17 que señala que la firma electrónica que no cumpla con los requisitos establecidos en la ley para su equiparación con la firma manuscrita, podrá constituir un elemento de convicción valorable en juicio, conforme a las reglas de la sana crítica.

El documento electrónico laboral, gracias a la aplicación del principio de equivalencia funcional, ha de ser valorado en materia de Derecho del trabajo, con aplicación de las reglas de la sana crítica, respetando los mismos criterios y normas empleadas para la valoración de los documentos escritos en soporte papel, dentro de los que se encuentran los auténticos o que tienen fe pública, los documentos privados que han sido reconocidos o se tienen legalmente por reconocidos y los documentos privados que no han sido reconocidos ni se tienen legalmente como tales.

Aplicando lo anterior a los documentos electrónicos en general y al documento electrónico laboral, se destacan entre otros, los siguientes supuestos:

1. **Documento electrónico con fe pública**. Tiene el mismo valor probatorio que el documento público o autentico, vale decir, hace plena fe de su contenido entre las partes y frente a terceros, mientras no sea declarado falso[53]. De forma tal que hace plena fe de los hechos jurídicos que el funcionario público declare haber efectuado, y de los hechos jurídicos que el funcionario público declare haber visto u oído, siempre que esté facultado para hacerlos constar. A manera de ejemplo, de la gran cantidad de documentos electrónicos que pueden existir, se señalan entre otros, los poderes, contratos electrónicos a los que el notario le dio fe pública[54] en ejercicio de las competencias atribuidas en el artículo 75 de la Ley de Registro Público y del Notariado, en concordancia con lo establecido en el artículo 23 de la citada ley, que establece que el proceso

52 Artículo 10 de la Ley Orgánica Procesal del Trabajo.

53 Aplicando por equivalencia funcional el artículo 1.359 del CC venezolano.

54 Tal y como se señaló anteriormente, antes del otorgamiento de dicha fe pública, el notario debe verificar la identificación de las partes, lo que implica la verificación de sus firmas y certificados electrónicos, según corresponda.

registral y notarial podrá ser llevado a cabo íntegramente a partir de un documento electrónico.

Asimismo, el notario puede autenticar firmas electrónicas, lo que facilitaría probar la autoría del mensaje de datos que tenga asociada dicha firma electrónica autenticada, siempre que no sea invalidada tal asociación, lo que pudiese ocurrir al quedar demostrado que la firma electrónica no corresponde a la asociada al mensaje de datos que se quiera hacer valer como medio de prueba, o que el mismo fue alterado, o que el firmante no tenía conocimiento del mensaje de datos al que se asoció su firma electrónica entre otros casos, o que el resultado de la tacha de dicho documento, invalidara el mismo perdiendo la valor probatorio que se le había otorgado.

Cabe destacar que el notario, que es un funcionario del Servicio Autónomo de Registros y Notarías tiene la potestad de dar fe pública de los hechos o actos jurídicos ocurridos en su presencia física o a través de medios electrónicos, indicando en este último caso los instrumentos mediante los cuales le otorga presunción de certeza al acto[55], debiendo señalar entre otros en el caso del contrato electrónico, la verificación del mensaje de datos, la firma electrónica asociada a éste y el certificado electrónico según corresponda, en aras de garantizar la integridad del mensaje de datos y la autoría del mismo.

2. Documento electrónico reconocido o tenido legalmente por reconocido. Este instrumento tiene entre las partes y respecto de terceros la misma eficacia probatoria que el documento público, ya explicado.

1) Documento electrónico con firma electrónica y certificado electrónico. Presentado como original por haberse cumplido los requisitos del articulo 7 LMDFE, tiene el mismo valor probatorio de un documento privado, vale decir, hace plena prueba de su contenido si no es desvirtuado o desconocido por la parte contra quien se produjo el mismo como emanado de ella.

2) Documento electrónico con firma electrónica pero sin certificado electrónico. A este instrumento no puede atribuírsele *a priori* el mismo valor probatorio de un documento privado firmado en soporte papel, ya que no hay garantía de la integridad del mensaje de datos y la autoría del mismo. Dependerá de la comprobación de su autoría y de la integridad del mensaje para que pueda atribuírsele el valor probatorio de un documento escrito, por lo que constituirá un elemento de convicción valorable conforme a las reglas de la sana crítica, según lo establecido en el artículo 17 de la LMDFE.

55 Según lo establecido en el artículo 69 de la LRPN.

3) Documento electrónico sin firma electrónica asociada. El problema para su valoración de este instrumento se encuentra en la determinación de su autoría, ya que al no estar firmado, ni siquiera aplican las normas del desconocimiento del documento, ya que las mismas versan directamente sobre la firma, que es lo que se coteja, o se prueba con testigos según sea el caso. De forma tal, que será un simple indicio que necesariamente deberá el sentenciador en aplicación de las reglas de la sana crítica, adminicular con otros elementos existentes, producido en el juicio y/o basados en la lógica y las máximas de experiencia del juzgador.

Ciberseguridad en Venezuela y su impacto en las redes sociales: protección vs. violación de derechos*

Gladys Rodríguez**

SUMARIO: I. Introducción. II. Algunas consideraciones previas. III. Clases de ataques y atacantes en las redes sociales virtuales. 1. Ataques. 2. Tipos de atacantes. 3. Iniciativas internacionales humanitarias frente a estas categorías de ataques y atacantes IV. Redes sociales y ciberseguridad en Venezuela. 1. Marco legal relativo a la libertad de expresión e información. 2. Impacto de la ciberseguridad en el entorno digital en Venezuela. V. Algunas consideraciones finales.

Resumen

El presente artículo expone el impacto que implica la ciberseguridad de la información en Venezuela, con especial referencia a las redes sociales virtuales. Se analiza la providencia administrativa 01/09 de fecha 22 de diciembre de 2009 de la Comisión Nacional de Telecomunicaciones (CONATEL) y los informes anuales 2009 y 2013 del Programa Venezolano Educación-Acción en Derechos Humanos (PROVEA), sobre "Derecho a la libertad de expresión e información", concluyendo que los intentos de dominación y control del ciberespacio menoscaban los derechos de los ciudadanos a la libertad de expresión, derecho a la información, secreto a las comunicaciones y su inviolabilidad.

Palabras Clave: Ciberseguridad. Redes sociales virtuales. Venezuela. Derechos de los ciudadanos.

Recibido: 11/8/2014 • Aceptado: 12/9/2014

* Este trabajo ha sido realizado en el marco del proyecto de Investigación intitulado: Regulación de la ciberseguridad de la información en el Estado venezolano: avances y desafíos en las redes sociales virtuales, financiado por el Consejo de Desarrollo Científico y Humanístico adscrito al Vicerrectorado Académico de la Universidad del Zulia.

** Abogada. Magister en Planificación y Gerencia de Ciencia y Tecnología, Doctora en Derecho. Postdoctora en Gerencia en las Organizaciones. Profesora Titular de la Universidad del Zulia. Investigadora adscrita al Instituto de Filosofía del Derecho de la Facultad de Ciencias Jurídicas y Políticas de L.U.Z.

Abstract

This paper presents the impact of cybersecurity of information in Venezuela, with special reference to social networks. The administrative ruling 01/09 dated December 22, 2009 of the National Commission Telecomunicacione (CONATEL), and annual reports 2009 and 2013 from Venezuelan Program Education-Action in Human Rights (PROVEA) on "Right to Freedom of Speech and Information" are analyzed, concluding that attempts to dominate and control of cyberspace, impair the rights of citizens to freedom of speech, right to information, communications secrecy and inviolability.

Key words: Cybersecurity. Social Networks. Venezuela. Citizens' rights.

I. Introducción

El presente trabajo reflexiona cualitativamente sobre la base de una investigación documental que expone el impacto que implica la ciberseguridad de la información en Venezuela, con especial referencia a las redes sociales virtuales. Se parte de la revisión de varios autores. De igual modo es objeto de referencia la providencia administrativa 01/09 de fecha 22 de diciembre de 2009 de la Comisión Nacional de Telecomunicaciones (CONATEL) (sustituida por la actual providencia administrativa N° 027, publicada en la Gaceta Oficial N° 40.415, de 20 de mayo de 2014)[1], y los informes anuales 2009 y 2013 del Programa Venezolano Educación-Acción en Derechos Humanos (PROVEA), sobre "Derecho a la libertad de expresión e información". Un primer aspecto a abordar es precisar conceptualmente algunos términos que se usaron a lo largo de la investigación, seguidamente se describen los principales ataques y atacantes en el entorno de las redes sociales virtuales, así como las iniciativas internacionales para enfrentar este fenómeno. Finalmente se explica la relación: redes sociales virtuales y ciberseguridad en Venezuela, destacándose el marco legal y el impacto que la ciberseguridad ha significado en el ámbito digital. Se concluye que los intentos de dominación y control del ciberespacio menoscaban la libertad de expresión, el derecho a la información, el secreto a las comunicaciones y su inviolabilidad, entre otros derechos y, son efectuados tanto por *totalitarios*, como por sedicentes democracias, en ambos extremos se tienen

1 Esta providencia contiene la actual Norma Técnica sobre los Servicios de Producción Nacional Audiovisual y otros Servicios de Producción Audiovisual y deja sin efecto el instrumento legal de 2009. Siguiendo el objeto de la investigación, se hace referencia a la norma de 2009 en el entendido que los hechos que se analizan ocurrieron bajo la vigencia de la norma derogada, aunque en el trabajo se hará una breve referencia comparativa entre ambas providencias y el impacto de la nueva "Norma Técnica" en materia de libertad de expresión.

como ejemplos por un lado: China, Arabia Saudita, entre otros y, por el otro: a los países *Echelon*[2].

II. Algunas consideraciones previas

En el marco de esta investigación, resulta oportuno precisar algunos conceptos básicos tales como: Internet o ciberespacio, ciberseguridad, computación en la nube y redes sociales virtuales. En atención a ello, Internet la define Joyanes (1997: 79)[3] como *"una red mundial de computadoras que permite la comunicación directa y transparente, compartiendo información y servicios a lo largo del mundo…"*. Por su parte, Boizard (1996: 1)[4] argumentan que *"la Internet es como la red de computadoras más grande del mundo, que conecta cientos de redes, permitiendo la comunicación de personas con distintos lugares o países y una posterior transferencia de información (documentos) a distancia"*. Así también, Internet permite que el concepto de comunicación que contiene en su definición la palabra –distancia– fuente básica de concepción de la realidad no represente una limitación, incorporándose a un modelo vecinal, por lo que sumergirse en ésta conlleva sorprenderse de la capacidad ilimitada que se adquiere de adentrarse en otros mundos. Estas definiciones se acercan a la idea de una sociedad interconectada, donde la red de redes, que se conoce como Internet, da paso a un escenario hoy denominado ciberespacio. Por ello, resulta conveniente agregar la definición del Diccionario de la Real Academia Española (DRAE) en su 22ª edición[5], el cual define ciberespacio, con una única acepción, como el *"Ámbito artificial creado por medios informáticos"*. En realidad, se entiende que la RAE se está refiriendo a un entorno no físico creado por un equipo informático con el objetivo de interoperar en una Red. En consecuencia, el mayor ámbito del ciberespacio es Internet.

El término fue utilizado por primera vez en la obra Neuromante del escritor norteamericano William Gibson y publicada en el emblemático 1984 que presagia Orwell. También podríamos definir el ciberespacio desde su perspectiva original como un conjunto o realidad virtual donde se agrupan usuarios, páginas web, chat y demás servicios de Internet además de otras redes. En definitiva el

2 Se considera que ECHELON, que pasó de un sistema de control contra la ex URSS a un sistema global de espionaje, controla el 90% de las comunicaciones en el ámbito global. Involucra a fieles aliados de Estados Unidos de América, léase: Australia, Nueva Zelanda, Canadá y Gran Bretaña en el marco del acuerdo UKUSA (conocido también como proyecto cinco ojos y que se remonta a la segunda guerra mundial) cuyo propósito principal era compartir información de inteligencia. Jofré, P (2013) **Echelon: Espionaje global** En: http://radio.uchile.cl/2013/09/13/echelon-espionaje-global consultado 4 de agosto de 2014)

3 JOYANES, L. (1997) *Cibersociedad: los retos sociales ante un nuevo mundo digital*. Editorial McGraw-Hill, Interamericana de España. p.155

4 BOIZARD, A. (1996) *Internet en acción*. México: Editorial McGraw-Hill. P. 237

5 www.rae.es (Consulta: 2014, julio, 30)

ciberespacio es, como apunta Joyanes (2011:30)[6], *"El espacio donde se navega por Internet, se realizan conversaciones por Skype o en las redes sociales, o estamos cuando consultamos el correo electrónico, chateamos o visitamos un periódico digital"*.

No obstante, los evidentes beneficios que resultan de tal combinación de realidad y virtualidad, el autor Castells (2003: 159)[7]:

> …defiende la idea que la expansión de Internet está conduciendo hacia un aislamiento social y una ruptura de la comunicación social y la vida familiar, porque los individuos se refugian en el anonimato y practican una sociabilidad aleatoria, abandonando la interacción personal cara a cara en espacios reales.

En consecuencia, se ha acusado a Internet de incitar gradualmente a la gente a vivir sus propias fantasías *on line* y huir del mundo real, en una cultura cada vez más dominada por la realidad virtual (Olivares, Vera y Durante, 2010)[8]. Ello ha significado ver el otro lado, quizás no tan positivo del fenómeno tecnológico en su interacción con el ser humano, y de allí que algunos como el propio Castells (1999)[9], se apunten por la idea de regular la Internet, concluyendo:

> Internet, en nuestro tiempo, necesita libertad para desplegar su extraordinario potencial de comunicación y de creatividad. Asimismo, la libertad de expresión y de comunicación ha encontrado en Internet su soporte material adecuado. Pero tanto Internet, como la libertad, sólo pueden vivir en las mentes y en los corazones de una sociedad libre, libre para todos, que modele sus instituciones políticas a imagen y semejanza de su práctica de libertad.

Por su parte, Castro (2003: 16)[10] afirma:

> La aplicación del derecho a Internet se fundamenta en el debate entre la defensa de la autonomía, privacidad y anonimato del usuario individual, y por otra parte la preocupación por el derecho de empresa a la libre actuación en Internet y a la defensa de la seguridad colectiva, aun si ésta implica un menoscabo de la seguridad individual.

6 JOYANES, L (2011). "Introducción. El estado del arte de la Ciberseguridad". *Ciberseguridad. Retos y Amenazas a la seguridad nacional en el ciberespacio*. Cuadernos de Estrategia. Grupo No. 03/10. Ministerio de Defensa. Instituto español de estudios estratégicos. Instituto Universitario "General Gutiérrez Mellado". Febrero, 2011

7 Castell, M. (2003). *La Galaxia Internet.* Primera Edición. Barcelona: Editorial Debolsillo.

8 OLIVARES, VERA y Durante 2010. "Sociedad de la información: Regulación del tejido de redes". *En: Revista Espacio Abierto*. Vol 19, No. 1 enero –marzo, 2010, pp. 137-147.

9 CASTELL, M. (1999) *La era de la Información: Economía, sociedad y cultura***.** Vol 1. La sociedad red. Madrid: Alianza Editorial.

10 CASTRO, A (2003). La regulación de Internet: un reto jurídico**.** Disponible: http://www.uned.ac.cr/redti/documentos/regulacion.pdf. (Consulta 2008, abril 08)

Como se puede observar, se trata de dos primeros significados –Internet y ciberespacio– íntimamente relacionados entre sí y con la propuesta de una regulación.

De igual manera, otro significado a exponer, es la ciberseguridad, a criterio particular de la autora, la ciberseguridad es un conjunto de estrategias tanto técnicas, militares, políticas y jurídicas que permiten evitar que principalmente los Estados y las organizaciones, públicas y privadas sean objeto de daño, amenazas y acciones terroristas a sus instalaciones físicas y de telecomunicaciones en su mayoría de carácter estratégico, para la defensa y seguridad del Estado o la organización mismo, empleando para ello sistemas sofisticados de virus, software y cualquier tecnología maliciosa.

Frente a potenciales amenazas, desde hace varios años, los Estados se han preocupado por mantener bajo sistemas de seguridad sus bienes, servicios y ciudadanos. De ello han surgido varios mecanismos de espionaje por parte de los Estados, uno de los casos ejemplificantes es la organización multinacional de escuchas UKUSA, creada por varios tratados secretos de posguerra entre Estados Unidos de América y Gran Bretaña, se llama hoy a sí misma los Cinco Ojos. Las agencias que forman parte de ella compiten por ver quién tiene más penetración en las comunicaciones privadas y comerciales a través de Internet. Los Cinco Ojos son los servicios de inteligencia de señales (SIGINT) de los Estados Unidos de América, el Reino Unido, Canadá, Australia y Nueva Zelanda. Engloban la Agencia de Seguridad Nacional estadounidense (NSA) y el Cuartel General de Comunicaciones del Gobierno Británico (GCHQ). En los documentos se encuentran numerosos comentarios informales que demuestran que la mayor satisfacción, para los agentes de los servicios de inteligencia, es vigilar todo, franquear el mayor número posible de sistemas de privacidad y, hoy es lo que se conoce como países Echelon. (Campbell, D 2013.)[11]

En este sentido, Venezuela ha venido denunciando, a través de la Comisión Nacional de Telecomunicaciones (CONATEL), una amenaza de ciberguerra, especialmente, si resulta aprobada la Ley S.2148[12] por parte del Congreso de los Estados Unidos de América. *"El estatuto tiene como escenario la instalación de posibles bases para la emisión de señales radioeléctricas, lo que podría crear una posible invasión de dicho espacio en Venezuela*

11 CAMPBELL, D (2013.) Bajo la vigilancia de los cinco ojos. http://internacional.elpais.com/internacional/2013/07/05/actualidad/1373038892_139217.html (Consulta 2014, agosto, 04)

12 Esta ley legaliza la ciberguerra contra Venezuela y coartaría el acceso libre a internet en el país, lo que le permitiría a los Estados Unidos desarrollar estrategias mediáticas en el aspecto radioeléctrico y tener acceso a la distribución de contenidos", dijo durante su participación el Presidente de CONATEL, en el programa "Temprano Con", que transmite el Sistema Radio Mundial. En: Correo del Orinoco (2014) Director de CONATEL: Ley S.2148 legaliza la ciberguerra contra Venezuela. En www.aporrea.org. (Consulta: 2014, agosto, 04)

tal y como ha ocurrido en Cuba, Irak y Siria, aseguró su Presidente". (Correo del Orinoco. 2014)[13].

En consecuencia, Venezuela al igual que el resto del mundo, ve amenazados sus intereses y en el caso particular, Venezuela ha creado un comando cibernético para enfrentar las situaciones de amenazas, entre otras estrategias a las que se harán referencia más adelante. El problema no es crear estrategias de seguridad y, en especial de ciberseguridad por parte de los Estados o las organizaciones, sino cuando estos mecanismos de protección frente a posibles amenazas y, en este caso, ciberguerras o ciberamenazas trascienden los límites y se cometen abusos o se impide el ejercicio de algún derecho a los ciudadanos.

La realidad es que existen cientos de software maliciosos como el *malware*, que atentan contra la seguridad de un terminal y, hoy evolucionan de los computadores de escritorio hacia los móviles, donde las redes sociales son un caldo de cultivo perfecto para acceder de manera maliciosa. Es entendible: acceder a un dispositivo móvil desde, por ejemplo, una red *wi-fi* desconocida, la cual puede ser la puerta de entrada perfecta para algún ansioso. Y el fin es el mismo: provocar daño o recoger datos personales "a la mala". Una de las regiones más propensas a caer en estas trampas virtuales es Latinoamérica.

La razón es sencilla, según explica Dmitry Bestuzhev[14], encargado de la región por parte de la empresa de Kaspersky Lab.. *"El mayor problema de los latinos es que son demasiado sociales. Esa región es más confiada y cálida con sus contactos. Sospechan menos, o puede ser que haya más ingenuidad por parte de los usuarios"*. El blanco de los creadores de *malware* apunta principalmente al Cono Sur, específicamente a cuentas bancarias. Otro riesgo es el denominado *phishing* (correos fraudulentos que se hacen pasar por casas comerciales o bancarias para obtener datos) y, que es altísimamente común. Porque saben que en esta región los usuarios son más curiosos a la hora que les llega un *link*, ya sea vía *Facebook* o a través de un mensaje directo en *Twitter*. Agrega Bestuzhev,

> …la amenaza tampoco deja afuera a los videojuegos, en aquellos multijugadores, donde uno se puede encontrar virtualmente con cualquier persona en el mundo, las posibilidades de acceder a un *link* o código virulento son altas. Por otro lado, también está el tema de las monedas virtuales (como *Bitcoin*) y los bienes en juegos de rol (como el *World of Warcraft*) que son vendidos en el mercado negro virtual por dinero real. Eso técnicamente también es un crimen, por el no pago de impuestos.

13 Correo del Orinoco. 2014. *Director de CONATEL: Ley S.2148 legaliza la ciberguerra contra Venezuela.* www.aporrea.org. (Consulta: 2014, agosto, 04)

14 Revista Qué pasa (Chile): La ciberseguridad de Mr. K.http://www.quepasa.cl/articulo/tecnologia/2013/08/23-12457-9-tecnologia (Consulta 2014, abril, 03)

Estos aspectos de ciberseguridad se retomarán más adelante. Continuando con las consideraciones previas, otro concepto empleado en el entorno digital recién es la computación en la nube. La nube o en inglés *Cloud Computing:* Es el conjunto "infinito" de servidores de información (computadores) desplegados en centros de datos, a lo largo de todo el mundo donde se almacenan millones de aplicaciones web y enormes cantidades de datos (*big data*), a disposición de miles de organizaciones y empresas, y cientos de miles de usuarios que se descargan y ejecutan directamente los programas y aplicaciones de software almacenados en dichos servidores tales como *Google Maps, Gmail, Facebook, Tuenti o Flickr*. La nube está propiciando una nueva revolución industrial soportada en las nuevas fábricas de "datos" (Centros de Datos, *Data Centers*) y de "aplicaciones web (*Web Apps*). (Joyanes, 2011)[15].

Existen organismos internacionales, uno de estos organismos más reconocido es el *National Institute of Standards and Technology (NIST*)[16], señala que el modelo de la nube se compone de cinco características esenciales, tres modelos de servicio y cuatro modelos de despliegue. La nube en sí misma, es un conjunto de *hardware* y *software*, almacenamiento, servicios e interfaces que facilitan la entrada de la información como un servicio. Los servicios de la nube incluyen el software, infraestructura y almacenamiento en Internet, bien como componentes independientes o como una plataforma completa –basada en la demanda del usuario–. Los modelos de entrega y despliegue de servicios en la nube más usuales que se ofrecen a los clientes y usuarios de la nube (organizaciones, empresas y usuarios) son: PaaS (*Platform as a Service*), plataforma como servicio, IaaS *(Infrastructure as a Service*), infraestructura como servicio y SaaS (*Software as a Service*), software como servicio.

Finalmente, en estas consideraciones previas el constructo referente a las redes sociales virtuales, es necesario abordarlo. Desde el ámbito jurídico, en Venezuela no hay una definición legal sobre qué entender por redes sociales. Sin embargo, el Grupo de Trabajo sobre Protección de Datos del artículo 29 de la Directiva 95/46/CE de protección de datos, de fecha 12 de junio de 2009, en su Dictamen 5/2009 sobre redes sociales en línea, define a éstas como: *"plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes…"*

Por su parte, Gil indica (2012:219)[17]:

15 JOYANES, L (2011). *Introducción. El estado del arte de la Ciberseguridad*…. op.cit.p.13 y ss

16 El NIST es una Agencia del Departamento de Comercio de los Estados Unidos de América. Dentro del NIST, el *Computer Security Resource Center* (CSRC) se encarga de los estándares de las Tecnologías de la Información y, en concreto, de *Cloud Computing.*

17 GIL, A (2012) "El fenómeno de las redes sociales y los cambios en la vigencia de los derechos fundamentales" En *Revista de Derecho UNED*, No. 10, 2012, pp. 209-255

> …se puede definir en forma genérica, una red social *on line* como aquellos servicios de la sociedad de la información que ofrecen a los usuarios una plataforma de comunicación a través de Internet para que estos generen un perfil con sus datos personales facilitando la creación de redes con base a criterios comunes y permitiendo la conexión de unos usuarios con otros y su interacción.

En definitiva se tiene que las redes sociales virtuales (RSV en adelante), independientemente de la tipología a la que pertenezcan, comparten un conjunto de características. Estas características comunes incluyen un fácil acceso, con conexión rápida y dinámica de los usuarios que forman parte de la RSV, la compartición de todo tipo de información entre los usuarios de la RSV, la difusión viral a través de sus usuarios y los riesgos a los que se ven expuestos los usuarios. Nos quedaremos con este último concepto. Los usuarios de las RSV están expuestos a un conjunto de amenazas y riesgos que, en mayor o menor medida, pueden afectar a su seguridad. En la actualidad, las RSV basadas en perfiles son la topología de RSV que exponen a sus usuarios a un mayor número de amenazas y riesgos[18]. Esto se debe, fundamentalmente, a que se trata de la topología que solicita y maneja mayor cantidad de datos de carácter personal[19]. Acciones tan cotidianas, dentro de una RSV, como publicar datos de carácter personal, enviar mensajes privados, publicar fotos, etiquetar amigos, descargar aplicaciones, etc. llevan asociados un conjunto de amenazas y riesgos contra nuestra privacidad y, por ende, contra la propia ciberseguridad en su conjunto.

III. Clases de ataques y atacantes en las redes sociales virtuales

1. Ataques

Según Caro (2011)[20], los ataques surgen al mismo tiempo que las Tecnologías de la Información, en estas tecnologías no sólo se engloban los ordenadores sino cualquier dispositivo electrónico, como es el caso de los teléfonos móviles, las agendas electrónicas, GPS, las tabletas electrónicas, etc., así como las comunicaciones. Estos ataques pueden afectar a cualquier nivel: ciudadanos,

18 La perspectiva interna del negocio abarca todos los procesos relacionados con la gestión de la seguridad de la plataforma que da soporte a la RSV como la seguridad lógica, el control de accesos, la continuidad del servicio, la gestión de incidencias, el cifrado de las comunicaciones, el *hacking* ético, los permisos sobre el contenido publicado, etc.

19 Por último, la perspectiva financiera incluye todas las cuestiones relacionadas con el comercio electrónico y las plataformas de pago de las RSV

20 CARO, M (2011) "Alcance y ámbito de la seguridad nacional en el Ciberespacio. *Ciberseguridad. Retos y Amenazas a la seguridad nacional en el ciberespacio. Cuadernos de Estrategia*. Grupo No. 03/10. *Cap. II*. Ministerio de Defensa. Instituto español de estudios estratégicos. Instituto Universitario "General Gutiérrez Mellado". Febrero, 2011. pp. 49-82

empresas, administración, infraestructuras críticas, sector bancario, etc. Se habla incluso de amenazas avanzadas[21].

La mayoría de los ataques se aprovechan de vulnerabilidades de los sistemas informáticos, agujeros de seguridad que surgen de una deficiente programación que no tiene en cuenta la seguridad en el ciclo de vida del desarrollo del software y los diversos protocolos de comunicación.

Con el tiempo muchos protocolos fueron avanzando hacia versiones más seguras, por ejemplo Telnet y SSL, http y https, ftp y sftp, etc. Un caso especial son las redes sociales cuya falta de seguridad afecta a la ciudadanía, en particular a los menores, que en ocasiones son objeto de la llamada ingeniería social y acaban siendo víctimas de acoso sexual, o revelación de información personal.

Algunos de los tipos de ataques más conocidos y cuya definición figura en una de las guías del Centro Criptológico Nacional (CCN) y en sus siglas en inglés *Computer Emergency Response Team* (CERT). En este caso CCN-CERT del gobierno español[22] son:

- Virus: programa que está diseñado para copiarse a sí mismo con la intención de infectar otros programas o ficheros.
- Código dañino, también conocido como código malicioso, maligno o "malware" en su acepción inglesa: software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial[23].
- Bomba lógica: segmento de un programa que comprueba constantemente el cumplimiento de alguna condición lógica (por ejemplo, número de accesos a una parte del disco) o temporal (satisfacción de una cierta fecha). Cuando ello ocurre, desencadenan alguna acción no autorizada. En ocasiones, si la condición a verificar es una cierta fecha, la bomba se denomina temporal.
- Troyano: programa que no se replica ni hace copias de sí mismo. Su apariencia es la de un programa útil o inocente, pero en realidad tiene propósitos dañinos, como permitir intrusiones, borrar datos, etc.
- Gusano: es un programa similar a un virus que se diferencia de éste en su forma de realizar las infecciones. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos realizan copias de ellos mismos, infectan a otros ordenadores y se propagan automáticamente en una red independientemente de la acción humana

21 Aunque las "amenazas avanzadas" cada vez son más numerosas y difíciles de detectar, las organizaciones carecen de medios, tecnología y personal para abordarlas. Este es el principal hallazgo del estudio "*Growing Risk of Advanced Threats*" realizado por el Instituto Ponemon, para cuya elaboración encuestó a 591 trabajadores del ámbito de las TIC's y de la seguridad, asentados en los EEUU. Este informe define "amenaza avanzada" como "*una metodología empleada para evadir las medidas de protección de una compañía, con el fin de desencadenar una variedad de ataques con un objetivo concreto"*

22 Guía de seguridad de la Seguridad de las Tecnologías de Información (STIC) de la serie de Manuales del (CCN-STIC-401), Glosario y abreviaturas, 1 de febrero de 2010.

2. Tipos de atacantes

Los atacantes se pueden clasificar atendiendo a su motivación: como puede ser la búsqueda de un cambio social o político, un beneficio económico, político o militar, o satisfacer el propio ego; su objetivo: ya sean individuos, empresas, gobiernos, infraestructuras, sistemas y datos de tecnologías de la información, ya sean públicos o privados; el método empleado: código dañino, virus, gusanos, troyanos, etc.

Atendiendo a su autoría se pueden clasificar en:

- **Ataques patrocinados por Estados**: los conflictos del mundo físico o real tienen su continuación en el mundo virtual del ciberespacio. En los últimos años se han detectado ciberataques contra las infraestructuras críticas de países o contra objetivos muy concretos, pero igualmente estratégicos. El ejemplo más conocido es el ataque a parte del ciberespacio de Estonia en 2007, que supuso la inutilización temporal de muchas de las infraestructuras críticas del país báltico o los ciberataques sufridos por las redes clasificadas del gobierno estadounidense a manos de atacantes con base en territorio chino o el último ataque reconocido por Irán a los sistemas informáticos de decenas de industrias que fueron atacados por un virus antes de este verano[24] y del que Irán dice haberse recuperado[25]. Aquí también puede incluirse el espionaje industrial.
- **Servicios de inteligencia y contrainteligencia**: empleados por los Estados para realizar operación de información. Suelen disponer de bastantes medios tecnológicos y avanzados.
- **Terrorismo, extremismo político e ideológico**: los terroristas y grupos extremistas utilizan el ciberespacio para planificar sus acciones, publicitarlas y reclutar adeptos para ejecutarlas, así como herramienta de financiación. Estos grupos ya han reconocido la importancia estratégica y táctica del ciberespacio para sus intereses.
- **Ataques de delincuencia organizada**: las bandas de delincuencia organizada han comenzado a trasladar sus acciones al ciberespacio, explotando las posibilidades de anonimato que éste ofrece. Este tipo de bandas tienen como

23 En el informe de inteligencia de seguridad aparece España entre los países con más infecciones por malware del mundo detrás de Corea del Sur con 12,4 infecciones por cada 1.000 computadoras escaneadas). *Battling Botnets for Control of Computers*. SIR -Microsoft Security Intelligence Report, volume 9, January through June 2010

24 El Mundo: Irán reconoce un ataque informático masivo por el gusano Stuxnet contra sus sistemas industriales. Artículo publicado en la edición digital del diario El Mundo. Enlace http://www.elmundo.es/elmundo/2010/09/27/navegante/1285571297.html. (consulta: 27.9.2010)

25 *Revista Atenea*: Irán dice haber limpiado todos los ordenadores infectados por virus Stuxnet. http://www.revistatenea.es/RevistaAtenea/REVISTA/articulos/GestionNoticias_3060_ESP.asp. (Consulta: 4.10.2010)

objetivo la obtención de información sensible para su posterior uso fraudulento y conseguir grandes beneficios económicos[26].

• **Ataques de perfil bajo.** Este tipo de ataques son ejecutados, normalmente, por personas con conocimientos en Tecnologías de Información y Comunicación (TIC) que les permiten llevar a cabo ciberataques de naturaleza muy heterogénea y por motivación, fundamentalmente, personal.

En perfecta armonía con lo planeado, debe ser considerado el tema de los delitos. En el caso de Venezuela y quizás coincidiendo con otros Estados, se tiene, entre los más relevantes:

- Delitos contra la intimidad: delitos contra la intimidad y el derecho a la propia imagen (arts. 60 Constitución Nacional, en concordancia con la Ley especial contra Delitos Informáticos, Capítulo III, relativo a los delitos contra la privacidad de las personas y de las Comunicaciones). Asimismo, la ley expone el delito de pornografía y prostitución infantil con el uso de las TIC. (arts. 23 y 24).
- Delitos contra la propiedad: hurtos (art.13), fraude (art. 14) obtención indebida de bienes y servicios (art. 15), manejo fraudulento de tarjetas inteligentes e instrumentos análogos (art.16), delitos relativos a la propiedad intelectual (art.25), delitos relativos al mercado y a los consumidores (Capítulo V, relativo a los delitos contra el orden económico).
- Otras referencias indirectas: en relación con la utilización de medios o instrumentos informáticos, cabe señalar: Ley Orgánica de Telecomunicaciones, Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos. Ley sobre protección a la privacidad de las comunicaciones, entre las más afines a la problemática.

3. Iniciativas internacionales humanitarias frente a estas categorías de ataques y atacantes

Igualmente, desde una perspectiva humanitaria afirman Cossío, Martínez, Nuñez, Cesteros, Liñero, Becana y Martín (2013)[27]; es indudable que estas actuaciones, a las que se hizo referencia producen un daño indiscriminado, y son perseguidas porque pueden ser utilizadas en el curso de un conflicto bélico.

26 Según datos del *Federal Bureau of Investigation* (FBI), en 2009 el impacto de la ciberdelincuencia por la acción de bandas organizadas ocasionó unas pérdidas, tanto a empresas como a particulares estadounidenses, por un valor superior a 560 millones de dólares.

27 Cossío, Martínez, Nuñez, Cesteros, Liñero, Becana y Martín (2013) "Ciberseguridad: El nuevo reto del Siglo XXI". *Aspectos económicos de la ciberseguridad*. Grupo No. 1. 30 de mayo de 2013.Centro Superior de Estudios de la Defensa Nacional. (CESEDEN). España.

El Comité Internacional de la Cruz Roja, (en adelante, CICR)[28], ha abordado la cuestión de las amenazas cibernéticas en numerosos documentos. Entre ellos cabe mencionar el que contempla las cuestiones jurídicas que se plantean ante la posibilidad de que se conduzcan hostilidades en el ciberespacio.

En este sentido y de un análisis de los principios generales sobre "empleo de las armas", y a la luz de las normas 70 y 71 de la Compilación del Derecho Internacional Humanitario Consuetudinario se examinará su aplicación a los ciberataques.

La norma 70, establece que "*queda prohibido el empleo de medios y métodos de guerra de tal índole que causen males superfluos o sufrimientos innecesarios*".

En cuanto a los supuestos de ataque cibernético, con efectos económicos, en la mayoría de los casos tienen una duración limitada en el tiempo y pasado el momento de la agresión sus efectos no permanecen, es decir, no producen un efecto de devastación permanente. Puede decirse que si quedan constatados, entrarían dentro del concepto de "daño o destrucción", pues en todo caso producen perjuicios de carácter moral en la población.

Dada la definición que el propio Comité Internacional de la Cruz Roja ofrece sobre los medios y métodos de guerra de tal índole que causen males superfluos o sufrimientos innecesarios, nada impediría la aplicación de esta norma a aquellos ataques que, utilizando la red, fueran lanzados en un contexto como el señalado.

La norma 71 establece que "*queda prohibido el empleo de armas de tal índole que sus efectos sean indiscriminados*".

El Informe del CICR emitido tras la XXXI Conferencia Internacional de la Cruz Roja y de la Media Luna Roja, "El derecho internacional humanitario (DIH en adelante) y los desafíos de los conflictos armados contemporáneos", aclara que en el supuesto de que se propagara un virus o una serie de virus en los sistemas informáticos de un determinado Estado, elegido como objetivo, el DIH sería aplicable.

A juicio del Comité, no cabe duda de que estos virus podrían considerarse ataques indiscriminados de conformidad con el DIH vigente, toda vez que no pueden dirigirse contra un objetivo militar concreto y, por lo tanto, tendrían la consideración de un medio o método de combate cuyos efectos no pueden ser limitados, tal como lo exige el DIH.

Una cuestión particular que surge y que requiere atenta reflexión es si en la práctica es posible anticipar totalmente las consecuencias o los efectos secundarios que un ataque dirigido contra un objetivo militar legítimo pueda tener en la población civil y los objetos de carácter civil.

A juicio del CIRC, en este caso es necesario, igualmente respetar los principios de distinción y proporcionalidad lo que, a su vez, implica que es indispensable

28 Comité Internacional de la Cruz Roja. (CICR) Compilación del Derecho Internacional Humanitario. Consuetudinario. Norma 70 y 71.

tomar algunas precauciones en el ataque. Ello incluye la obligación de que el autor del ataque tome todas las precauciones factibles al seleccionar los medios y métodos de ataque con miras a evitar y, en cualquier caso a reducir al mínimo las víctimas y los daños civiles incidentales. Concluye el mencionado Informe que, puesto que en determinados casos las operaciones cibernéticas podrían causar un número menor de víctimas civiles incidentales y menos daños civiles incidentales, en comparación con los que ocasionan las armas convencionales, en ese caso y en tales circunstancias esta norma requeriría que un Alto Mando considerara la posibilidad de lograr la misma ventaja militar utilizando un medio y método de guerra que recurra al uso de la tecnología cibernética, en caso de que pudiera ponerse en práctica.

Otro esfuerzo en el ámbito internacional es el Convenio sobre Ciberdelincuencia[29], aprobado y abierto a la firma por el Plenario del Consejo de Ministros en Budapest, el 23 de noviembre de 2001. Este Convenio pretende armonizar la legislación de los diversos países que lo ratifiquen, no sólo en materia de derecho penal sustantivo, sino también de derecho procesal para hacer frente a ese tipo de delincuencia. El Convenio define los delitos informáticos agrupándolos en cuatro grupos:

a) ***Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos***. Engloba las conductas de acceso ilícito, interceptación ilícita, interferencia de datos, interferencia de sistemas y el abuso de dispositivos.

b) ***Delitos por su contenido***. Comprende las conductas que se engloban en los delitos relacionados con la tenencia y distribución de contenidos de pornografía infantil en la Red.

c) ***Delitos relacionados con la informática***. Se definen dos tipos penales, la falsificación informática y el fraude informático.

d) ***Delitos relacionados con las infracciones de la propiedad intelectual y de los derechos afines***. En este grupo, el Convenio hace una remisión normativa a los tratados y convenios internacionales sobre propiedad intelectual. En un Protocolo adicional al Convenio, de enero de 2003, se incluyeron las conductas de apología del racismo y la xenofobia a través de Internet, como delitos de contenido.

29 Consejo de Europa. Serie de Tratados Europeos No. 185. Convenio sobre Ciberdelincuencia, Budapest 23.XI.2001. El Convenio, hasta la fecha, sólo ha sido firmado por 46 países y ratificado por 30 estados firmantes. Se puede ver la lista actualizada de los países firmantes y los que lo han ratificado en http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=29/ (Consulta 2014, julio, 30)

Como puede observarse, es un catálogo de sucesos que pueden escenificarse en la red y hoy cuenta con la calificación de delitos y, por tanto ser objeto de sanción.

Salom (2013)[30], señala que la importancia del Convenio no está tanto en el número de países que lo han firmado y ratificado sino en que se ha constituido en el referente internacional a la hora de hablar de la delincuencia informática, y de aproximarnos a una legislación global.

En definitiva, los primeros escenarios de la delincuencia organizada se focalizaban en el fraude en el comercio electrónico y en la banca electrónica, como instrumentos más rápidos para obtener beneficios. Pero hoy, esas acciones delictivas pueden abarcar temas como la privacidad y la intimidad, configurando uno de los atentados mayores a los derechos humanos.

IV. Redes sociales y ciberseguridad en Venezuela

De acuerdo con los aspectos antes descritos en materia de ciberseguridad se observará el reto frente a la tensión que generan estas medidas a los derechos de los ciudadanos, algunos autores, en la materia entre ellos, Suñé (2013)[31] señala que en los tiempos actuales, en los que la sociedad se debate sobre los derechos y libertades de las personas en un mundo cada vez más global y estructurado con base a las nuevas tecnologías, se hace imprescindible que el mundo del Derecho haga su aportación en defensa de los mismos.

1. Marco legal relativo a la libertad de expresión e información

En el caso de Venezuela se puede decir que existe un marco legal encaminado a otorgar un orden a la actividad que se desarrolla por Internet, pero que peligrosamente debe mantener un equilibrio y proporcionalidad entre el derecho de los ciudadanos a estar informados y expresarse y el derecho del Estado a mantener en secreto algunas comunicaciones o regular de manera excesiva con base a algunas atribuciones. A continuación, se hará referencia a los documentos legales en la materia y con especial referencia a las telecomunicaciones y redes sociales, a saber:

30 SALOM (2011) "El Ciberespacio y el crimen organizado". *Ciberseguridad. Retos y Amenazas a la seguridad nacional en el ciberespacio Cuadernos de Estrategia.* Grupo No. 03/ 10.*Cap. III*. Ministerio de Defensa. Instituto español de estudios estratégicos. Instituto Universitario "General Gutiérrez Mellado". Febrero, 2011, pp.131-164

31 SUÑÉ, LLINAS, E (2013) "Hacia una Declaración de Derechos del Ciberespacio". http:/ /oiprodat.com/2013/06/24/hacia-una-declaracion-de-derechos-del-ciberespacio/ (Consulta 2014, julio, 30)

a) Constitución Nacional[32]

La máxima norma del país, consagra en su art. 48 el derecho al secreto e inviolabilidad de las comunicaciones. El art. 57 de la Carta Magna, consagra el derecho a la libertad de expresión y, el art. 58 establece el derecho a la información.

b) Ley Orgánica de Telecomunicaciones[33]

Esta ley tiene por objeto establecer el marco legal de regulación general de las telecomunicaciones, a *fin de garantizar el derecho humano de las personas a la comunicación* y a la realización de la actividad económica de telecomunicaciones necesarias para lograrlo, sin más limitaciones que las derivadas de la Constitución y las leyes…. (Art. 1) La ley también contempla en su art. 11 en concordancia con el art. 35, la creación de una Comisión Nacional de Telecomunicaciones[34], hoy CONATEL. En su Título II De los Derechos y Deberes de los Usuarios y Operadores, Capítulo I, contempla los derechos y deberes de los usuarios (Art. 12) y en su Capítulo II los derechos y deberes de los operadores (Art. 14). En su Título VI De los Recursos Limitados, Capítulo II Del Procedimiento para la Concesión de Uso y Explotación del Espectro Radioeléctrico (Arts. 76 al 78), serán estos los artículos a los que haremos alusión más adelante.

c) Ley de Responsabilidad social en Radio, Televisión y Medios electrónicos[35]

Esta ley tiene por objeto establecer, en la difusión y recepción de mensajes, la *responsabilidad social de los prestadores de los servicios de radio y*

32 Asamblea Nacional Constituyente. Constitución de la República Bolivariana de Venezuela. Gaceta Oficial Extraordinaria No. 5453. Caracas, 24 de marzo de 2000.

33 Comisión Legislativa Nacional Ley Orgánica de Telecomunicaciones. Gaceta Oficial No. 36.970, 12 de junio de 2000. Ediciones Babosan, C.A.

34 La Comisión Nacional de Telecomunicaciones (CONATEL), es un instituto autónomo, dotado de personalidad jurídica y patrimonio propio e independiente del Fisco Nacional, con autonomía técnica, financiera, organizativa y administrativa (Art. 35 de la Ley Orgánica de Telecomunicaciones). CONATEL es el organismo del Estado venezolano que ejerce la regulación, supervisión y control sobre las telecomunicaciones. La Ley Orgánica de Telecomunicaciones, promulgada el 12 de junio de 2000, otorgó las competencias estatales para la regulación del sector a CONATEL. Esta Comisión, inicialmente fue creada mediante el Decreto Nº 1.826 del 5 de septiembre de 1991 (Gaceta Oficial Nº 34.801 de fecha 18 de septiembre del mismo año) atribuyéndosele el carácter de servicio autónomo sin personalidad jurídica, y la jerarquía de una Dirección General del Ministerio de Transporte y Comunicaciones. Reemplazo al Consejo Nacional de Telecomunicaciones (CNT)

35 Asamblea Nacional. Ley de Responsabilidad social en radio, televisión y medios electrónicos. Gaceta Oficial 39579 de fecha 22 de diciembre de 2010.

televisión, proveedores de medios electrónicos, los anunciantes, los productores y productoras nacionales independientes y los usuarios y usuarias, *para fomentar* el equilibrio democrático entre sus deberes, derechos e intereses *a los fines de promover la justicia social y de contribuir a ….los derechos humanos,…."* Entre sus objetivos, el artículo 3, los refiere y en particular el objetivo 2 señala*: "Garantizar el respeto a la libertad de expresión e información, sin censura, dentro de los límites propios de un Estado Democrático y Social de Derecho y de Justicia y con las responsabilidades que acarrea el ejercicio de dicha libertad,….* y 5 *"Promover la difusión de producciones nacionales y producciones nacionales independientes y fomentar el desarrollo de la industria audiovisual nacional*". En su Capítulo VII Del Procedimiento Administrativo Sancionatorio, hace alusión a los sujetos sobre los cuales recae el mismo, solo señala: *"Se sancionará al prestador de servicios de radio, televisión o difusión por suscripción…"* (Art. 28) y el art. 29 ejusdem refiere a las sanciones de suspensión y revocatoria de los sujetos anteriormente indicados cuando a) promuevan, hagan apología o inciten a alteraciones del orden público y, b) promuevan, hagan apología o inciten al delito, entre otros actos.

d) Ley sobre Protección a la Privacidad de las Comunicaciones[36]

Esta ley fue publicada en la Gaceta Oficial No. 34.863, de fecha 16 de diciembre de 1991, tiene por objeto proteger la privacidad, confidencialidad, inviolabilidad y secreto de las comunicaciones que se produzcan entre dos o más personas (Art. 1). En concatenación con la Constitución Nacional que en su art. 48, que establece el derecho al secreto e inviolabilidad de las comunicaciones.

e) Providencia 01/09 de CONATEL, de fecha 22 de diciembre de 2009[37]

Norma técnica sobre los servicios de producción nacional audiovisual (sustituida por la actual providencia administrativa N° 027, publicada en la Gaceta Oficial N° 40.415, de 20 de mayo de 2014). Su objeto era desarrollar el régimen jurídico aplicable a los servicios de producción nacional audiovisual, de conformidad con la Ley de Responsabilidad Social en Radio y Televisión; en la vigente providencia Nº 027 el objeto de la misma se mantiene igual. En su

36 Congreso de la República de Venezuela. Ley Sobre Protección a la Privacidad de las Comunicaciones Gaceta Oficial de la República Bolivariana de Venezuela Nº 34863 de fecha 16 de Diciembre de 1991.

37 República Bolivariana de Venezuela. Directorio de Responsabilidad Social. Providencia Administrativa. 01/09. CONATEL Norma Técnica sobre los servicios de producción nacional audiovisual. 22 de diciembre de 2009.

artículo 3 se definía al servicio de producción nacional audiovisual[38]. En la actual providencia se mantiene la misma definición. Por su parte, el art. 5 de la providencia del año 2009, contemplaba lo relativo a las transmisiones de mensajes o alocuciones oficiales. En la actual providencia del año 2014, esto está contemplado en el art. 7 *ejusdem*[39]. Por su parte, la providencia 01/09 en sus artículos 7, 9 y 11, aludía al proceso de notificación del interesado para prestar el servicio a CONATEL, la calificación que CONATEL hace y el registro respectivo. En la providencia Nº 027, esto está establecido de igual manera en los artículos 4 y 5.

Finalmente, la nueva Providencia Administrativa 027 publicada en la Gaceta Oficial 40.415, del martes 20 de mayo de 2014, dictamina bajo la denominada "Norma Técnica" que los prestadores de servicios de producción nacional audiovisual deberán introducir dentro de su red de programación, bajo contrato previo, al menos 8% de servicios de producción audiovisual nacional en proporción al resto de canales ofrecidos (art. 9). Esta medida no estaba contemplada en la providencia 01/09, significando que pudiese ser aplicada esta norma con discrecionalidad y afectar la operación tanto de los canales de televisión por suscripción como a las empresas operadoras. Por esta razón, al igual que la providencia derogada (vigente frente a los hechos referenciados en esta investigación), la nueva providencia también se pudiese considerar contraria a los estándares de protección de la libertad de expresión, por configurar un uso abusivo del poder estatal, ante controles en telecomunicaciones arbitrarios que podrían restringir la libertad en la labor de algunos medios por suscripción.

2. Impacto de la ciberseguridad en el entorno digital en Venezuela

Una vez revisados los artículos de las leyes, incluida la Constitución Nacional, con mayor incidencia en la materia del derecho a la libertad de expresión e información, se hará una descripción de la vulnerabilidad de este derecho en

38 Se consideran como servicios de producción nacional audiovisual, a aquellos canales cuya recepción y/o difusión de imágenes y sonidos ocurran dentro del territorio de la República Bolivariana de Venezuela, y se difundan sólo a través de la red de un prestador del servicio de difusión por suscripción habilitado por la Comisión Nacional de Telecomunicaciones, con excepción, de al menos, uno de los siguientes supuestos:

1. Que el canal contenga en su programación semanal más del 70% de programas, publicidad o propaganda que, en su conjunto, no califiquen como producción nacional, de conformidad con lo establecido en el artículo 2 de la presente norma técnica.
2. Que el canal contenga en el tiempo total de su programación semanal más del 70% de programas, publicidad o propaganda que, en su conjunto, no califiquen como producción nacional, de conformidad con lo establecido en el artículo 2 de la presente norma técnica.

39 **Providencia Nº 027**. **Artículo 7 Transmisiones de mensajes o alocuciones oficiales**. "Los Servicios de Producción Nacional Audiovisual, deben transmitir gratuitamente los mensajes o alocuciones oficiales conforme a lo establecido en el artículo 10 de la Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos".

forma general y, en particular en el medio digital. Se seguirá para los fines correspondientes los dos Informes de PROVEA[40], correspondientes a enero-diciembre 2009[41] y, enero-diciembre 2013[42], sobre Derecho a la Libertad de Expresión e Información, con referencia a restricciones administrativas que se desprenden de las Providencias de CONATEL, en los últimos años y que se han aplicado bajo la excusa de la defensa de la patria. Estos informes servirán para evidenciar el impacto que el tema de la ciberseguridad en el país ha significado para los usuarios de los medios de información y comunicación y especialmente para los usuarios de las RSV.

Entre estas acciones se encuentran: las privativas de libertad que se dictaron como consecuencia de investigaciones penales iniciadas contra dirigentes políticos de oposición, dueños de medios y periodistas en virtud de su opinión política; la sentencia de censura previa que prohibió a todos los medios impresos del país publicar información sobre violencia durante un mes; la sentencia que condenó a un comunicador social en Valencia a prisión e inhabilitación profesional por un lapso de 3 años y medio por haber denunciado nepotismo en una alcaldía del Partido Socialista Unido de Venezuela (PSUV); los cierres temporales y definitivos de medios de comunicación privados, entre los cuales destaca la salida definitiva de RCTV (Radio Caracas Televisión) de la programación disponible en la televisión por suscripción; el aumento de detenciones arbitrarias por parte de funcionarios policiales para incautar material periodístico; y la creación del Centro de Estudio Situacional de la Nación y de las guerrillas comunicacionales, ambos órganos vigilantes de los intereses del Ejecutivo en la información que difunden los medios de comunicación privados. Desde octubre de 2009 hasta septiembre de 2010 se registraron 81 casos que implicaron 98 violaciones a la libertad de expresión. También durante este período, concretamente el 04 de agosto de 2010, CONATEL pasó a depender de la vicepresidencia de la República, con lo cual el Ejecutivo incumplió con el artículo 35 de la Ley Orgánica de Telecomunicaciones, antes indicado y le resta autonomía e independencia que por ley le corresponde.

Además, PROVEA en su informe de 2009, resalta que este ente ha aplicado una serie de restricciones administrativas, lo cual es otro elemento violatorio a los derechos de los ciudadanos. Las restricciones administrativas ocupan el 13,26% de los ataques a la libertad de expresión y han dejado fuera del aire

40 El Programa Venezolano de Educación-Acción en Derechos Humanos (PROVEA) es una organización no gubernamental (ONG) independiente venezolana dedicada a analizar la situación de los derechos humanos en Venezuela y a la promoción y defensa de los mismos. El trabajo de la organización, se resume en un informe anual que publica y distribuye a entidades públicas y privadas, nacionales e internacionales

41 PROVEA Informe Anual enero-diciembre 2009. Derecho a la Libertad de Expresión e Información

42 PROVEA Informe Anual enero-diciembre 2013. Derecho a la Libertad de Expresión e Información

definitivamente: un canal de televisión privado con señal abierta, un canal de televisión por suscripción y una radio comunitaria. También, cinco canales de televisión por suscripción, cuatro emisoras de radio y dos periódicos regionales fueron cerrados temporalmente; y una radio privada se vio afectada con la reducción significativa de su ámbito de transmisión. Esto como consecuencia, de la aplicación de la Providencia Administrativa de CONATEL, antes referida, que da un control excesivo al Estado sobre los servicios de programación nacional. Con relación a estas acciones administrativas hasta la fecha no ha habido pronunciamiento del Tribunal Supremo de Justicia (TSJ) sobre el fondo en los procedimientos administrativos adelantados por CONATEL contra emisoras y canales de televisión.

En este mismo sentido, cabe resaltar la creación por parte del Presidente venezolano, del Centro Estratégico de Seguridad y Protección de la Patria (CESPPA), cuyo presidente pasó a tener muy amplias facultades ya que podrá "*declarar el carácter de reservada, clasificada o de divulgación limitada, cualesquiera información, hecho o circunstancia que en cumplimiento de sus funciones tenga conocimiento*". Lo cual atenta y viola lo consagrado en la Constitución y las leyes en la materia (arts. 47,57 y 58, de la Constitución)

Ahora bien en el tema de los medios digitales, es de resaltar que el Informe de PROVEA 2013, señala que el 63,8% de los medios afectados (periódicos, radios, televisoras y medios digitales) resultaron de carácter privado, como ha sido una tendencia clara de los últimos años. Al desagregar por sectores específicos, la gran novedad de este 2013 ha sido la aparición de un sector como lo es "proveedores de Internet", para dar cuenta de las limitaciones impuestas por CONATEL contra los principales proveedores de Internet del país, con la finalidad de restringir información que el gobierno consideró ilegal (caso de la "caída" de las páginas que informaban sobre la tasa del dólar negro). El 10 de noviembre de 2013, el Presidente Nicolás Maduro le ordenó a CONATEL bloquear las páginas de Internet que difundían las cotizaciones del llamado dólar paralelo, en el marco de lo que el gobierno denominó "la guerra económica". Esta acción de censura fue seguida de la apertura de un inédito proceso administrativo sancionatorio contra ocho empresas proveedoras del servicio de Internet por tener alojadas dichas páginas o políticamente inoportuna, (suspensión de sitios con información que revelaban la gravedad en el estado de salud del Presidente Chávez).

Otro caso fue el de la jueza María Lourdes Afiuni, quien quedó obligada a presentarse cada 15 días al tribunal y no salir del país, ambas son medidas tradicionales; pero además se le impuso la prohibición de comunicarse por la red social Twitter, en la cual contaba con más de 250 mil seguidores.

De igual manera, la web también ha sido la herramienta de los medios y periodistas que han salido del aire por las presiones gubernamentales. Un caso emblemático es el de Alberto Federico Ravell, quien después de ser obligado a dejar la dirección editorial de Globovisión abrió el sitio web www.lapatilla.com.

Luego de su salida de la programación de televisión por suscripción, RCTV Internacional también transmite su noticiero a través de la web. Los portales de noticias han adquirido popularidad por la misma razón que explica el crecimiento de los usuarios del *Twitter*: muchos de estos ofrecen la posibilidad a sus lectores de comentar y/o agregar información.

En Venezuela son seguidos por muchos usuarios los noticieros web Noticiero Digital y Noticias 24, que recogen opiniones sobre el desempeño del gobierno como de la oposición. El Ejecutivo Nacional y la Asamblea Nacional han seguido de cerca la información producida en los medios de comunicación digital y en el último año solicitaron en dos oportunidades al Ministerio Público que investigara a los dueños de estas páginas, entre ellas a quienes conducen Noticiero Digital. Gracias a la providencia de CONATEL 01/09, antes indicada, ahora estos son servicios de producción nacional y como tales se les ha aplicado algunas restricciones pues lo somete a una regulación que implica más que regulación control y autocensura, en lo relativo a las transmisiones de mensajes o alocuciones oficiales, estos servicios deben transmitir las cadenas oficiales, para su legalidad deben llevar a cabo el proceso de notificación del interesado para prestar el servicio a CONATEL, luego esperar la calificación que debe hacer CONATEL y el registro respectivo, de acuerdo a los artículos antes referidos de esta providencia.

En perfecta armonía con lo planteado, desde el año 2010, en el país se tiene como antecedentes la detención de personas por difundir mensajes en las redes sociales. En ese año fueron aprehendidas dos personas por críticas al sistema bancario vía Twitter. Posteriormente, un ingeniero de CORPOELEC[43] corrió la misma suerte por comentarios en la red que, a juicio del CICPC[44], "incitaban al magnicidio". Todo de acuerdo con lo planteado en la Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos, en su artículo 29, letras a y b, como se hiciera referencia antes. En marzo de 2013, una mujer de 53 años fue privada de libertad por presuntamente "descubrírsele algunos mensajes desestabilizadores". Luego, en abril, un joven fue acusado de difundir un video en YouTube en el que aparecía el entonces Ministro de Hábitat, Ricardo Molina, amenazando a empleados que apoyaban al candidato presidencial Henrique Capriles.

En este sentido, se puede agregar que CONATEL hizo un exhorto para castigar a los medios que hicieran apología de la violencia en la cobertura de las

43 Empresa Eléctrica Socialista, adscrita al Ministerio del Poder Popular de Energía Eléctrica, es una institución que nace con la visión de reorganizar y unificar el sector eléctrico venezolano a fin de garantizar la prestación de un servicio eléctrico confiable, incluyente y con sentido social.

44 El Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), antes conocido como Cuerpo Técnico de Policía Judicial (CTPJ) y en sus orígenes como Policía Técnica Judicial (PTJ), es el principal organismo de investigaciones penales de Venezuela. Se encarga del esclarecimiento científico de los delitos con miras a la posterior aplicación de la justicia por los órganos competente

protestas desarrolladas en el país a partir del mes de febrero de 2014, incluyendo por primera vez a las páginas de Internet. (De Abasolo, 2014)[45]. Esto otra vez con base a las sanciones contempladas en la Ley sobre Responsabilidad Social en Radio, Televisión y Medios Electrónicos.

Stelling (2014)[46], experta socióloga en materia de comunicación social, define la medida impulsada por CONATEL sobre la cobertura de protestas como *"una línea muy débil entre el exhorto y la censura"*. Considera que desde hace tiempo las redes sociales están en el ojo del huracán debido a que generan una suerte de normas propias. No obstante, califica de "peligroso" cualquier intento de control mediante amenazas. *"Eso podría convertirse en un error grande para el gobierno porque avalaría esas acusaciones de totalitarismo, violación de los derechos humanos y ataque a la libertad de expresión que tanto denuncian internacionalmente"*.

La experta resalta que las redes sociales "*tienen un altísimo nivel de penetración en Venezuela*", y se han convertido en un canal de información, estimulación y hasta de provocación entre un sector y otro. Lo define como una ventana vital para el ciudadano y hasta para el mismo gobierno que estratégicamente ha apelado a su uso para conectarse con sus seguidores. *"La mejor manera de abordar a los medios de comunicación es con responsabilidad y compromiso, pero sin presiones*". (De Abasolo, 2014)[47].

Por su parte, Carlos Correa, Director de la organización no gubernamental "Espacio Público", señala que el llamado de CONATEL pretende "*generar autocensura e inhibición"* en los medios de comunicación, lo que a su vez, se extiende a la interacción de las redes. "Hay consciencia de la importancia de estas redes; tanto, que existe *un viceministerio. Al reducirse los espacios la gente busca opciones y éstas se han convertido en las más importantes"*. (De Abasolo, 2014)[48].

Correa cree que atentar contra las redes sociales es complicado, no solo porque el gobierno también hace uso de éstas, sino porque tales sistemas tienen mecanismos que permiten burlar cualquier tipo de censura. A su juicio, el control no solo atentaría contra la Constitución sino que generaría más incertidumbre en una población que se mantiene en la constante búsqueda de espacios de

45 De Abasolo, 2014. "Controlar las redes sociales sería un "error" del gobierno". http://www.hinterlaces.com/sin-categoria/controlar-las-redes-sociales-seria-un-error-del-gobierno (Consulta 2014, Julio, 30)

46 De Abasolo, 2014. "Controlar las redes sociales sería un "error" del gobierno". http://www.hinterlaces.com/sin-categoria/controlar-las-redes-sociales-seria-un-error-del-gobierno (Consulta 2014, Julio, 30)

47 De Abasolo, 2014. "Controlar las redes sociales sería un "error" del gobierno". http://www.hinterlaces.com/sin-categoria/controlar-las-redes-sociales-seria-un-error-del-gobierno (Consulta 2014, Julio, 30)

48 De Abasolo, 2014. "Controlar las redes sociales sería un "error" del gobierno". http://www.hinterlaces.com/sin-categoria/controlar-las-redes-sociales-seria-un-error-del-gobierno (Consulta 2014, Julio, 30)

expresión *"debido a la censura y autocensura que ya ha sido impuesta en los medios tradicionales"* (De Abasolo, 2014)[49].

Por ello, se ha observado que en el país durante estos últimos años de conflictividad social, se han desarrollado una serie de eventos, que merecen ser objeto de estudio, frente a la evidente vulnerabilidad de algunos derechos fundamentales que ahora se extiende a los sitios web y RSV.

V. Algunas consideraciones finales

En consecuencia a lo expuesto, hoy tiene mucho más sentido el documento sobre la Declaración de Derechos del Ciberespacio, en el cual se expresa el derecho a la protección de los datos personales y al secreto de las telecomunicaciones, la regulación de derechos y obligaciones, de la fiscalidad (regulando las transacciones, cada vez más comunes, que se realizan por este medio), la elaboración de una normativa global penal (encaminada a perseguir, de forma efectiva, aquellos delitos que superar la estructura, física y política, de los Estados), un desarrollo coherente de la propiedad intelectual, y el amparo de los derechos fundamentales inherentes a la persona. Señala Suñé (2008)[50]:

> *…En esencia, los mecanismos de dominación y de limitación de los derechos humanos en este nuevo espacio de información o ciberespacio tienen más que ver con la limitación del acceso a las condiciones necesarias (ya sean técnicas, económicas o culturales) que permitirían el desarrollo de formas más avanzadas de participación pública y de intercambio y libre expresión de ideas y creencias…..".*

Por su parte, son variadas las formas de ataque y los atacantes en el medio digital, frente a ello los Estados, desde los más conservadores o de izquierda hasta los más modernos o de democracias representativas, buscan evitar daños a sus ciudadanos y bienes, no obstante las acciones de Estado en la mayoría de las ocasiones violentan los derechos humanos de quienes quieren expresarse y estar informados. Por otro lado, es peligroso dejar de tomar medidas frente a los posibles ataques en la red, que pueden significar verdaderas amenazas no sólo para los Estados en sí mismos sino para la humanidad. Es necesario pues encontrar un acuerdo que armonice y otorgue proporcionalidad, tanto por una parte, al derecho de los Estados y organizaciones a protegerse frente a los ciberataques, pero por otro lado, reconocer y respetar el derecho ciudadano y humano a expresarse e informarse por medios lícitos, creándose foros de

49 De Abasolo, 2014. "Controlar las redes sociales sería un "error" del gobierno". http://www.hinterlaces.com/sin-categoria/controlar-las-redes-sociales-seria-un-error-del-gobierno (Consulta 2014, Julio, 30)

50 Suñé Llinás, E. (2008). La ausencia de privacidad en Internet: Hacia una Constitución y Declaración de Derechos del Ciberespacio. *Contrastes*, 50. Págs. 66 ss.

participación multidisciplinarios donde tanto los entes gubernamentales, como organizaciones internacionales y la sociedad organizada puedan conformar planes estratégicos de defensa sin menoscabo de los derechos ciudadanos.

¿La libertad de programación afectada? Análisis de la Norma Técnica sobre Producción Nacional Audiovisual del Consejo de Responsabilidad Social

Miguel Arrieta Zinguer*

SUMARIO: I. Introducción. II. Libertades comunicacionales. III. Los servicios audiovisuales. IV. Necesidad de regulación y libertad de programación. V. La Norma sobre los Servicios de Producción Nacional Audiovisual. VI. Conclusiones.

Resumen

El derecho a la libertad de programación es considerado como una manifestación de la libertad de expresión y del derecho a la información. En Venezuela recientemente se aprobó una Norma Técnica Sobre los Servicios de Producción Nacional Audiovisual, donde se establecen los requisitos para prestar los servicios de producción televisiva, aplicable a los operadores de televisión por suscripción, bien sea por cable o por servicios satelitales. En el presente artículo se analiza la pertinencia de esta norma, así como su consideración dentro de la libertad de programación de las empresas de televisión por suscripción y su papel en el ejercicio de la libertad de expresión.

Palabras clave: Producción nacional audiovisual. Libertad de expresión. Derecho a la información. Servicios de difusión por suscripción.

Abstract

Freedom of programming on television is considered a form of freedom of speech, and of right to information. In Venezuela, a law was recently approved with regards to Technical Standards on Domestic Audiovisual Services Production, where the

Recibido: 10/10/2014 • Aceptado: 25/10/2014

* Profesor Titular de la Universidad Católica del Táchira. Magíster en Gerencia de Empresas (Universidad Nacional Experimental del Táchira), Especialista en Derecho Mercantil (Universidad de Carabobo), Especialista en Derecho Tributario (Universidad Católica del Táchira), Doctorando en Ciencias, Mención Derecho (Universidad Central de Venezuela). Asesor Gerencial.

requirements to provide television production services are established. This law applies to subscription television operators, either by cable or satellite services. In this paper the relevance of this standard, its considerations within the freedom of programming of cable TV companies, and their role in the freedom of speech are analyzed.

Keywords: Domestic Audiovisual Production. Freedom of Speech. Right to information. Cable Television Services.

I. Introducción

En fecha 07 de Marzo de 2014, el Directorio de Responsabilidad Social en Radio y Televisión, emitió la Norma Técnica Sobre los Servicios de Producción Nacional Audiovisual y otros Servicios de Producción Audiovisual (Providencia Administrativa N° 027, publicada en la Gaceta Oficial N° 40.415, de fecha 20 de mayo de 2014), que establece el régimen jurídico aplicable a la producción audiovisual en Venezuela, de conformidad con lo establecido en la Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos (en lo sucesivo LRSRTVME), lo cual implica que para poder prestar tal tipo de servicios en Venezuela, se requiere cumplir con los requisitos y condiciones establecidos en la normativa señalada, que por lo demás, deroga la anterior norma, establecida en la Providencia N° 01-09 de dicho Directorio, que databa de fecha 22 de Diciembre de 2009 (publicada en Gaceta Oficial N° 39.333, de igual fecha). La norma en cuestión, resulta a todas luces polémica por cuanto se estima que afecta la libertad de programación de las empresas prestadoras de servicios de televisión por suscripción, al establecer estrictas normas para la prestación de tales tipos de servicios, al tiempo que establece potestades discrecionales en cuanto a la posibilidad de otorgar o no el permiso para colocar determinadas señales de ciertos canales, y en cuanto a la posibilidad correlativa de revocar sin más dicha autorización.

De conformidad con la Norma Técnica en cuestión (en lo sucesivo NTSPNA), las personas que deseen prestar servicios de producción nacional audiovisual tienen la obligación de calificar tanto los programas, como la publicidad o propaganda a ser difundidos a través de dichos servicios y que constituyan producción nacional de acuerdo a las disposiciones de la Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos (LRSRTVME) y la presente Norma Técnica. A tales fines, deben elaborar una ficha técnica que contenga información que evidencie la referida calificación, la cual debe presentarse ante la Comisión Nacional de Telecomunicaciones (CONATEL) conjuntamente con la solicitud de obtención del permiso al que hace referencia el artículo anterior.

II. Libertades comunicacionales

Esta normativa, ciertamente polémica, toca aspectos vinculados con el ejercicio de las libertades comunicativas y particularmente con el derecho a la comunicación, consagrado en el artículo 58 de la Constitución de la República Bolivariana de Venezuela, en su artículo 58, en los siguientes términos:

> La comunicación es libre y plural y comporta los deberes y responsabilidades que indique la ley. Toda persona tiene derecho a la información oportuna, veraz e imparcial, sin censura, de acuerdo con los principios de esta Constitución, así como a la réplica y rectificación cuando se vea afectada directamente por informaciones inexactas o agraviantes. Los niños, niñas y adolescentes tienen derecho a recibir información adecuada para su desarrollo integral.

Como puede apreciarse, el derecho a la comunicación, conforme el régimen constitucional venezolano, constituye una amplia vinculación con la libertad de expresión, que a su vez está al derecho a la información, la cual implica la prohibición de censura, en general; no obstante el derecho de informar implica las responsabilidades ulteriores que pudiesen generarse en caso de emitirse informaciones que generen perjuicios morales, o que resulten inexactas. Por otra parte, se establece el derecho de los menores de edad a recibir informaciones adecuadas. Este marco conceptual ha sido desarrollado ampliamente a nivel normativo en los últimos años, por cuanto la LOTEL establece el desarrollo del derecho a la comunicación, cuando ésta se expresa mediante la utilización de elementos radioeléctricos, electromagnéticos, etc.; además el derecho a que la comunicación sea libre y plural, se manifiesta en la posibilidad de establecer radioemisoras y televisoras comunitarias de servicio público, sin fines de lucro, que dicha norma establece. La responsabilidad que se deriva del ejercicio de la labor comunicativa e informativa también está regulada por la Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos, que establece las normas, límites y sanciones a las personas que se dedican a la labor informativa y comunicativa, cuando realizan dichas actividades a través de medios radioeléctricos (radio y televisión de señal abierta, servicios de difusión por suscripción y medios electrónicos).

Hoy en día, el ejercicio de la comunicación, comprende tanto la expresión escrita, como oral e incluso telecomunicacional, por cuanto el desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC), ha permitido el advenimiento de nuevos medios para el ejercicio de este derecho humano fundamental, particularmente a partir del desarrollo intenso que han tenido en las últimas décadas, las telecomunicaciones. Las telecomunicaciones se refieren precisamente a los nuevos medios para el ejercicio del derecho de la

comunicación[1]. No obstante, esta consideración ha venido modificándose con el advenimiento de los medios radioeléctricos y como consecuencia de la aparición de la televisión por cable, que ha modificado sustancialmente los hábitos de consumo televisivo desde hace 25 años, ya que determina una mayor oferta de canales, que por lo demás son especializados, temáticos 'a la carta', lo cual permite al telespectador escoger dentro de una oferta cada vez más amplia, y que desestima la tradicional importancia de los canales de señal abierta, por la conformación de una programación, adaptada a las preferencias y gustos personales de cada televidente.

Las transformaciones que se han venido produciendo en los medios de comunicación, como consecuencia de las modificaciones y evoluciones que han tenido el desarrollo e interacción de nuevas tecnologías de la comunicación, así como de la convergencia tecnológica entre los medios, y particularmente por la irrupción de las tecnologías de redes abiertas, han traído como consecuencia que los distintos medios tengan la necesidad de transformarse. Así, los periódicos, que originalmente solo se imprimían sobre soporte papel, comenzaron a integrarse a Internet, generando una nueva consideración acerca de su valor e importancia, dada la nueva estimación del poder multimediático que ofrece Internet; de manera que se genera un nuevo medio interactivo, que no solo es un periódico en la red, sino que precisa la constitución de valores agregados capaces de atraer y mantener el interés del público consumidor. Estas consideraciones no sólo se aplican a los medios impresos en su interacción con Internet, sino a todos los demás, incluso los televisivos y radiales, puesto que las TIC (particularmente en cuanto al desarrollo de los estándares de televisión digital y radio digital), cambian profundamente la conformación de dichos medios de comunicación. La convergencia de estos medios a Internet permite la ampliación significativa del volumen de medios de cualquier parte del mundo a los que el público sediento de información, puede acceder desde la comodidad de sus casas, con un simple dispositivo que le brinde acceso a Internet. De allí que la consideración del poder mediático, deberá tener a su vez una imbricación global, a mi manera de ver indetenible.

Ahora bien, en cuanto al papel de los medios de comunicación en la actualidad, desde una perspectiva social y política, Benido, A.[2], estima que:

> Los medios tienen una función social y política, pues no son sino un poder en una red de poderes que se controlan y contrapesan mutuamente. El primer rol

1 Así lo establece en su artículo 1°: "*Esta Ley tiene por objeto establecer el marco legal de regulación general de las telecomunicaciones, a fin de garantizar el derecho humano de las personas a la comunicación y a la realización de las actividades económicas de telecomunicaciones necesarias para lograrlo, sin más limitaciones que las derivadas de la Constitución y las leyes…*"

2 BENIDO, Angel (1989) *Ecología de la Comunicación de Masas*. Eudema. Madrid. P. 181.

> es la recogida y presentación de información objetiva, tiene su propia objetividad que queda absolutamente subjetivizada, en realidad lo que se trata de evitar es la parcialidad, es decir, la manipulación deliberada en el contenido y presentación de las noticias con el propósito de promover la causa de un determinado partido….la segunda es la interpretación y explicación de las informaciones, teniendo en cuenta que se debe tender a que las informaciones sean comprendidas y por los sectores menos expertos, y que dentro del el caben una serie de géneros periodísticos. Una tercera función es la de contribuir a la formación de la opinión pública, pues los medios llaman la atención tanto del público como del gobierno acerca del clima de opinión imperante y supuesto el papel básico de la opinión pública en una sociedad democrática. También es importante la formación de una agenda política, por último la función del control de gobierno. Si no se ponen las bases para un equilibrio generalizado en el mundo de la comunicación, para una estructura ecológica de los medios, en su distribución, en su propiedad, en sus contenidos y en su control verdaderamente social, la comunicación llegará a ser un instrumento de dominación.

Como puede apreciarse, las funciones que los medios de comunicación cumplen dentro de la sociedad en la actualidad son trascendentes desde el punto de vista de la obtención de la información relevante sobre los hechos y noticias que ocurren dentro de la sociedad, así como para la interpretación y decodificación de la información, de manera que la sociedad pueda acceder a la inteligencia de dicha información, y en definitiva poseen un rol esencial en la formación de la opinión pública.

El derecho a la información se ha convertido en un derecho inalienable que corresponde a cualquier ciudadano, que forma parte de los derechos civiles y políticos en cualquier parte del mundo (aunque existe la tendencia, por parte de algunas organizaciones, con la UNESCO a la cabeza, que lo ubican dentro de los derechos culturales). El derecho a la información constituye por tanto, un pilar de la convivencia democrática, y al tiempo un derecho fundamental del individuo. Ha sido calificado como un derecho humano de primera generación, vale decir, los derechos civiles y políticos, que tienen por finalidad la protección de la libertad, integridad física y moral de los seres humanos.

Este derecho comprende un conjunto de derechos y facultades que varían en su consideración y contenido, en general se considera que está integrado básicamente por tres facultades: investigar, recibir y difundir mensajes informativos; de los que la facultad de recibir implica la obtención y recepción de información, de acuerdo con sus propios intereses, mientras que la facultad de investigar la poseen tanto los profesionales de la información como el público y le permite acceder a las fuentes de la información y opinión, sin limitaciones, siendo un deber permitir este acceso para quienes manejan las fuentes de información.

Nogueira-Alcalá, H.[3], estima que el derecho a la información es un complejo de derechos que guardan relación, tanto con respecto al que informa (informador), como a quien percibe la información (informado), difiriendo en cada caso en cuanto a los derechos que lo conforman, así:

a) En relación con el informador. Se encuentran los derechos, a: i) investigar y buscar informaciones y opiniones[4]; ii) difundir informaciones de relevancia pública por cualquier medio y opiniones; iii) emitir informaciones u opiniones[5]; iv) no ser censurado[6], ni objeto de

3 Nogueira, H. (2000) *El Derecho a la información en el ámbito del Derecho constitucional comparado en Iberoamérica y Estados Unidos*. Publicado en "El Derecho a la Información y Derechos Humanos" Jorge Carpizo y Miguel Carbonell (coords.) [Libro en línea] Universidad Nacional Autónonma de México. México. Disponible en: http://www.bibliojuridica.org/libros/1/7/3.pdf [Consulta: 2013, abril 25]. Pp. 21-22.

4 En la obtención de la información, el profesional de la información (periodista, reportero), o persona normal, tiene derecho de realizar los contactos, entrevistas, que estime convenientes, con la condición de que dicha información vaya dirigida al público. Según Escobar de la Serna, L. (1998) *Derecho de la información***.** Editorial Dykinson. Madrid. P. 57., debe entenderse como: "*…la facultad atribuida a los profesionales de la información, a los medios informativos en general y al público, de acceder directamente a las fuentes de las informaciones y de las opiniones y de obtener éstas sin límite general alguno, facultad que debe considerarse en su doble faceta, es decir, como derecho del ciudadano y como deber de los que manejan las fuentes de información*".

5 La garantía que permite la existencia de información verdaderamente libre, precisa que la legislación del país de que se trate garantice la confidencialidad de la fuente y el secreto profesional del periodista; el cual se debe acompañar de una normativa profesional adecuada en cuanto a la ética profesional, así como un manejo legítimo de la información, de tal suerte que no afecte ilegítimamente la honra o reputación de las personas. La libre difusión de las ideas, tiene como límite la confidencialidad para las personas naturales o jurídicas.

6 Con respecto a la prohibición de censura, conviene precisar que el artículo 13.2 de la Ley Aprobatoria de la Convención Americana de Derechos Humanos, establece límites a la libertad de expresión o de pensamiento, contemplando responsabilidades ulteriores a la expresión que comprenden específicamente que el ejercicio del derecho a la libertad de expresión: "*…no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar: a) el respeto a los derechos o a la reputación de los demás, o b) la protección de la seguridad nacional, el orden público o la salud o la moral pública. 3. No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones. 4. Los espectáculos públicos pueden ser sometidos por la ley a censura previa con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia, sin perjuicio de lo establecido en el inciso 2. 5. Estará prohibida por la ley toda propaganda a favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma o origen nacional*". Por su parte, el Tribunal Supremo de Justicia de Venezuela, en Sala Constitucional, en su sentencia N° 1942, pareciera legitimar la posibilidad de la censura previa, en ciertas ocasiones, al establecer lo siguiente: "*A juicio de esta Sala, el artículo 13.2 colide en cierta forma con el artículo 57 constitucional. Este prohíbe la censura a las expresiones que se difundirán por los medios de comunicación o difusión, lo que es coincidente*

> restricciones preventivas en forma explícita o implícita, directa o indirecta, a excepción de medidas destinadas a proteger la moral de los menores o adolescentes, o en casos de estados de excepción constitucional; v) acceso a las fuentes de información[7]; vi) secreto profesional periodístico y a la reserva de las fuentes[8]; vii) la cláusula de conciencia[9]; viii) el acceso y utilización de los instrumentos y medios naturales o tecnológicos necesarios que permitan emitir las opiniones e informaciones.

con la letra del artículo 13.2 comentado, pero el artículo 57 constitucional no permite el anonimato, ni la propaganda de guerra, ni los mensajes discriminatorios, ni los que promuevan la intolerancia religiosa, sin diferenciar, al no prohibirla, en qué oportunidad se impedirá su difusión. Como el artículo 58 constitucional se refiere a la comunicación de la expresión e información "*sin censura, de acuerdo a los principios de esta Constitución*"*, la Sala interpreta que en materia comunicacional y por aplicación de otros principios constitucionales, la ley puede impedir la difusión de informaciones que dejen sin contenidos otras normas constitucionales o los principios que rigen la Carta Fundamental. A juicio de la Sala, ello puede tener lugar aun antes de que los medios de comunicación lo hagan conocer, ya que, de no ser así, el efecto nocivo, que reconoce la norma constitucional y que trata de impedir, tendría lugar irremisiblemente... Para que no se permitan tales expresiones, la ley puede crear censura previa a su difusión o comunicación, siempre que actos jurisdiccionales la ordenen. Sin embargo, las prohibiciones del artículo 57 constitucional son en parte distintas de aquellas que el artículo 13 de la Convención Americana sobre Derechos Humanos contempla, las cuales nunca pueden ser objeto de censura anterior a su difusión o comunicación, pero que sí generan responsabilidades (de acuerdo con lo que establece la ley) a quien las exprese en cualquier forma. Apunta la Sala que son en parte distintas, ya que hay supuestos contemplado2s en ambas normas, las cuales al ser diferentes, otorgan efectos distintos a los supuestos coincidentes.*

7 Esto determina la obligación para los Estados de no efectuar actuaciones destinadas a evitar o limitar la libre recepción de la información de carácter público, así como promover condiciones que permitan el libre ejercicio de la obtención de la información, de modo que el ordenamiento jurídico debe establecer la obligación que las autoridades gubernamentales de entregar la información sobre todo asunto público de relevancia para la población, con excepción de la información reservada por ley.

8 El derecho al acceso a la información pública supone el derecho de inquirir acerca del origen de los datos almacenados, por lo que cobra relevancia respecto de la reserva respecto de la fuente de información, que se puede utilizar para limitar la facultad indagatoria, a la que se contrapone también la negativa de informar en determinados casos, fundada en el deber de secreto acerca de la fuente de información, que comprende uno de los elementos fundamentales dentro del secreto profesional, propio del ejercicio de la función de periodista. De hecho el secreto profesional del periodista se concibe como un derecho subjetivo de naturaleza pública que integra la libertad institucional de la prensa. Entonces queda claro que las fuentes de información de los periodistas son secretas por mandato constitucional (artículo 28 de la Carta Fundamental venezolana) y legal (artículo 8 de la Ley de Ejercicio del Periodismo). En consecuencia, cualquier tipo de exceso por parte de los periodistas que atente contra el derecho de los demás y contra el artículo 58 constitucional, generarían responsabilidades legales de los editores o de quienes los publican, al no tener la víctima acceso a la fuente de la noticia que lo agravia. Pero además de estas acciones, y sin que sean excluyentes, las personas tienen el derecho de réplica y rectificación cuando se vean afectados por informaciones inexactas o agraviantes.

9 La cláusula de conciencia, se encuentra representada por aquellas cláusulas legales que se consideran implícitas en los contratos de trabajo con los periodistas, conforme la cual, en los supuestos en que la ley tipifica en relación con la conciencia del informador, los efectos económicos

b) **Por lo que respecta al informado**. Comprende los derechos a: i) recibir opiniones e informaciones; ii) seleccionar la información que recibe y los medios a través de la cual recibirla; iii) ser informado veraz y oportunamente; iv) que sea preservada su honra y vida privada; v) rectificación o respuesta[10]; vi) solicitar la imposición judicial de responsabilidades civiles y penales en los casos determinados por el ordenamiento jurídico.

De manera que el derecho a la información, se reputa como un 'derecho de doble vía'[11], en el sentido de poseer esa doble vertiente de recibir y dar información, pero está claro que su núcleo operacional está representado por la posibilidad de buscar, recibir y difundir información, que según Urbina Serjant, J.[12] constituye 'el derecho genérico a la libertad de información'. De manera que todo ser humano tiene el derecho, tanto de manera individual como colectiva, de buscar información para obtener un conocimiento cabal de los hechos, ideas y sucesos que le atañen, con el objeto de poder formar con verdadera libertad su opinión, con respecto a los aspectos que le atañen; pero también a recibir la información que resulte relevante para tomar posición sobre los asuntos que le afecten.

de la extinción de la relación laboral periodística producidos por voluntad unilateral del trabajador, equivalen a los de despido por voluntad del empleador. De modo que la cláusula de conciencia busca salvaguardar la libertad ideológica, el derecho a expresar libremente la opinión y la ética profesional del periodista, concebida como parte de la libertad de expresión, como elemento conformante del derecho a la información.

10 En cuanto al derecho a la réplica corresponde únicamente a las personas que son agraviadas o afectadas por informaciones incorrectas, mas no corresponde a los periodistas o medios de comunicación; en efecto, la Sentencia 1013 del Tribunal Supremo de Justicia de Venezuela, ha sentado que: "*… el derecho a la réplica y a la rectificación no lo tienen ni los medios, ni quienes habitualmente ejercen en ellos el periodismo, ni quienes mantienen en ellos columnas o programas, ni quienes mediante «remitidos» suscitan una reacción en contra. Se trata de un derecho concedido a quienes se ven afectados por la información de los medios, y que carecen de canales públicos para contestar o dar su versión de la noticia. Quien publica un remitido en un medio, si un interesado le contesta en otro medio, no puede pretender (quien publicó el primero) le den gratis un espacio en el segundo medio para contrareplicar, ya que los remitidos no forman parte del periodismo de información al cual se refiere el artículo 58 comentado; pero tampoco pueden los periodistas, directores y editores de medios de comunicación, pretender que en otro medio se le permita responder lo que en el se haya difundido y consideren los perjudica, ya que estarían utilizando innecesariamente un espacio, cuando muy bien ellos, utilizando sus canales de difusión escritos, orales o audiovisuales, pueden hacerlo*".

11 Así lo ha declarado la Corte Constitucional colombiana, en Sala Tercera de Revisión, Sentencia T-512, del 09-09-1992.

12 URBINA, J. (2006) *Nuevos rasgos del Derecho a la Información en Venezuela.* Universidad del Zulia. Maracaibo. Pp. 17-20.

III. Los servicios audiovisuales

Si bien es cierto que hasta el momento se ha hecho referencia a la información en general, se debe precisar que son particularmente los medios radioeléctricos los que tienen un especial interés, por su poder de difusión de ideas, así como por el carácter dinámico e influyente que han tomado en la sociedad contemporánea. Así, originalmente los medios radioeléctricos se referían inicialmente a la radiodifusión sonora, luego referida a la televisión de señal abierta y posteriormente a los servicios de difusión por suscripción. Así por ejemplo, en el caso de Venezuela, la LRSRTVME regula los servicios de: a) radiodifusión sonora de señal abierta (en amplitud modulada <AM>; en frecuencia modulada <FM>; radiodifusión sonora por onda corta; radiodifusión sonora comunitaria de servicio público, sin fines de lucro; y servicios de producción nacional audio, difundidos a través de un servicio de difusión por suscripción); b) servicios de televisión en señal abierta (televisión UHF; televisión VHF; televisión comunitaria de servicio público, sin fines de lucro; y servicios de producción nacional audiovisual, difundidos a través de un servicio de difusión por suscripción); c) servicios de difusión por suscripción, que comprende los servicios de televisión y audio por cable o servicios satelitales; d) medios electrónicos (definición amplia e imprecisa que la norma no determina claramente, pero que pareciera referirse fundamentalmente a los servicios de Internet generados desde o hacia Venezuela)[13].

Los medios audiovisuales han cobrado una gran relevancia en virtud de su poder y capacidad de influenciar a los espectadores, por la capacidad de recrear la realidad, por cuanto brindan la posibilidad de establecer estructuras temporales distintas respecto de la percepción de la realidad (rompen el principio de irreversibilidad del tiempo, cuentan historias, representan la realidad, informan sobre hechos presentes y pasados, reales o imaginados). Además permiten participar en la elaboración de la realidad, en el relato de los hechos cotidianos y en el entretenimiento y la formación. Esta capacidad de recreación de la realidad y la tendencia al espectáculo es mayor en el cine y en la televisión, que en la radio, pues ésta tiene un lenguaje más discursivo, que le brinda a su vez un mayor poder informativo. No obstante, poseen siempre una capacidad de representar la realidad, con un gran poder de convencimiento, teniendo los mensajes audiovisuales la posibilidad de presentar la realidad en sus múltiples dimensiones. En todo caso, el lenguaje televisivo se considera ciertamente más influyente, en atención a su poder de sugestión, especialmente por la actitud del telespectador, que usualmente asume una posición pasiva frente al televisor, por ejemplo en relación a la posición que asume frente a la prensa escrita,

13 El artículo 1° de la norma referida, establece además que se aplica a los servicios en referencia, pues: "*Las disposiciones de la presente ley, se aplican a todo texto, imagen o sonido cuya difusión y recepción tengan lugar dentro del territorio de la República Bolivariana de Venezuela…*"

donde tiene una mayor capacidad reflexiva y más activa desde el punto de vista intelectivo.

IV. Necesidad de regulación y libertad de programación

Dentro de los motivos que han alegado tradicionalmente los gobiernos para regular el otorgamiento de permisos o licencias para los servicios audiovisuales, se encuentran fundamentalmente:

a) El carácter escaso de las ondas que integran el espectro radioeléctrico. En la mayor parte de los países (como por ejemplo, Venezuela), se considera al espectro radioeléctrico como un recurso escaso, cuya regulación y control le corresponde al Estado, quien otorga diversos tipos de permisos (en el caso venezolano, se habla de títulos habilitantes, integrados por las habilitaciones administrativas que tienen el carácter de autorizaciones operativas para las diferentes actividades de telecomunicaciones y las concesiones administrativas para el uso y explotación de determinadas porciones del espectro radioeléctrico). No obstante, se debe advertir que por su propia naturaleza, que tiene un carácter transfronterizo, por lo que el reparto de porciones del espectro radioeléctrico ha sido objeto de regulación por parte de diversos Tratados Internacionales para regular el reparto internacional de dicho recurso escaso entre los diversos y cada vez más complejos servicios de telecomunicaciones en las distintas regiones geográficas dentro del denominado dominio público radioeléctrico, no susceptible de propiedad privada por tratarse de un medio para el ejercicio de derechos fundamentales.

b) Elemento esencial para la difusión de las ideas. Desde la aparición del telégrafo, los gobiernos de los diversos países advirtieron que los medios radioeléctricos poseían una particular posición para la difusión de mensajes y para la difusión de informaciones e ideas, por lo que establecieron regímenes de intervención sobre los mismos. Si bien es cierto que este argumento constituye un elemento de dudosa justificación para establecer una regulación intensa sobre los servicios de radiodifusión, en el fondo siempre constituye un elemento de peso para los gobiernos a la hora de establecer el interés y control sobre dichos servicios de difusión, sobre todo por la posible utilización de los mismos en situaciones de emergencia.

c) La protección de los niños y adolescentes. Constituye uno de los elementos que tradicionalmente justifica la intervención intensa de los Estados dentro de los servicios de radiodifusión, con la finalidad de

garantizar que se difundan mensajes que resulten apropiados para este sector especialmente protegido de la población. En atención a este factor, por ejemplo, la LRSRTVME, establece la clasificación de los elementos (lenguaje, salud, sexo y violencia), y los combina con los horarios para la difusión de mensajes según que los mismos puedan ser percibidos libremente por niños niñas y adolescentes (horario todo usuario), que precisen el acompañamiento de padres, representantes o adultos responsables (horario supervisado), o bien que no resulten aptos para los niños y adolescentes (horario adulto).

d) La prohibición de difusión de contenidos que inciten al odio, la intolerancia, propaganda de guerra, etc., que se encuentran igualmente proscritas en Venezuela por la ley en referencia.

e) La tendencia oligopólica. Este razonamiento apunta a la tendencia a la concentración económica de los medios audiovisuales, en virtud de las importantes inversiones que se precisan para desarrollar dicha actividad, por lo que la regulación de la actividad debe apuntar hacia la democratización del espectro radioeléctrico y a la garantía de la diversidad de visiones y voces en los medios radioeléctricos. En el caso venezolano, la Ley Orgánica de Telecomunicaciones (LOTEL) (en desarrollo del derecho establecido en la Constitución a que la comunicación sea «libre y plural»), establece el derecho a la fundación de radioemisoras y televisoras de señal abierta, comunitarias, de servicio público y sin fines de lucro; que precisa que se trate de radioemisoras o televisoras que se dirijan a una determinada comunidad (lo que implica que no pueden tener carácter nacional), que deben dirigir su programación hacia la satisfacción de los intereses de la comunidad a la que sirvan y que no tengan fines de lucro. En cuanto a la implementación de este tipo de estaciones ha resultado ciertamente polémico, toda vez que la mayoría de los cientos de emisoras que se han establecido en el país, tienen un contenido marcadamente político y de carácter propagandístico en favor del oficialismo, lo cual desdice en gran medida su objetivo fundamental. De igual modo, su carácter no lucrativo ha determinado la necesidad de financiamiento, que en general se ha satisfecho mediante un intenso financiamiento oficial, que en gran medida se ha garantizado gracias a los tributos parafiscales que pagan las empresas de telecomunicaciones.

f) Su papel preponderante en la formación de la opinión pública. Resulta indudable el papel persuasivo de la radio y especialmente de la televisión, y además la extensa y masiva penetración que tiene en la sociedad, este carácter preponderante acentúa su influencia y relevancia desde

el punto de vista social y político, que determina su poder e influencia dentro de la conformación de la opinión pública. De allí el interés de los gobiernos por controlar la actividad de los medios de comunicación, en virtud de su poder comunicacional. Por ello es tan importante garantizar la diversidad y pluralidad de voces y rechazar los monopolios dentro de los servicios de difusión (en la mayoría de los países, las leyes impiden la concentración de conglomerados de medios de comunicación impresos, radiofónicos y televisivos, como por ejemplo en los Estados Unidos de América).

g) Constatada la penetración y carácter persuasivo de la radio y sobre todo de la televisión, se teme su influencia social y el poder político que supone su control. En realidad, el argumento se bifurca en una desconfianza social ante sus posibles efectos perniciosos (y, por tanto, se refiere tanto a situaciones de monopolio como de pluralidad de emisoras) y en la necesidad de neutralizar políticamente el medio bajo formas de control democrático en los casos de monopolio. O, en una versión debilitada, buscar formas de expresión del pluralismo social en situaciones de diversidad de emisoras.

h) Nuevos medios, nuevos canales. Desde hace varias décadas los servicios de radiodifusión no sólo se difunden en señal abierta, sino mediante los servicios por suscripción, mediante los sistemas de televisión y audio por cable, servicios satelitales que han multiplicado la posibilidad y disposición de señales que pueden transmitirse, diversificando la oferta de señales, así como las posibilidades de especialización temática de las mismas, lo cual obedece a la tendencia hacia la segmentación de las señales conforme los intereses de la audiencia. A esto se suman dos tendencias significativas en los últimos años, en primer lugar, el advenimiento de la televisión digital terrestre, que multiplica las posibilidades de transmisión de canales, lo cual puede incidir positivamente en la democratización de la oferta televisiva (no obstante, en Venezuela, las autoridades gubernamentales han optado por determinar qué canales podrán transmitir en señal digital, suministrando la infraestructura para tal fin, lo cual genera dudas en cuanto a la transparencia en los métodos de otorgamiento de los permisos para transmisión en el estándar digital escogido). De modo que el advenimiento de la televisión digital, hace que la consideración de «recurso escaso» entre en crisis, y se abran posibilidades para la democratización, diversificación y especialización de la oferta de canales mediante los servicios de televisión. En segundo lugar, otro factor que determina cambios en la prestación de los servicios de radiodifusión, es precisamente el advenimiento de los servicios de televisión por Internet

> y de radio por Internet, que multiplican la posibilidad de transmisión y recepción de señales más allá de las fronteras tradicionales y que por otra parte, plantea retos esenciales en cuanto al planteamiento tradicional del negocio en general, por cuanto permite acceder a señales mediante el protocolo de Internet desde cualquier lugar y en muchos casos, sin que resulte preciso acceder a servicios de suscripción, mediante la convergencia tecnológica de los servicios audiovisuales, que ya es accesible en muchos países y para lo cual se han desarrollado los denominados PC-TV o Smart-TV que reúnen las especificaciones propias de ordenadores con acceso a Internet y los terminales de servicios de TV, por ejemplo.

Como puede apreciarse, los factores tanto de índole legal, económico y político, influyen necesariamente en la libertad de programación. Si bien es cierto que conforme las tendencias predominantes en las democracias liberales se precisa garantizar la pluralidad de señales, de tal suerte que se garantice el pluralismo democrático, salvaguardando al tiempo la diversidad de opciones y la protección de los sectores sensibles de la sociedad, las consideraciones de carácter económico siguen vigentes, pues a pesar de que se han abaratado los recursos necesarios para la prestación de los servicios de radio y televisión, correlativo por ejemplo al encarecimiento de la prensa; de modo que han disminuido los costos de las infraestructuras técnicas, no así los costos de producción, particularmente en materia de televisión, que siguen siendo muy altos. Aparte se debe considerar que la sola multiplicación de señales, no garantiza necesariamente la pluralidad, como ha quedado demostrado en el caso venezolano, en el que la proliferación de radioemisoras y televisoras comunitarias (alrededor de 300), mantienen en general bajísimos niveles de audiencia. De modo que sólo la posibilidad de brindar una programación atractiva para el televidente o radioescucha (que brinde lo que resulta de interés para el público, que se refiera a los problemas, información, entretenimiento, deporte, etc., que logre responder a los gustos y necesidades de las comunidades), garantiza que las personas efectivamente prefieran los canales en cuestión. De modo que es ciertamente complejo, responder a las obligaciones de servicio público que deben cumplir las empresas de televisión y radiodifusión, con las necesidades propias de empresas que deben ser rentables y presentar ofertas de programación atractivas para la población.

Aunado a lo anterior, el progreso tecnológico y la diversificación de medios para la prestación de los servicios de radio y televisión (televisión digital terrestre, IPTV, televisión mediante dispositivos móviles, etc.), incide en una doble dimensión al hacer más diversa la oferta y al tiempo favorecer curiosamente la concentración de los grupos de comunicación en atención a que estos nuevos métodos técnicos exigen grandes recursos financieros. Debe destacarse igualmente que estos cambios esenciales que en el negocio de la radio y televisión,

suceden por los cambios tecnológicos recientes, también se producen en los demás medios de comunicación, pues por ejemplo, la prensa escrita, publicaciones periódicas, etc., se encuentran ante la disyuntiva de migrar definitivamente a plataformas digitales, mantener los soportes tradicionales sobre papel, o afrontar el reto multimedia, diversificando la oferta garantizando una oferta atractiva e interactiva para mantener vigencia.

Por otra parte, el supuesto carácter totalizante e intrusivo de la televisión se ha puesto en cuestionamiento frente a los servicios de televisión por suscripción, que permiten, al diversificar la oferta de canales, y gracias a la especialización de señales (de entretenimiento, espectáculo, variedades, deportes, viajes, compras, programación para niños, etc.), elegir las señales que desean ver. En todo caso, la libertad de programación queda determinada en una doble consideración, porque por una parte en la televisión y radiodifusión de señal abierta, la normativa venezolana de la LRSRTVME establece franjas horarias, la obligación de transmitir determinados contenidos de producción nacional independiente y obligaciones positivas en el sentido de tener que transmitir mensajes de responsabilidad social obligatorios de hasta setenta (70) minutos a la semana[14] (amén de las demás disposiciones en materia de publicidad, contenidos musicales, prohibiciones de determinados contenidos, elementos de

14 El artículo 10 de la LRSRTVME, establece las siguientes modalidades de acceso del Estado a espacios gratuitos y obligatorios para los servicios de radio y televisión: "*El Estado podrá difundir sus mensajes a través de los servicios de radio y televisión. A tales fines, podrá ordenarle a los prestadores de estos servicios la transmisión gratuita de: 1. Los mensajes previstos en la Ley Orgánica de Telecomunicaciones. La orden de transmisión gratuita y obligatoria de mensajes o alocuciones oficiales podrá ser notificada válidamente, entre otras formas, mediante la sola difusión del mensaje o alocución a través de los servicios de radio o televisión administrados por el Ejecutivo Nacional. 2. Mensajes culturales, educativos, informativos o preventivos de servicio público, los cuales no excederán, en su totalidad, de setenta minutos semanales, ni de quince minutos diarios. A los fines de garantizar el acceso a los servicios de radio y televisión, el órgano rector del Ejecutivo Nacional, con competencia en comunicación e información, cederá a los usuarios y usuarias diez minutos semanales de estos espacios, de conformidad con la ley. El órgano rector del Ejecutivo Nacional, con competencia en comunicación e información, estará a cargo de la administración de estos espacios, determinando los horarios y la temporalidad de los mismos, así como cualquier otra característica de tales emisiones o transmisiones. No está permitida la utilización de estos espacios para la difusión de publicidad o propagandas de los órganos y entes del Estado. Los prestadores de servicios de radio o televisión y difusión por suscripción no podrán interferir, en forma alguna, los mensajes y alocuciones del Estado que difundan de conformidad con este artículo, y deberán conservar la misma calidad y aspecto de la imagen y sonido que posea la señal o formato original. Se entiende como interferencia de mensajes la utilización de técnicas, métodos o procedimientos que modifiquen, alteren, falseen, interrumpan, editen, corten u obstruyan, en forma alguna, la imagen o sonido original. Los prestadores de servicios de difusión por suscripción cumplirán la obligación prevista en el numeral uno, a través de un canal informativo, y la prevista en el numeral dos, la cumplirán a través de los espacios publicitarios que dispongan en cada canal que transmiten. Los setenta minutos semanales se distribuirán entre los canales cuya señal se origine fuera del territorio de la República Bolivariana de Venezuela, de conformidad con la ley*".

clasificación, difusión del himno nacional, obligación de transmitir las alocuciones presidenciales, etc.), y en el caso de los servicios de difusión por suscripción, la norma en análisis determina los requisitos para la consideración de los productores nacionales de servicios audiovisuales, así como las normas que determinan el número de canales públicos, nacionales que como mínimo deben estar integrados en la grilla de programación de las televisoras por suscripción.

Es por ello que dentro de las particularidades propias de los servicios de televisión por suscripción, la contratación de un servicio específico, que ofrece un conjunto de canales con un sinnúmero de opciones es posible, pero en cambio, la recepción de determinadas señales sigue sin ser un acto previamente planificado y la prueba es que estos servicios intentan desarrollar dispositivos técnicos (control parental para contenidos sexuales explícitos o de violencia, para el bloqueo de determinadas señales por parte de los mismos usuarios abonados), para proteger por ejemplo a los menores.

El régimen de concesiones ha sido cuestionado por su posibilidad para limitar el ejercicio del derecho a la información, por cuanto el otorgamiento de concesiones siempre será un acto discrecional, que supone negar la preexistencia de un derecho a ejercer el derecho a prestar este tipo de servicios; no obstante, si el mecanismo para el otorgamiento de las concesiones se basa en criterios fundamentalmente técnicos y presupone la remoción de obstáculos para el ejercicio de un derecho subjetivo, como mera constatación de unos requisitos establecidos (en Venezuela en el régimen de la Ley de Telecomunicaciones de 1940 se consideraba que estos servicios eran de titularidad estatal, mientras que en la actualidad se presupone la existencia de un derecho subjetivo a la prestación de los servicios, sometida al cumplimiento de requisitos técnicos que se constatan mediante la obtención de los títulos habilitantes). De hecho, tras la promulgación de la Ley Orgánica de Telecomunicaciones de 2000, se estableció un régimen transitorio para la transformación de los títulos concesionales otorgados bajo la ley anterior, por los títulos establecidos al amparo de la nueva norma. No obstante, este proceso no estuvo exento de polémica por cuanto se revocaron un número significativo de concesiones, de forma discrecional y en muchos casos bajo la sospecha de consideraciones de carácter político, relativos a las líneas editoriales o informativas críticas con el gobierno nacional[15].

15 En su Informe Democracia y Derechos Humanos en Venezuela 2009, la Comisión Interamericana de Derechos Humanos, destacó: "*En relación con este punto, la CIDH reconoce, tal como lo indicara la Relatoría Especial en su pronunciamiento de 26 de junio de 2009, que los Estados tienen la facultad de regular las ondas radioeléctricas y de adelantar procedimientos para asegurar el cumplimiento de las disposiciones legales. En todo caso, esta facultad estatal, debe desarrollarse con estricto apego a las leyes y al debido proceso, de buena fe y respetando los estándares interamericanos que garantizan el derecho a la libertad de expresión de todas las personas. En un tema de tanta sensibilidad para la libertad de expresión como la regulación, asignación o fiscalización del uso de las frecuencias radioeléctricas, el Estado debe asegurar que ninguna de sus actuaciones está motivada o dirigida a premiar a los medios que comparten su política de gobierno o castigar a aquéllos que son críticos o independientes*". Disponible en

Particular gravedad tuvo el caso de Radio Caracas Televisión (RCTV), estación de televisión pionera del país y líder de audiencia en los servicios de televisión abierta en Venezuela, que ante la culminación de la concesión, no le fue renovada por parte de la Comisión Nacional de Telecomunicaciones (CONATEL), a pesar de haber cumplido con todos los requisitos y extremos establecidos en las leyes, bajo el argumento por parte del Presidente Chávez de que se trataba de un «canal golpista» (por su supuesta participación en los hechos que condujeron al golpe de estado de 2002). A pesar de tener todas las posibilidades para haber llevado los procedimientos administrativos y/o judiciales que hubieran podido conducir a revocar dicha concesión, se esperó hasta 2007 para no renovarla, conduciendo al cese de sus operaciones en señal abierta (a lo que se sumó la expropiación de sus equipos de transmisión que constituían la red más amplia del país, con el que se creó un canal de televisión oficial, destinado en principio a ser de servicio público «Televisora Venezolana Social <TVES>», que no obstante, mantiene bajísimos niveles de audiencia). Aunado a lo anterior, RCTV comenzó a transmitir en señal por suscripción, llegando a ser el canal de televisión por cable más visto del país, hasta que en el año 2009 se dictó la Norma Técnica sobre Servicios de Producción Nacional Audiovisual (Providencia N° 01) del año 2009 (que fue derogada por la norma en comento, que estableció condiciones que determinaron su segunda (y definitiva hasta el momento) salida del aire de esa televisora de las pantallas venezolanas. La promulgación de dicha norma sembró dudas acerca de si era precisamente esa finalidad la que se perseguía con la normativa de producción nacional audiovisual en particular.

De manera que si bien es cierto que no se puede negar la potestad incontestable del gobierno nacional de otorgar o no una concesión para la prestación de servicios de televisión o de radiodifusión en señal abierta, también es cierto que el proceso de otorgamiento o renovación de las mismas no debe ser un elemento de presión para establecer, premiar o castigar a un medio de comunicación que posea una posición crítica contra un gobierno de turno. La doctrina internacional en materia de protección de la libertad de expresión, ha reconocido que el otorgamiento de las concesiones puede ser una medida de restricción indirecta de dicho derecho (Así ha sido establecido no sólo en el caso RCTV vs. Venezuela y en el caso Baruj Ivcher vs. Perú por la Corte Interamericana de Derechos Humanos)[16]. De modo que se debe garantizar un

fuente electrónica, en: http://www.cidh.oas.org/countryrep/Venezuela2009sp/VE09CAPIVSP.htm [Consulta: 2014, agosto 25].

16 En su Informe "Democracia y Derechos Humanos en Venezuela" de 2009, la Comisión Interamericana de Derechos Humanos, estableció: *«El artículo 13.3 de la Convención Americana establece que: "No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones". En*

proceso de selección y otorgamiento de los títulos habilitantes transparente, que garantice un acceso objetivo en términos de igualdad. Por eso, el criterio del pluralismo debe objetivarse al máximo, no sólo en el sentido de establecer normas contra la concentración de medios en pocas manos, como sucede en Europa, sino también mediante la adopción de medidas que permitan seleccionar a asociaciones, grupos ciudadanos sin ánimo de lucro, que cuenten con el apoyo de subvenciones públicas, para contrarrestar el dominio de las empresas comerciales de forma transparente (emisoras comunitarias).

Conviene precisar que en cuanto a los servicios de televisión, se debe distinguir las empresas de producción televisiva, de las empresas de transmisión. En los servicios de televisión de señal abierta, normalmente las empresas de transmisión son también de producción, aunque también pueden transmitir producciones de otras empresas nacionales o extranjeras. En Venezuela, deben contar con una concesión administrativa que presupone la obtención de la correspondiente habilitación y la suscripción del contrato de concesión respectivo. No obstante, la normativa en análisis se refiere es a la producción televisiva, que fundamentalmente transmite su señal mediante otras empresas de televisión abierta o de televisión por suscripción (cable o satélite), las cuales suelen ser calificadas como generalistas o temáticas, según el tipo de programación que produzcan, y en públicas o privadas según la titularidad que presenten las mismas.

Cabe destacar, con respecto a la consideración de los servicios de televisión como servicios de naturaleza pública, que en la mayor parte de los países existen emisoras oficiales de servicio público, que por ejemplo en los Estados Unidos de América son las empresas emisoras institucionales, conectadas en la cadena *Public Broadcasting System* (PBS), y en otros países asumen la forma de empresas del Estado, que deberían sin embargo garantizar la pluralidad y transparencia como sucede en países como Inglaterra e incluso España. En Venezuela, han proliferado las emisoras televisivas públicas como Venezolana de Televisión (VTV), Televisora Venezolana Social (TVES), la Televisora de la Asamblea Nacional (ANTV), de la Fuerza Armada Bolivariana (FANBTV), entre otras, que en muchos casos no son precisamente un modelo de equilibrio informativo, ni de garantía de pluralidad, y que por lo demás resulta obligatorio para las operadoras de televisión por suscripción incluir en sus correspondientes grillas de programación. Estas empresas deberían servir con objetividad los

el mismo sentido, el principio 13 de la Declaración de Principios establece que "el otorgamiento de frecuencias de radio y televisión, entre otros, con el objetivo de presionar y castigar o premiar y privilegiar a los comunicadores sociales y a los medios de comunicación en función de sus líneas informativas, atenta contra la libertad de expresión y deben estar expresamente prohibidos por la ley. Los medios de comunicación social tienen derecho a realizar su labor en forma independiente. Presiones directas o indirectas dirigidas a silenciar la labor informativa de los comunicadores sociales son incompatibles con la libertad de expresión". Disponible en fuente electrónica, en: http://www.cidh.oas.org/countryrep/Venezuela2009sp/VE09CAPIVSP.htm [Consulta: 2014, agosto 25].

intereses generales y actuar de acuerdo con los principios de eficacia, equilibrio y objetividad. Si bien es cierto que no se considera negativo que un canal oficial difunda la obra del gobierno, también es cierto que sería perfectamente deseable que se diera cabida a la representación de todos los sectores de la sociedad, como canales del Estado y no sólo de un gobierno que debe tener un carácter contingente.

V. La Norma sobre los Servicios de Producción Nacional Audiovisual

La normativa en análisis establece el régimen de los servicios de producción nacional audiovisual, es decir aquellos que se difundan y/o reciban en el territorio venezolano, y que sean transmitidos mediante servicios de difusión por suscripción, a cuyo efecto se considera como tales los que emitan (bien en su programación semanal, como en su programación total), menos del setenta por ciento (70%) de su programas, publicidad o propaganda de producción nacional. A estos efectos se considera como: a) programas de producción nacional, aquellos difundidos por servicios de radio y televisión, en los cuales haya capital, locaciones, guion, directores, autores, personal artístico, personal técnico venezolanos, y también valores de la cultura venezolana; b) publicidad de producción nacional, entendiendo por tal aquellos mensajes publicitarios dirigidos a los habitantes de Venezuela; c) propaganda de producción nacional, aquel mensaje dirigido a los habitantes del país, destinado a persuadirlos para que se hagan adeptos o seguidores de ideas, políticas, filosóficas, morales, sociales o religiosas determinadas. A estos efectos se consideran no solamente la ejecución, sino también en el proceso de creación, dirección producción y postproducción.

La normativa analizada determina la obligación para los prestadores de servicios de difusión por suscripción, de incluir un número mínimo de servicios de producción nacional audiovisual en sus grillas de programación, que debe alcanzar como mínimo el ocho por ciento (8%) del número total de canales que ofrezca (artículo 9°), exceptuándose a efectos del cálculo respectivo: el canal informativo que deben ofrecer los prestadores de servicio de televisión por suscripción (cable o satelital), así como el canal de producción nacional independiente y comunitaria (establecido por el artículo 17 de la LRSRTVME), los canales exclusivos y los canales de pago por evento o programa (sistema *'Pay Per View'*). No obstante, conforme al artículo 15° de la norma en comento, los servicios de producción nacional y otros servicios de producción nacional «en los que el Estado tenga participación o interés»; no contarán a efectos del cálculo del número de servicios de producción nacional audiovisual obligatorio.

Establece por lo demás, el artículo 10 de la norma que la duración de los permisos para la prestación de los servicios de producción nacional audiovisual no podrá ser menor de dos años, ni exceder de cinco años, pudiendo ser renovada a juicio de CONATEL (debe solicitarse la renovación con noventa días continuos de anticipación a la fecha de su vencimiento). Por otra parte, queda evidenciado

el carácter discrecional de la norma cuando se establece en su artículo 11, que los permisos para la prestación de los servicios de producción nacional audiovisual se extinguirán cuando CONATEL, lo juzgue conveniente a los intereses de la Nación, o cuando así lo exigiere el orden público o la seguridad nacional, pudiendo a su juicio revocar o suspender, en cualquier momento, los permisos en cuestión.

De igual modo, se establece que los prestadores de servicios de producción nacional audiovisual que desarrollaran su actividad para el momento de promulgación de la norma, a través de las redes de los operadores del servicio de difusión por suscripción, deben solicitar a CONATEL el permiso correspondiente, dentro de los treinta (30) días continuos siguientes a la publicación de la Providencia en cuestión, contando CONATEL con un lapso de ciento veinte (120) días continuos a partir del vencimiento del plazo anterior, para decidir sobre el otorgamiento o no de los permisos solicitados.

Esta norma establece la obligación para los prestadores de servicios de producción nacional audiovisual de someterse a la aplicación de las disposiciones de la LRSRTVME para poder emitir su señal desde Venezuela, lo cual en la práctica implica que deben someterse a las normas acerca de los contenidos en cuanto a obligaciones positivas (necesidad de transmitir ciertos contenidos), así como a obligaciones de carácter prohibitivo (respecto de determinados contenidos considerados como nocivos, o limitados en cuanto a los horarios de transmisión). En efecto, la norma establece elementos de clasificación en cuanto a los contenidos transmitidos (lenguaje, salud, sexo y violencia), que a su vez tienen varias categorías, que determinan que por ejemplo, los contenidos de tipo sexual explícito o de violencia real, no simulada, no puedan ser difundidos, y que otros sólo puedan ser transmitidos en determinados horarios[17].

Otro aspecto polémico de la norma analizada, es la obligación para los prestadores de servicios de producción nacional audiovisual de transmitir obligatoria y gratuitamente, las alocuciones oficiales (obligación de transmitir las denominadas ‘cadenas’), que conforme a la LOTEL, el Ejecutivo Nacional puede ordenar, sin limitación y de forma conjunta, mediante los servicios de televisión y radiodifusión por señal abierta. De igual modo limita la posibilidad de incluir mensajes publicitarios interrumpiendo la transmisión de los programas, por lo que sólo se pueden transmitir estos mensaje al concluir o iniciar los mismos, y con los límites máximos establecidos en la LRSRTVME, vale decir quince

17 La LRSRTVME, establece en su artículo 7°, la clasificación de los horarios de transmisión, distinguiendo el horario “todo usuario”, como aquel en el que se pueden transmitir contenidos que sean susceptibles de ser percibidos por niños y adolescentes, sin compañía de padres o adultos responsables (7:00 a.m. a 6:59 p.m.); el horario “supervisado”, que es aquel en que se pueden difundir contenidos que puedan ser percibidos por niños y adolescentes en compañía de sus padres o adultos responsables (5:00 a.m. a 6:59 a.m. y de 7:00 p.m. a 10:59 p.m.), y el horario «adulto» que es aquel en el que se pueden transmitir contenidos no aptos para niños y adolescentes (11:00 p.m. a 4:59 a.m.).

(15) minutos de publicidad por cada hora de transmisión, con la inclusión de un máximo de dos (2) minutos para promoción del propio canal.

VII. Conclusiones

La norma mencionada tiene sin duda un doble efecto sobre el derecho a la libertad de expresión. En primer lugar, el derecho a certificar qué tipo de material puede ser comprendido dentro de la categoría de producción nacional atendiendo al contenido de dicho material, es claramente un mecanismo que puede conducir a la censura previa de la producción nacional. De manera que será el Estado quien previamente decidirá la calificación de los productores nacionales, lo cual podría comprometer su neutralidad frente a los contenidos y al derecho del público de acceder a una información plural y diversa, distinta a aquélla que los funcionarios estatales consideren que debe ser divulgada. En segundo lugar, estas disposiciones podrían imponer el contenido de la programación que debe ser difundida, lo cual puede incidir negativamente en el ejercicio del derecho a la libertad de expresión. Conviene puntualizar que tanto la Constitución venezolana, como la Convención Americana de Derechos Humanos disponen que el ejercicio de la libertad de expresión no puede estar sujeto a previa censura sino a responsabilidades ulteriores, por lo que mal podrían establecerse estas normas que discriminan el tipo y calidad de la producción que se puede transmitir para calificar como producción nacional, y en consecuencia, poder se transmitida por medio de los servicios de difusión por suscripción.

En conclusión, la norma referida afecta el derecho a la libertad de programación de las empresas prestadoras de servicios de televisión por suscripción, al someter a controles no muy claros a las empresas que pueden prestar estos servicios, estableciendo mediante la introducción de conceptos jurídicos indeterminados, una potestad discrecional para el otorgamiento o no de los permisos requeridos, así como de una posibilidad muy amplia e igualmente discrecional para el ente rector de las telecomunicaciones para revocar dicha autorización, lo cual levanta sospechas acerca de la neutralidad y equilibrio que se pueda prestar en el otorgamiento de los permisos en cuestión.

Los nuevos nombres de dominio de primer nivel genéricos y la aplicación del *Uniform Rapid Suspensión System* (URS) de ICANN

Mónica Lastiri Santiago*

SUMARIO: I. Los nuevos nombres de dominio de primer nivel genéricos. II. Diferencias entre los gTLD, los ccTLD y los nuevos gTLD. III. Las nuevas políticas del ICANN. IV. El sistema uniforme de suspensión rápida (URS). V. Diferencias entre la Política Uniforme de Solución de Controversias en materia de nombres de dominio (UDRP) y el URS. VI. La *Trademark Clearinghouse*. VII. El URS y su aplicación. 1. Caso Facebook. 2. Caso Branson. 3. Caso BBVA. 4. Caso Aeropostale. 5. Caso Wolfram. VIII. Conclusiones.

Resumen

Debido a la repercusión que ha tenido Internet en las economías de todo el mundo, la cuestión de los nuevos nombres de dominio de primer nivel es de gran importancia. El *Uniform Rapid Suspension System* (URS) es un nuevo sistema de resolución de conflictos en materia de nombres de dominio que ha sido diseñado para casos de cybersquatting en los nuevos gTLD. Este mecanismo permite que los titulares de marca obtengan de forma rápida el bloqueo de un nombre de domino que vulnere sus derechos, siempre y cuando prueben de forma «clara y convincente» dicha infracción. El análisis de distintos casos resueltos por la National Arbitration Forum (NAF) nos muestra cuáles están siendo los criterios en la aplicación de esta nueva política de ICANN.

Palabras clave: Nuevos gTLD. URS. UDRP. Marcas.

Abstract

Because of Internet's impact on world's economies, the new generic domain names issue it is a very important issue. The Uniform Rapid Suspension System (URS) is a new domain name dispute resolution system specially designed to tackle cybersquatting

Recibido: 21/10/2014 • Aceptado: 9/11/2014

* Doctora en Derecho por la Universidad Carlos III de Madrid. Profª Ayudante de Derecho Mercantil Universidad Carlos III de Madrid.

cases in the new generic top level domains (New gTLD) extensions. This mechanism allows trademark owners to block in a fast way a domain name that infringes its rights insofar such infringement can be clearly and convincingly evidenced. The study of various cases decided by the National Arbitration Forum (NAF) shows us what the criteria are being implementing this new policy of ICANN.

Keywords: New gTLD. URS. UDRP. trademarks.

I. Los nuevos nombres de dominio de primer nivel genéricos

Antes del mes de octubre del año 2013, el sistema de nombres de dominio estaba formado por los nombres de dominio de primer nivel genéricos (*Generic Top Level Domains*, gTLD) ***.arpa., gov,v.edu, .mil, .aero, .coop, .museum, .cat, .jobs, .mobi, .travel, .tel, .asia, .post. y los conocidos .com, .net, .org, .int, .info, .name, .pro, .xxx.*** Igualmente forman parte del sistema los nombres de dominio de primer nivel geográficos o territoriales (*Country Code Top Level Domains*, ccTLD) que identifican a un país concreto y se corresponden con la codificación de países y territorios establecida por la norma ISO 3166-1.

Junto a estas extensiones de primer nivel se incluyen los no menos importantes dominios de segundo nivel. Estos dominios de segundo nivel junto con las extensiones de primer nivel forman el nombre de dominio tal y como lo conocemos. El conflicto que surge entre éstos con los signos distintivos de propiedad industrial es la fuente inspiradora del actual régimen jurídico de los nombres de dominio que ataja, principalmente, el problema del *cybersquetting*.

Por último, aparecen los nombres de dominio internacionalizados (*Internationalized Domain Names*, IDN) o plurilingües que contienen caracteres con signos diacríticos (utilizados por numerosos idiomas europeos) o caracteres de códigos no latinos, tales como el árabe o el chino[1]. En un principio se instauraron en los nombres de dominio de segundo nivel[2] bajo extensiones de primer nivel que podían contener letras o caracteres ajenos al ASCII[3].

1 *Vid.* http://www.icann.org/en/topics/idn/ [visita: 12 de agosto de 2014].

2 ICANN, «IDNs: Nombres de Dominio Internacionalizados», http://www.icann.org/es/topics/idn/factsheet-idn-fast-track-oct09-es.pdf [visita: 12 de agosto de 2014].

3 El ASCII es un código numérico común para los ordenadores y otros equipos que trabajan con texto. Los ordenadores únicamente interpretan números, y para facilitar su uso al ser humano se utiliza este código que es la representación numérica de un carácter. Casi todos los sistemas informáticos actuales utilizan el código ASCII, pues se trata de un código de caracteres basado en el alfabeto latino. *Vid*. JENNINGS, T., «An Annotated History of Some Caracter Codes or ASCII: American Standard Code for Information Infiltration», octubre de 2004, http://wps.com/projects/codes/index.html [visita: 12 de agosto de 2014].

En la actualidad, con la llegada de los nuevos gTLD existirán numerosos nombres de dominio con su primer y segundo nivel con caracteres ajenos al ASCII, ya que concurrirán gTLDs IDN por primera vez en la historia de Internet.

La inclusión de los IDN en el sistema de nombres ha sido una de las innovaciones más importantes de la Red de redes, ya que estos nombres de dominio ofrecen nuevas oportunidades y beneficios para los usuarios de Internet en todo el mundo, teniendo en cuenta que para el 60% de los mismos el inglés no es su idioma materno. No obstante, el progreso más significativo de Internet es la incorporación de los nuevos gTLD en el sistema de direcciones.

Este año 2014 estamos experimentando la verdadera innovación de Internet, pues están entrando (de forma gradual) en el *Domain Name System* (DNS) un gran número de nuevas extensiones de primer nivel genéricos, lo cual está transformando la forma que tienen las personas de encontrar información en Internet[4].

Desde el nacimiento de Internet, es decir, desde que los ordenadores de la Universidad de Standford y la UCLA conectarán por primera vez, el número de usuarios ha aumentado en aproximadamente 2,27 mil millones en el mundo, y su número sigue incrementándose diariamente[5]. En este punto, la incógnita que rodeaba a este exponencial crecimiento era si la infraestructura de Internet era capaz de soportar adecuadamente este gran incremento de usuarios.

Según la *Internet Corporation for Assigned Names and Numbrer* (en adelante, ICANN) el espacio de nombres era limitado para responder a la vertiginosa evolución de la Sociedad de la Información y el comercio electrónico establecido en ella. Por ello, en estos meses el mundo se encuentra en medio de la culminación del cambio más radical que se ha llevado a cabo en la infraestructura de Internet[6]: el programa de los nuevos gTLD.

ICANN se formó en 1998 para supervisar una serie de funciones relacionadas con Internet[7] incluyendo el procedimiento de registro de nombres de dominio del que anteriormente se encargaba IANA.

4 La ICANN publicaba las delegaciones de nuevas extensiones como son .auction, .lacaixa, .healthcare o .ong. Para mayor información, vid. http://newgtlds.icann.org/en/program-status/delegated-strings (visita: 18 de agosto de 2014). En agosto entraron a registro a todo el público varias extensiones relacionadas con la medicina como.care, .clinic,.dental.surgery y otras relacionadas con las finanzas .cash,.fund,.investments y.tax. *Vid*. *http://www.domisfera.com/9-nuevas-extensiones-para-esta-semana/* [visita: 18 de agosto de 2014].

5 Sobre este particular, *vid.* www.internetworldstats.com [visita: 1 de febrero de 2014]. La cifra actual de usuarios de Internet es el doble que hace cinco años. *Vid.* además ICANN, «Nuevo Programa gTLD», http://www.icann.org/en/topics/new-gtld-program.htm [visita: 15 de enero de 2014].

6 Vid. ICANN: New Generic Top Level Domains. «Frequently Asked Questions» en http://newgtlds.icann.org/en/applicants/customer-service/faqs/faqs-en [visita: 12 de agosto de 2014].

7 Para mayor información de todas las funciones de ICANN. Vid. Ascencio…

Desde el principio, ICANN trabaja para desarrollar el espacio de Internet y dar cabida a un sin número de empresas en línea, comunidades, organizaciones, etc. Siguiendo ese objetivo de mejorar la Red de redes se discutió acerca de la conveniencia de crear otros gTLD, pues se estaba advirtiendo una saturación en tres de los dominios de «libre registro», o, como los llama la ICANN, «no patrocinados»: *.com, .net* y *.org*. Debido a ello, en noviembre de 2000 se decidió introducir siete gTLD más al DNS[8]. Entre los años 2000 y 2002 nacieron los dominios *.aero, biz, .info, .name* y *.pro*. Un año más tarde, la ICANN inició un nuevo proceso que condujo a la introducción de otros seis nuevos TLD, *.asia, .cat, .jobs, .mobi, .tel y .travel*, en el año 2004[9]. Los más recientes dominios genéricos de nivel superior son, como ya se señaló, *.post*, que entró al DNS a mediados del 2010, y *.xxx*, que lo hizo en 2011.

En junio de 2008, ICANN aprobó las recomendaciones de la *Generic Name Supporting Organization* (GNSO) para la inclusión de los nuevos gTLD. Ello, con el objetivo de mantener y generar procesos que aseguren la competencia y velar por los intereses de los consumidores. Actualmente, existen ya 276 millones registrados en el mundo[10].

II. Diferencia entre los gTLD, los ccTLD y los nuevos gTLD

Las distinción básica es que mientras los gTLD y ccTLD se crearon para facilitar la comunicación entre algunos ordenadores, los nuevos gTLD responden a la demanda de nuevas direcciones para el establecimiento de sitios web, principalmente comerciales entre otras sin ánimo de lucro.

El programa para los nuevos gTLD es una iniciativa para permitir la introducción de una cantidad ilimitada de gTLD. La decisión de expandir de esta forma el espacio de nombres de dominio surge de la necesidad de eliminar las limitaciones que existen en los gTLD que no reflejan la realidad y las necesidades actuales de la Red. Igualmente, nacen para crear una plataforma para la innovación en la industria e Internet y para aumentar la cantidad de opciones y la competencia en el mercado[11].

El proceso de solicitudes para la gestión de una nueva extensión de primer nivel comenzó en enero de 2012 y el 23 de octubre de 2013, después de ocho años de estudio y 47 solicitudes de comentario público, que resultaron en 2400 comentarios, 55 memorandos explicativos y siete versiones de la *Guía para el*

8 ICANN, «New TLD Program Application Process Archive», October 2000, http://www.icann.org/en/tlds/app-index.htm [visita: 6 de marzo de 2008].

9 *Vid.* ICANN, «Information Page for Sponsored Top-Level Domains», 28 November 2005, http://www.icann.org/en/tlds/stld-apps-19mar04 [visita: 6 de marzo de 2008].

10 *Vid. The Domain name industry brief*. Vol.11, Issue 2, August 2014. http://www.verisigninc.com/assets/domain-name-brief-july2014.pdf [visita: 12 de agosto de 2014].

11 http://archive.icann.org/es/topics/new-gtlds/basics-new-extensions-21jul11-es.pdf [visita: 12 de agosto de 2014].

solicitante, la ICANN anunció la delegación de los cuatro primeros nuevos gTLD: شبك, (entidad registradora: International Domain Registry Pty. Ltd); .онлайн y .сайт que significa «online» o «sitio web» en ruso (entidad registradora: Core Association) y游戏, que significa «juego» en chino y estará a cargo de su gestión Spring Fields, LLC[12].

El 21 de enero de 2014, la ICANN anunció que el número de nuevos gTLD que están ya incluidos en el DNS es de 100[13]. El 4 de febrero de 2014 se incorporaron al sistema: *.blues, .flights, .cruises, .rental, .tokio.* entre muchas otras nuevas extensiones[14]. El 1 de abril de 2014 había 439,565 nombres de dominio registrados en nuevas extensiones y en julio de este mismo año la cifra aumentó a 1,471,166, un millón de dominios más. Entre las extensiones más populares figuran .berlin, .club, .guru,.photography, .email, .link, .toy y .wang más el IDN.在线[15].

Los nuevos gTLD serán progresivamente introducidos en la zona raíz de Internet y en la base de datos central del sistema de nombres de dominio. Cada extensión cuenta con su entidad gestora y en cualquier momento pueden implementar los procesos finales necesarios para poner sus dominios a disponibilidad de los usuarios de Internet. El DNS pasará de tener 25 gTLD a más de 1 400 nuevas extensiones[16].

El *Uniform Rapid Suspension System* nace como resultado del programa de lanzamiento de los nuevos gTLD. Su objetivo esencial es contrarrestar los posibles problemas que surjan entre los titulares de marca y los nombres de dominio de segundo nivel registrados bajo las nuevas extensiones de primer nivel.

III. Las nuevas políticas de ICANN

Los planes de ICANN sobre la introducción de los nuevos gTLD causaron una gran preocupación dentro de la comunidad marcaria. La Organización Mundial de Protección de Propiedad Intelectual (OMPI) indicó que dicha

12 *Vid*. ICANN. «Internet Domain Name Expansion Now Underway», en http://www.icann.org/en/news/press/releases/release-23oct13-en [visita: 27 de octubre de 2013].

13 http://www.icann.org/es/news/press/releases/release-21jan14-es. [visita: 18 de agosto de 2014].

14 Para realizar el seguimiento de los nuevos gTLD incorporados al DNS, *vid. http://newgtlds.icann.org/en/program-status/delegated-strings* [visita: 27 de abril de 2014].

15 *Vid. http://www.domisfera.com/situacion-actual-de-las-nuevas-extensiones-julio-2014/* La ICANN publicaba las delegación de nuevas extensiones como .auction, .lacaixa, .healthcare o .ong. [visita: 18 de agosto de 2014].

16 Antes de que el público en general pueda acceder a estos nuevos gTLD, las entidades registradores deberán finalizar un último proceso que ha sido incorporado en el Programa de Nuevos gTLD con el objetivo de proteger a los titulares de derechos de marca, consistente en un período obligatorio de 30 días en el que sólo los titulares de marca podrán acceder al registro de SLD para solicitar su signo distintivo en la extensión que les interese. *Vid.* ICANN. «Internet

inclusión debía ser deliberada y responder apropiadamente al potencial aumento del *cybersquatting* y a la confusión del consumidor.

Con el fin de atenuar los conflictos que pudiesen surgir entre las marcas y los nuevos gTLD surgieron nuevos instrumentos en materia de nombres de dominio. El objetivo de estas nuevas políticas es brindar oportunidades a los titulares de derechos de propiedad industrial, quienes deberán hacer frente a otros problemas de orden jurídico y práctico como: a) la expansión del espacio de nombres con la creación a ritmo acelerado de centenares de nuevos gTLD y b) la creación de nombres de dominio internacionalizados (IDN) y su inclusión en el nivel superior.

Para alcanzar este objetivo se formó el *Implementation Recommendation Team* (en adelante, IRT) de 2009[17]. El propósito de este fue formular recomendaciones relativas a la puesta en marcha de los nuevos gTLD con el objeto de elaborar y proponer soluciones a la cuestión global de la protección de las marcas en las nuevas extensiones de primer nivel genéricas[18]. Esa iniciativa de ICANN estuvo motivada por las dudas que manifestaron las partes interesadas en la propiedad intelectual a propósito del alcance de la protección que brindaba la *Guía para del solicitante* de nuevos gTLD en sus primeras versiones. Este equipo analizó la actual situación de la protección de marcas y respondió con nuevas propuestas para proteger a los titulares de las mismas[19].

El IRT de la ICANN formuló inicialmente seis propuestas: 1) la creación del denominado *IP Clearinghouse,* 2) la creación de una lista de marcas protegidas a nivel mundial, 3) el establecimiento del *Uniform Rapid Suspension System*[20], 4) la existencia de un procedimiento para la resolución de disputas de marcas postdelegación (*post-delegation dispute resolution mechanisms*, en adelante,

Domain Name Expansion Now Underway», en http://www.icann.org/en/news/press/releases/release-23oct13-en [visita: 27 de octubre de 2013].

17 El IRT nació a solicitud de la ICANN al *Intellectual Property Constituency.* El IRT, aunque refleja la diversidad de la experiencia en la composición del grupo –formado por personas con extensos conocimientos en los campos del derecho de marcas, la protección de los consumidores, la competencia desleal, la interacción de las marcas y el sistema de nombres de dominio–, desarrollan en sus propuestas una sobreprotección a los titulares de marcas en relación con la introducción de nuevos gTLD sin tomar en cuenta a los registrantes de los nombres de dominio ni a los usuarios finales. *Vid.* Declaración conjunta de ALAC y NCUC sobre el Informe Final del IRT en http://archive.icann.org/en/topics/new-gtlds/irt-final-report-trademark-protection-29may09-en.pdf [visita: 12 de agosto de 2014].

18 El IRT fue formado por la Junta directiva para la evaluación de riesgos de la Política de los gTLD de la ICANN el 6 de marzo de 2009. ICANN, *Introduction: Implementation Recommendation Team (IRT), ICANN*, 1 (24 de abril de 2009), http://www.icann.org/en/topics/new-gtlds/irt-draft-report-trademark-protection-24apr-09-en.pdf [visita: 12 de agosto de 2014].

19 *Vid.* ICANN, *An Open Letter from the IRT Introducing Our Work,* 29 de mayo 2009.

20 En su expresión en español, Sistema Uniforme de Suspensión Rápida. Traducción de la ICANN. Borrador del 19 de septiembre de 2011.

PDDRP), 5) la reconsideración de los requisitos de *Whois* para los nuevos gTLD, y 6) un procedimiento de objeciones previo a la introducción del gTLD[21]. Asimismo, se propuso el uso de un algoritmo para el examen de confusión de las extensiones en la fase inicial, desarrollado por la ICANN.

De estas recomendaciones, sólo tres tuvieron repercusión. Las propuestas sobre la base de datos *Whois* y el uso del algoritmo no tuvieron aceptación. Igualmente, la ICANN rechazó sin más trámite la propuesta de redactar la lista de marcas protegidas a escala mundial[22].

Sucintamente, los nuevos mecanismos de protección de derechos que han sido adoptados por ICANN son los siguientes:

- Mecanismos de protección de derechos correspondientes a los nuevos gTLD.
  - El procedimiento de controversias para la etapa previa a la adjudicación de un nuevo gTLD
  - Procedimiento de solución de controversias post-delegación de nuevos gTLD.

  Estos procedimientos fueron desarrollados para proporcionar una alternativa para aquellos que se vean afectados por la conducta de un operador de registro de un nuevo gTLD e incluye:
  - Trademark Post-Delegation Dispute Resolution Procedure

  La ICANN adoptó un procedimiento general para la resolución de disputas de marcas postdelegación: *el Trademark Post-Delegation Dispute Resolution Procedure* (PDDRP)[23].
  - *Registration Restriction Dispute Resolution Procedure* (RRDRP)
  - *Public Interest Commitments Dispute Resolution Procedure* (PICDRP). Todos estos mecanismos se refieren solo a la extensión de primer nivel.

21 IRT Recommendations, p. 7.

22 *Vid*. OMPI, Asamblea General de la OMPI. Cuadragésimo periodo de sesiones (20º ordinario) Ginebra, 26 de septiembre de 5 de octubre de 2011. WO/GA/40/9. 26 de julio de 2011.

23 ICANN. Trademark Post-Delegation Dispute Resolution Procedure. *Applicant Guidebook*. Module 5. http://newgtlds.icann.org/en/applicants/agb [visita: 19 de abril de 2013]. En respuesta a la necesidad de los titulares marcarios de disponer de un procedimiento administrativo con carácter permanente, que permitiera la presentación de demandas relacionadas con un nuevo administrador de registro de gTLD que haya sido aprobado, cuando la forma en que funciona y se utiliza en la práctica el registro dé lugar supuestamente al uso abusivo de la marca o contribuya sustancialmente a ello tuvo respuesta con la propuesta concreta que en 2009 el Centro de la OMPI presentó ante la ICANN sobre el contenido de un procedimiento de solución de controversias (en relación con las marcas) para la etapa *posterior* a la adjudicación de la nueva extensión. Ello con el fin de incluir conductas de este tipo que pudieran darse en los registros de los gTLD nuevos. http://www.wipo.int/-amc/en/docs/icann130309.pdf [visita: 5 de agosto de 2009].

- Mecanismos de protección de derechos correspondientes a los nombres de dominio de segundo nivel bajo los nuevos gTLD:
  - El *Uniform Suspension Rapid System*
  - La *Trademark Clearinghouse*

IV. Funcionamiento de la URS y sus diferencias con la UDRP

El sistema uniforme de suspensión rápida de ICCAN pese a que nació con la intención de lograr un equilibrio prudencial entre la protección de los derechos de marca reconocidos por ley, el interés de orden práctico de los administradores de registros de buena fe por buscar volúmenes de trabajo mínimos, y las expectativas legítimas de los titulares de nombres de dominio que actúan de buena fe[24], es un mecanismo más que protege a los titulares de derechos de marca.

Su principal característica es que bloquea el nombre de dominio objeto de la reclamación y se aplica en aquellos casos en que esté involucrado un nombre de dominio de segundo nivel registrado bajo cualquier gTLD. Sin embargo, nace con las nuevas extensiones de primer nivel genéricas. El URS, además de bloquear el nombre de dominio de forma rápida, pues se puede obtener una decisión en 14 días, tiene un coste más económico que el de su antecesora: la Política Uniforme de Solución de Controversias en materia de Nombres de Dominio (UDRP).

Los proveedores de este sistema son el *National Arbitration Forum* (NAF o FORUM) y la *Asian Domain Name Dispute Resolution Centre* (ADNDRC), ambos organismos cuentan con vasta experiencia en la resolución de conflictos entre marcas y nombres de dominio bajo la UDRP[25].

El procedimiento se inicia mediante la «reclamación» del titular de la marca que se considera vulnerada ante un proveedor del URS[26]. Dicha presentación es en cualquier caso vía electrónica y deberá contener, entre otros requisitos, la mención de la marca en la que se fundamente la demanda y una declaración exponiendo los motivos sobre los cuales basa su petición[27].

La principal cualidad del procedimiento del URS es que para que el reclamante pueda obtener una orden de bloqueo del nombre de dominio que considera vulnera su derecho de marca debe demostrar, con pruebas *claras y convincentes*, cada uno de los tres elementos que a continuación se detallan[28]:

24 OMPI, «Asamblea…», *op. cit.*, apartado 30.

25 ICANN, «URS Providers», http://newgtlds.icann.org/en/applicants/urs [visita: 18 de agosto de 2014].

26 Regla 1 de ICANN, «Uniform Rapid Suspension System», Versión del 1 de marzo de 2013, http://newgtlds.icann.org/en/applicants/urs [visita: 18 de agosto de 2014].

27 Reglas 1.2.1 a 1.2.5 del URS

28 *Vid.* 1.2.6 del URS

1) que el nombre de dominio es idéntico o similar hasta el punto de crear confusión con respecto a la marca de la cual es titular[29],

2) que tiene un registro nacional o regional válido y actualmente en vigor, o bien que la marca de la cual es titular ha sido reconocida a través de un procedimiento judicial o está debidamente protegida por una ley o tratado vigente al momento de la presentación de la reclamación bajo el URS[30], además

3) tendrá que acreditar que el registrante no tiene ningún derecho o interés legítimo respecto al nombre de dominio[31] y que éste ha sido registrado y utilizado de mala fe[32].

Entre las pruebas de registro y utilización de mala fe, se expone una lista de las circunstancias que demuestran que se trata de un registro y uso de mala fe y reproduce lo establecido en el artículo 4 (b) (i)(ii)(iii) y (iv) de la UDRP:

a. Que se ha registrado o adquirido el nombre de dominio fundamentalmente con el fin de vender, alquilar o ceder de otra manera el registro del nombre dominio al reclamante que es titular de la marca de productos o servicios o a un competidor de ese reclamante, por un valor cierto que supera los costos diversos documentados que están relacionados directamente con el nombre de dominio; o
b. Que se ha registrado el nombre de dominio con el fin de impedir que el titular de la marca de productos o servicios refleje la marca en un nombre de dominio correspondiente, siempre y cuando el registrante haya participado en conductas de esa índole; o
c. Que se ha registrado el nombre de dominio fundamentalmente con el propósito de perturbar la actividad comercial de un competidor; o
d. Que al utilizar el nombre de dominio, el registrante ha intentado de manera intencionada atraer, con ánimo de lucro, usuarios de Internet o su sitio web o cualquier otro sitio en línea, creando un riesgo de confusión con la marca del reclamante en cuanto a la fuente, patrocinio, afiliación o promoción de su sitio web o ubicación o de un producto o servicio que figure en su sitio web o ubicación.

29 Regla 1.2.6.1 del URS

30 En dicha reclamación se debe presentar una prueba de uso de la marca, que puede consistir en una declaración de ese uso en el comercio junto con una muestra o ejemplo de ello. Dicha prueba debe ser certificada por la *Clearinghouse.*, *Vid.* Regla 1.2.6.1, del Uniform Rapid Suspension System.

31 Regla 1.2.6.2 del URS.

32 Regla 1.2.6.3 del URS.

Es preciso señalar que una vez presentada la reclamación, se llevará a cabo una «revisión administrativa»[33], y el proveedor del sistema deberá informar a la entidad de registro de la «notificación de reclamación», por lo que ésta debe proceder al «bloqueo» del nombre de dominio objeto de la reclamación. Este bloqueo restringirá todos los cambios de los datos de registro, incluyendo la transferencia y eliminación de nombres de dominio, pero el dominio seguirá funcionando con la dirección IP al que está vinculado. Posteriormente, la entidad de registro informará al proveedor del URS de la suspensión del nombre de dominio a través de la «notificación de bloqueo»[34].

En la respuesta o contestación de la reclamación, el registrante, además de que debe cumplir con ciertos requisitos de tiempo y forma[35] puede refutar la afirmación de registro de mala fe al establecer cualquiera de las siguientes circunstancias:

a) que antes de haber recibido cualquier aviso de la reclamación, no ha utilizado ni ha efectuado preparativos demostrables de utilización del nombre correspondiente al nombre de dominio en relación con una oferta de buena fe de productos o servicios; o

b) que en calidad de particular, empresa u otra organización ha sido conocido por el nombre de dominio, aún cuando no haya adquirido derechos de marca de productos o de servicios; o

c) que está llevando a cabo un uso legítimo y leal, sin intención de desviar a los consumidores de forma equívoca o empañar el buen nombre de la marca de productos o de servicio del reclamante[36].

Si sobre la base de estas circunstancias el examinador considera probados los hechos planteados por el registrante, ello dará lugar a un pronunciamiento a favor de este último[37].

V. Diferencias entre la Política Uniforme de Solución de Controversias en materia de nombres de dominio (UDRP) y el URS.

En realidad, todas las medidas de este sistema mencionadas hasta ahora son idénticas, a las reglas establecidas en la UDRP. Las diferencias entre un sistema y otro están principalmente en que:

33 Dada la naturaleza rápida del procedimiento y la intención proporcionar tarifas accesibles, no habrá oportunidad para corregir deficiencias en los requisitos de presentación. Regla 3.3 del URS.

34 Deben transcurrir 24 horas para notificar la reclamación y otras 24 horas para notificar el bloqueo (apartado 4.1 del URS). El idioma predominante será el inglés (apartado 4.2 del URS).

35 *Vid.* Reglas 5.1 al 5.7 del URS.

36 *Vid.* Reglas 5.7.1 a 5.7.3.

37 Regla 5.7.3.

1. El URS bloquea el dominio a las 24 horas de recibida la notificación de la reclamación al proveedor URS. La UDRP no bloquea el nombre de dominio, sus resoluciones se basan en la transferencia o no del nombre de dominio al titular de la marca.
2. El procedimiento URS puede tener una duración de 14 días[38]. El procedimiento administrativo de la UDRP debe completarse en el plazo de 60 días.
3. El URS exige un alto grado de carga probatoria por parte del reclamante. Deben tratarse de casos claros de *cybersquatting*. Este sistema no da lugar a argumentos sobre libertad de expresión u otros que pueden plasmarse en una demanda bajo la UDRP. El URS solo permite que el demandante realice una declaración que no rebase las 500 palabras[39].
4. El URS proporciona una especie de derecho al registrante del nombre de dominio demandado, al establecer de forma un tanto tibia que puede defenderse ante dicha reclamación demostrando que el uso del nombre de dominio no es de mala fe. Para ello debe probar, por ejemplo, uno de los siguientes factores:

a. Que el nombre de dominio no vulnera el derecho previo del reclamante porque se trata de un nombre de dominio genérico o descriptivo y está haciendo un uso leal del mismo.
b. Que el sitio web que aloja el nombre de dominio objeto de la reclamación funciona únicamente como tributo, homenaje o crítica de una persona o empresa, que a juicio del examinador constituya un uso leal.
c. Que la «titularidad» del nombre de dominio se justifica con base en un contrato de licencia o uso temporal celebrado entre el titular del derecho anterior y el registrante del dominio, y que dicho acuerdo sigue vigente.
d. Que el nombre de dominio no es parte de una serie de registros abusivos debido a que es significativamente distinto a otros que tiene en su poder[40].

5. El URS también indica que con el propósito de demostrar la buena fe en el uso del nombre de dominio por parte del registrante, el examinador podrá tomar en cuenta que la compra y venta de nombres de dominio y contar con una amplia «cartera» o serie de registros de nombres de dominio no constituyen en sí mismos indicios de mala fe. No obstante, tal comportamiento puede ser abusivo, dependiendo de las circunstancias de la controversia. El examinador deberá analizar cada caso concreto[41].

38 *Vid*. Weslos, David. «Cyberquatting how to win a URS dispute» en http://www.trademarksandbrandsonline.com/article/cybersquatting-how-to-win-a-urs-dispute [visita: 18 de agosto de 2014].
39 Regla 1.2.7 del URS
40 'Reglas 5.8.1 a 5.8.9.
41 Regla 5.9.1.

6. Establece que la venta de tráfico (es decir, conectar los nombres de dominio a las páginas de publicidad para obtener ganancias mediante el pago por *click*) no constituye mala fe en sí misma, en virtud del URS. Sin embargo, tal comportamiento puede ser abusivo en un caso determinado dependiendo de las circunstancias de la controversia. El examinador deberá tener en cuenta: a) la naturaleza del nombre de dominio, b) la naturaleza de los enlaces publicitarios en la página asociada con el nombre de dominio y c) que el uso del nombre de dominio sea en última instancia responsabilidad del registrante[42].

7. El URS sistematiza los casos de reclamos abusivos donde se sanciona el abuso por parte de los titulares de marca, protegiendo así a los registrantes de nombres de dominio del *domain hijacking*. La demanda puede ser considerada como abusiva si el examinador determina, en primer lugar, que fue presentada únicamente con el propósito de acosar, causar retrasos o innecesariamente aumentar el coste de la actividad comercial del registrante, y en segundo lugar, que las reclamaciones u otras afirmaciones no están fundamentadas bajo ninguna legislación existente o norma contenida en el URS, o bien que las alegaciones fácticas carezcan de cualquier apoyo probatorio[43]. En el caso de que se estime lo que este sistema llama *deliberate material falsehood* o «deliberada falsedad material[44], no se podrá participar en un procedimiento del URS por un año[45]. Quien reincida en la presentación de reclamaciones abusivas, no podrá formar parte de un procedimiento URS de forma permanente[46].

Es importante mencionar que el URS cuenta con la posibilidad de apelar la resolución del examinador y enumera con una serie de indicaciones de forma y tiempos para ello[47]. El escrito de apelación debe presentarse dentro de los 14 días desde la resolución y la respuesta a dicho recurso se dará en otros 14 días.

Respecto a esta nueva política de ICANN es imprescindible resaltar que la reclamación debe incluir una prueba de uso de la marca, que puede consistir en una declaración de ese uso en el comercio junto con una muestra o ejemplo de ello. Dicha prueba debe ser certificada y validada por la *Trademark Clearinghouse (*en adelante, *Clearinghouse).* Este requisito es la muestra del vínculo indisoluble entre el URS y esta *Clearinghouse.*

42 Reglas 5.9.2.1 a 5.9.2.3.
43 Regla 11.2.
44 Reglas 11.5. y 11.6.
45 Regla 11.4.
46 Regla 11.5.
47 Regla 12 y ss.

VI. La *Trademark Clearinghouse*

La *Trademark Clearinghouse*[48], se puso en marcha el 26 de marzo de 2013 y tiene como objeto almacenar, validar y difundir información relativa a los derechos de los titulares de marcas. Consta de un archivo central o base de datos en el cual los titulares de marcas pueden solicitar la inscripción de las mismas de cara a su protección frente al lanzamiento de los nuevos gTLD. La inscripción tiene una vigencia de un año, renovable por el mismo periodo de forma indefinida y para efectuar la misma es necesario especificar la clase de productos o servicios que el signo protege, además de indicar el país donde se ha registrado la marca[49].

Este mecanismo protege a las marcas a través de dos vías: mediante un servicio de *sunrise period*[50], o fase preferencial de registro, y con un *claims services*[51], o sistema de alertas[52]. Cuenta con unas directrices que deben seguir las personas físicas o jurídicas que deseen incluir sus marcas en su base de datos[53]. Estas directrices establecen los requisitos de elegibilidad para la inclusión de marcas en la *Clearinghouse*, así como las exigencias para la participación en los servicios de *sunrise period* y *claim services*

48 ICCAN. «What is the Trademark Clearinghouse», http://newgtlds.icann.org/en/about/trademark-clearinghouse/faqs [visita: 18 de agosto de 2014].

49 Regla 4.3.3 de las *Trademark Clearinghouse Guidelines. Vid. Trademark Clearinghouse Guidelines*. Version. 1.1. March 2013 en http://www.trademark-clearinghouse.com/sites/default/files/files/downloads/TMCH%20guidelines%20v1.1_0.pdf [visita: 18 de agosto de 2014].

50 De conformidad con las disposiciones impuestas por la ICANN, esta fase preferencial de registro es obligatoria para todas las nuevas extensiones que permitan registrar nombres de dominio de segundo nivel y debe tener una duración de al menos 30 días. Durante la misma, los titulares de marcas cuentan con la ventaja de poder registrar dominios coincidentes con las mismas bajo el nuevo gTLD correspondiente antes de la apertura del registro de dichos dominios al público en general. Será requisito esencial para los titulares que quieran registrar un nombre de dominio durante el *sunrise period* tener inscritas sus marcas en la *Clearinghouse.* Para ello, el titular de la marca deberá presentar una prueba de uso de la marca. Para la verificación de la prueba de uso, el titular de la marca habrá que entregar una declaración de uso debidamente firmada junto con una muestra o ejemplo de esa utilización. Respecto a las muestras que pueden ser aceptadas para la acreditación de uso, la guía indica que puede tratarse de etiquetas, envases del producto o publicidad o materiales de marketing, como folletos, catálogos, manuales, carteles, comunicados de prensa y capturas de pantalla, *vid*. ICANN, «Sunrise services», http://trademark-clearinghouse.com/content/sunrise-services [visita: 12 de febrero de 2014] y Regla 2 de las *Trademark Clearinghouse Guidelines.*

51 Es el paso siguiente al *sunrise period.* Su objetivo es facilitar a los titulares de las marcas la defensa de sus derechos una vez que las nuevas extensiones entren en funcionamiento. *Vid*. ICANN. «Claim services», http://trademark-clearinghouse.com/content/claims-services [visita: 28 de abril de 2013].

52 ICANN. «What are trademark claims and Sunrise services», http://newgtlds.icann.org/en/about/trademark-clearinghouse/faqs [visita: 25 de abril de 2013].

53 Estas directrices son complementarias a los *Clearinghouse Validation Terms and Conditions*; *vid*. http://trademark-clearinghouse.com/sites/default/files/files/downloads/TMCH terms and conditions - Trademark Holder.pdf [visita: 12 de agosto de 2014].

Cuando una marca registrada esté inscrita en la *Clearinghouse*, el titular de la misma deberá aportar únicamente un código de autenticación para justificar sus derechos para el registro del nombre de dominio, lo que evita la presentación de documentación por cada registro durante este periodo.

La verificación de los datos sobre las marcas incluidas en la base de datos de la *Clearinghouse* respaldará tanto las reclamaciones que pueda haber como los servicios necesarios para el registro de nombres de dominio dentro del *sunrise period* de todas las nuevas extensiones[54].

El servicio del *sunrise period* incluye en primer lugar la generación de un archivo SMD[55], y en segundo, se envían las *Notifications of Registered Names* (NOR) que son notificaciones de registro de nombres a los titulares de marcas o a sus representantes. Dichas comunicaciones sirven para informar durante esta fase preferencial del registro de un nombre de dominio que coincide con una marca incluida en la base de datos[56].

En el caso de que el titular de una marca decida no registrar un nombre de dominio bajo un nuevo gTLD durante el *sunshine period*, la inscripción de dicha marca en la *Clearinghouse* le aportará igualmente ventajas para su defensa mediante el *claim services*. Se trata de un servicio de notificaciones que advierte tanto a los titulares de marca como a los registrantes de un nombre de dominio sobre una posible infracción sobre derechos anteriores. Este servicio funciona dentro de los primeros sesenta días desde que el dominio idéntico al de la marca inscrita haya sido registrado bajo el nuevo gTLD que se trate.

La *Clearinghouse* aceptará y verificará los siguientes derechos de propiedad intelectual: (i) marcas nacionales y regionales[57]; (ii) marcas validadas por los Tribunales de Justicia[58] y; (iii) las marcas protegidas por alguna ley o tratado[59].

54 Regla 1.3. En esta directriz indica que se podrá aceptar y verificar otros tipos de marcas a solicitud de las entidades de registro, pero no indican qué tipo de marcas podrían ser admitidas. Sólo señala que la actuación de la *Trademark Clearinghouse* no se extenderá a otros derechos de propiedad intelectual que no puedan ser integrados en un nombre de dominio, tales como las patentes, los diseños y dibujos industriales, el *know how* y los secretos industriales; *vid*. regla 1.3 de las directrices.

55 La *Clearinghouse Validation Terms and Conditions* indica que estas siglas corresponden al archivo que permite a los titulares de las marcas o sus representantes registrar nombres de dominio que coincidan exactamente con las marcas de la que son titulares o a las que representan, pero no hace ninguna referencia acerca de que respondan a alguna expresión que explique su significado.

56 *Vid*. Regla 3.1 de las *Trademark Clearinghouse Guidelines.*

57 Según las directrices, se considera como marca nacional o regional a la marca registrada en las oficinas nacionales o multinacionales. La marca que se quiera añadir a la base de datos deberá tener efecto nacional y estar vigente al momento de su presentación para su inclusión en la *Trademark Clearinghouse*. Igualmente, señalan que no serán incluidas en la base de datos: 1) las solicitudes de marcas, 2) las marcas registradas que contengan denominaciones de una ciudad, Estado, provincia o región, 3) solicitudes de marca internacional realizadas a través del sistema de Madrid, salvo que la marca base tenga efecto nacional, y 4) las marcas registradas que fueron objeto de nulidad, cancelación, oposición u otros procesos de rectificación. Podrían incluirse en la

Es preciso resaltar que puede inscribirse una marca en la *Trademark Clearinghouse* sin presentar la prueba de uso. La diferencia radica en que si se inscribe la marca incluyendo la prueba de uso, podrá realizar múltiples registros durante el periodo *sunrise* y contará con el sistema de activación de alertas. Si se inscribe la marca sin presentar la prueba de uso, sólo contará con el sistema de activación de alertas.

Deloitte Enterprise Risk Services (Deloitte) y la *International Business Machines (IBM)*[60] son los proveedores de servicio de la *Trademark Clearinghouse*. El primero es el proveedor de servicios de autenticación y

base de datos las marcas notorias o renombradas, las marcas no registradas (en conformidad con el *common law*), las marcas validadas por los tribunales de justicia, las marcas protegidas por la ley o un tratado u otras marcas que constituyan propiedad intelectual. *Vid*., regla 2 (2.2.1) de las *Trademark Clearinghouse Guidelines*.

Como excepción, no se admitirán en la base de datos marcas registradas que incluyan un dominio de primer nivel (TLD), por ejemplo, *icann.org o .icann.* Igualmente, no se incluirán las marcas registradas que comiencen o contengan un «punto», por ejemplo, *deloitte. Vid*. Regla 2.2.5 de las *Trademark Clearinghouse Guidelines.*

58 Según las directrices, se considera una marca validada por un Tribunal de Justicia a aquella que ha sido admitida como tal por un Tribunal u otro procedimiento judicial nacional, como por ejemplo, una marca no registrada o marca notoria o renombrada. No serán incluidas en la base de datos: 1) las solicitudes de marcas, 2) las marcas registradas en un Estado de EE. UU., 3) las solicitudes de marca internacional realizadas a través del sistema de Madrid, y 4) las marcas registradas que fueron objeto de nulidad, cancelación, oposición u otros procesos de rectificación. *Vid*., regla 2 (2.3.1) de las *Trademark Clearinghouse Guidelines.*

Como excepción, no se admitirán en la base de datos cualquier marca legitimada por un Tribunal de Justicia que incluya un dominio de primer nivel como por ejemplo ***icann.org o .icann***. Igualmente, no se incluirá cualquier marca legitimada por un Tribunal de Justicia que comience con un «punto» o contenga un «punto» o bien no contenga ninguna letra, palabras, números o cualquier carácter válido para el sistema de nombres de dominio. Además, no se incluirá cualquier marca reconocida por un Tribunal de Justicia que contenga el nombre de un Estado o ciudad. *Vid*. Regla 2.3.4. de las *Trademark Clearinghouse Guidelines.*

59 La ley o el tratado deberá estar vigente al momento que el titular de la marca solicite la inclusión de la misma en la base de datos. Estas marcas pueden comprender las indicaciones geográficas y las denominaciones de origen. No serán incluidas en la base de datos: 1) las solicitudes de marcas; 2) las marcas notorias y renombradas salvo que estén protegidas por una ley o un tratado; 2) las marcas registradas en un Estado de EE.U; 3) solicitudes de marca internacional realizadas a través del Sistema de Madrid; y 4) las marcas registradas que fueron objeto de nulidad, cancelación, oposición u otros procesos de rectificación. *Vid*., regla 2 (2.4.1) de las *Trademark Clearinghouse Guidelines.*

Como excepción, no se admitirán en la base de datos cualquier marca legitimada reconocida por una ley o un tratado que incluya un dominio de primer nivel como por ejemplo ***icann.org o .icann***. Igualmente, no se admitirán cualquier marca que comience con un «punto» o contenga un «punto», además de cualquier marca que no incorpore ninguna letra, palabras, números o cualquier carácter válido para el sistema de nombres de dominio y tampoco se incluirá, salvo que sea reconocida por una ley o tratado, cualquier marca que contenga el nombre de una región, ciudad o Estado.*Vid*. Regla 2.4.4. de las *Trademark Clearinghouse Guidelines.*

60 Un departamento de Deloitte Bedrifsrevisoren.

validación de marcas, mientras que el segundo es el proveedor de servicios de administración técnica de la base de datos[61].

VII. El URS y su aplicación

1. Caso Facebook

El 21 de agosto de 2013 Facebook Inc. presentó la primera demanda en el marco del URS por considerar que el registro del nombre de dominio facebok.pw era abusivo y vulneraba los derechos de marca de la empresa.

En su reclamación Facebook. Inc. manifestó que es el líder mundial en redes sociales con más de 1110 millones de usuarios registrados en el mundo. Igualmente, mencionó que es el número 1 en el ranking de los sitios web más visitados en el mundo y que en Eslovaquia (domicilio del demandado) ocupa el segundo lugar más tráfico en la Red. Por último, indicó que la empresa tiene numerosos registros nacionales e internacionales con la denominación FACEBOOK incluyendo la marca comunitaria nº 006455687 registrada en octubre de 2008.

Facebook, Inc. también señaló que el nombre de dominio facebok.pw es similar en grado de confusión a su marca FACEBOOK y consideraba que el demandado no tenía derechos ni interés legítimo en el dominio además de que había sido utilizado y registrado de mala fe.

Por su parte, el demandado solo manifestó lo siguiente:

> «*Im was offline, could you please tell me what I have doing? I want removed this domain from my account!*»

Por todo ello, el examinador (Darryl Wilson) en aplicación a los requisitos establecidos en el URS, concretamente 1.2.6.1 al 1.2.6.3. resolvió el asunto a favor de la famosa empresa. En este asunto se refleja que la URS se aplicó en un caso claro y evidente de cybersquatting.

2. Caso Branson

El 27 de febrero de 2014, el famoso empresario Richard Branson presentó demanda URS a través de su empresa *Virgin Enterprises Limited of Geneva* 27 contra *Lawrence Fain of Chicago*. La parte demandante, haciendo uso de las 500 palabras que le son permitidas en este tipo de procedimiento, reclama que el registro del nombre de dominio branson.guru es abusivo y lesiona su

61 Sobre el particular, *vid.* ICANN, «Protecting Trademark Rights in New gTLDs: Selection of Trademark Clearinghouse Service Providers», http://www.icann.org/en/news/announcements/announcement-3-01jun12-en.htm [visita: 18 de agosto de 2014].

derecho de marca. En su declaración aporta los registros de las marcas sudafricanas donde consta como titular y reivindica la relevante reputación del Sr. Branson[62]. Por otra parte, Lawrence Fain no contestó ni alegó nada en su defensa.

El 17 de marzo de 2014, el examinador desestimó la demanda por considerar que el demandante, el conocido empresario Richard Branson no había demostrado, mediante pruebas claras y convincentes, ninguno de los tres elementos que exige el URS, para que el dominio objeto de la demanda, siguiera bloqueado. El examinador señaló que el contenido de la página web que alojaba el dominio branson.guru no incluía ninguna referencia a la demandante, y que no se había presentado ninguna prueba específica que pudiera considerar el registro como de mala fe[63].

3. Caso BBVA[64]

El 14 de marzo de 2014, el Banco Bilbao Vizcaya Argentaria, S.A. (BBVA) presentó demanda URS contra Gandiyorl SL de Gandia, Valencia, por considerar que el nombre de dominio bbva.land era abusivo y lesionaba sus derechos de marca. Por ello, aportó los registros de las marcas de las que es titular, además de hacer constar su relevancia en el sector de las finanzas.

La parte demandante destacó que la página web que se alojaba en el dominio objeto de la reclamación se encontraba en un *parking* y que contaba solo con una serie de anuncios y enlaces de publicidad relacionada con los servicios financieros incluyendo links de competidores de BBVA. Que no otorgó licencia ni autorización para que incorporara su marca en el nombre de dominio. Igualmente, resaltó que la demandada no era conocida por ese nombre y que no había presentado pruebas de tener legítimo interés en el nombre de dominio.

Además, el demandante destacó que el nombre de dominio bbva.land solo ha sido utilizado para visualizar los anuncios de terceros, con enlaces de publicidad relacionados con la industria del demandante. Que lo anterior, era indicativo de mala fe, pues que la parte demandad utilizaba y explotaba la marca para obtener ingresos a través de click.

En este caso, pese a la evidencia de que el nombre de dominio incorporaba la marca del demandante en el dominio, estaba en un *parking* y se utilizaba para alojar una página web que solo tenía anuncios publicitarios relacionados con los servicios financieros y de competidores de la demandante. El 28 de

62 *Vid.* Resolución número FA1402001545807 del *National Arbitrarion Forum URS Final Determination.* Disponible en http://domains.adrforum.com/domains/decisions/1545807D.htm. Visita: 12 de agosto de 2014.

63 *Ibid.*

64 Resolución número FA1403001548656 del *National Arbitrarion Forum URS Final Determination.* Disponible en http://domains.adrforum.com/domains/decisions/1548656F.htm [visita: 12 de agosto de 2014].

marzo de 2014, el examinador resolvió que el demandante no había demostrado de forma *clara y convincente* los tres elementos exigidos por el URS, por ende, el nombre de dominio debía ser devuelto al control del demandando.

Es de llamar nuestra atención que los argumentos de la parte demandada fueron fundamentales para la decisión del examinador. En ellos, la parte demandada declara que la parte demandante tenía el registro de las marcas en casi todas las clases de la clasificación de Niza, en concreto de la 1 a la 42, pero solo demostró el uso de la marca en la clase 36 (operaciones financieras, etc). Que reconocía que BBVA era conocida en el sector bancario. Sin embargo, no era una marca que se utilizara en las 41 clases restantes.

Asimismo, rechazó no tener interés legítimo en bbva.land, pues creía que la extensión .land fue creada para actividades relacionadas con la agricultura, de forma similar como se fue creada .org para organizaciones o .edu para la educación. Además que las siglas «BBVA» obedecían a los servicios que prestaban cuyo nombre es Bellreguart, Beniarjo, Villalonga y Almonines, que son 4 ciudades ubicadas en la comunidad valenciana. Igualmente, destacó que su marca se encontraba protegida en la clase 44 (agricultura, hortalizas, etc), categoría en la que la parte demandante no tenía registrada su marca.

La parte demandada destacó que tiene actividades relacionadas con la extensión .land en cuatro ciudades vecinas de Valencia cuya inicial coincide con las siglas B-B-V-A. Expresó que los criterios que siguieron para el registro del nombre de dominio fueron los siguientes:

1) Verificar que el nombre de dominio bbva.land estaba disponible, si dicho dominio estaba vacante significaba que el demandante no tenía interés en el dominio bajo la extensión .land. 2) leer el aviso donde se informa que la denominación estaba registrada como marca y verificar que BBVA no estuviera incluida en las clases (1 a la 42) registradas por la parte demandante y 3) registrar el dominio.

Por último, la empresa valenciana defendió su postura y negó la mala fe basándose en el hecho de que recibió la demanda una semana después de haber registrado el dominio y que era complicado demostrar buena o mala fe cuando no había dado tiempo de hacer nada. Igualmente, argumenta que lo dicho por BBVA respecto al 1.2.6.3 era falso, ya que la demandante tuvo dos meses (*sunrise period*) para registrar ese dominio. Además, enfatizó que la parte demandante tenía varios procesos URS abiertos pretendiendo que nadie pueda utilizar BBVA y concluyó su defensa diciendo que era falso que estuviera obteniendo ingresos a través del click, ya que la empresa en donde realizó el registro (Godaddy.com) ofrece el *parking* gratuito en espera a la construcción de sito web de su negocio, tal y como se podía mostrar en la captura de pantalla que aportó la parte demandada al proceso URS.

De este caso, se desprende una cuestión muy importante y es aquella que pone nuevamente de relieve el problema del principio de especialidad de la

marca (la coexistencia del derecho de marca) con el sistema de nombres de dominio.

En cuanto al principio de especialidad de la marca, se dice que una marca es especial en el sentido de que sólo se aplica a la categoría de productos o servicios para los que fue creada y registrada. De ahí surge la regla general según la cual una marca no puede registrarse para proteger indeterminadamente cualquier mercancía. Esto quiere decir, al menos en principio, que una misma marca puede ser registrada por cualquier otra persona para distinguir productos de otra clase[65]. Está permitida la coexistencia de marcas idénticas para distinguir productos o servicios distintos, cosa que no puede ocurrir con el nombre de dominio, que por su naturaleza técnica –no puede existir un nombre de dominio igual a otro bajo un mismo TLD– no cuenta con esta capacidad de coexistencia entre las denominaciones iguales registradas como *Second Level Domain* (SLD). Se origina de esta manera un gravísimo problema, pues sólo una de las empresas podrá contar con el nombre de dominio que incorpora su marca, pese a que puede haber distintos titulares de una misma marca.

Este problema existe desde que comenzaron los conflictos con las marcas, y no fue abordada por la UDRP, ni ahora por el URS. Se deja al criterio del examinador casos de este tipo. Sin embargo, esta resolución invita a la reflexión sobre la necesidad de atajar esta cuestión, ya que con la existencia de más extensiones de primer nivel esta problemática crecerá.

Somos conscientes que, en ocasiones, no se puede pretender proteger la marca en todas las extensiones de primer nivel, se presentarán situaciones como la que acabamos de describir. Por ello, consideramos que la ICANN desaprovechó la oportunidad de que el URS diera alguna solución al respecto.

Si la marca es el activo inmaterial más importante de la empresa y el nombre de dominio es el activo digital esencial de una sociedad que quiera ejercer el comercio electrónico ¿por qué no existe un derecho sobre el nombre de dominio? La inauguración de una nueva categoría de bienes intangibles daría cabida a un régimen jurídico del nombre de dominio más completo e incluiría a otros activos electrónicos de gran importancia para la empresa, habida cuenta de que estos bienes forman parte fundamental del patrimonio de las empresas en el ámbito electrónico[66].

Dotar al nombre de dominio de un derecho no significaría desproteger a los titulares de marca, sino todo lo contrario. Éstos obtendrían, además del régimen

65 RANGEL MEDINA, D., «La especialidad de la marca en la jurisprudencia mexicana», *Revista Mexicana de Propiedad Industrial y Artística*, año X, núm. 20, julio-diciembre de 1972, p. 185. En el mismo sentido, *vid*., del mismo autor, *Tratado de Derecho marcario*, México, Libros de México, 1960, p. 153-169, y FERNÁNDEZ-NÓVOA, C., *Tratado sobre derecho de marcas*, Madrid, Marcial Pons, 2001.

66 Para profundizar sobre este tema, *Vid*. LASTIRI SANTIAGO, Mónica. *La comercialización del nombre de dominio*. Marcial Pons, Madrid, 2014.

jurídico que claramente les favorece, un derecho sobre un bien digital, y no una cuestionable extensión del derecho de marca caracterizado por su territorialidad.

4. Caso Aeropostale

El 26 de marzo de 2014, *Aeropostale Procurement Company*, Inc. presentó demanda bajo la URS por considerar que el registro del nombre de dominio aeropostale.uno, inscrito por Michael Kinsey, vulneraba su derecho de marca. Por ello, presentó como prueba los respectivos registros de marca con los que buscaba demostrar que se trataba un registro abusivo, ya que quedaba probado con ello lo establecido en las reglas 1.2.6.1, 1.2.6.2 y 1.2.6.3 del URS. Sin embargo, en los certificados de registro de marca aportados por la parte demandante constaba como titular de cuatro registros *R.H.Macy&Co., Inc* y uno a nombre de *Aeropostale Inc*[67].

Por lo anterior, el 10 de abril de 2014 el examinador desestimó la demanda, señalando que no se habían presentado pruebas que demostraran la relación entre el propietario de la marca y el demandante, ya que las marcas pertenecían a otras entidades.

5. Caso Wolfram

El 8 de abril de 2014, *Wolfram Research, Inc*, presentó demanda URS contra Andrew Davis, por considerar que el registro del nombre de dominio wolfram.ceo era abusivo y vulneraba su derecho de marca.

El 10 de abril de 2014, el examinador resolvió que las marcas objeto de la controversia estaban registradas por *Wolfram Group LLC of Champaign* y no por *Wolfram Research Inc.*[68]. Por ello, desestimó la demanda por considerar que la demandante, no presentó pruebas claras y convincentes que establecieran la relación entre el titular de la marca y *Wolfram Research Inc*.

La empresa volvió a presentar la reclamación bajo el URS, pero esta vez, lo hizo en nombre de *Wolfram LLC of Champaign* y en este segundo intento gano el caso[69]. Es preciso resaltar que esta segunda ocasión no se trató de una apelación, situación que es permitida por el URS. De hecho, técnicamente, no

67 *Vid.* Resolución número FA1403001550933 del *National Arbitration Forum. URS Final Determination.* Disponible en http://domains.adrforum.com/domains/decisions/1550933F.htm. [visita: 12 de agosto de 2014].

68 *Vid.* Resolución número FA14044001553139 del *National Arbitration Forum. URS Final Determination.* Disponible en http://www.udrpsearch.com/naf/1553139. [visita: 12 de agosto de 2014].

69 *Vid.* Resolución número FA1404001554143 del *National Arbitration Forum. URS Final Determination.* Disponible en http://domains.adrforum.com/domains/decisions/1554143F.htm. [visita: 12 de agosto de 2014].

se trató de un «segundo intento», pues la reclamación no fue presentada por la misma empresa.

VIII. Conclusiones

De los casos arriba descritos y de otros[70] se desprende que los examinadores parecen ser más escépticos con las reclamaciones presentadas bajo el URS. La limitación de las 500 palabras en las demandas URS[71] y el alto grado que se exige al titular de la marca en las pruebas que presente, es lo esencial para tener éxito en una reclamación de este tipo. La parte reclamante debe asegurarse que toda la información y documentación presentada sean e*videncia clara y convincente* de que el registrante del nombre de dominio está vulnerando la marca a través del *cybersquatting*. Y se dice *clara y convincente,* ya que si no prueba de forma contundente la infracción, se pierde el caso.

El URS no da lugar a segundas interpretaciones. Se debe determinar con precisión cuáles son los hechos que van aportar a la reclamación y qué elementos de prueba son los que van a usar para dotar de certeza a esos hechos aportados, porque estos hechos y pruebas serán los instrumentos necesarios para establecer los fundamentos que lleven al examinador a bloquear el nombre de dominio objeto de la reclamación. Las pruebas presentadas deben ser concluyentes.

Si se logra afrontar esta fuerte carga de la prueba impuesta al titular de la marca vulnerada dará lugar al bloqueo del nombre de domino y aparecerá la siguiente leyenda en la página web alojada en dicho dominio: *«el nombre de dominio que has introducido no está disponible. Ha sido bloqueado como consecuencia de un procedimiento URS».*

El bloqueo del dominio es la única consecuencia en un procedimiento URS, el dominio no puede ser cancelado o transferido como resultado de una resolución positiva por parte del examinador.

El URS permite a los titulares de marca combatir de forma rápida y menos costosa que la URDP o cualquier acción judicial los casos de *cybersquatting* y es aplicable a todos los nuevos gTLD y para aquellos ccTLD que se adhieran voluntariamente a este mecanismo. No se considera un sustituto de la UDRP sino un complemento de ésta así como de las leyes nacionales relativas a la protección del derecho de marcas.

Es evidente la gran ventaja que representa poder bloquear los nombres de dominio de aquellos *cyberquatters* que aprovechando las nuevas posibilidades que ofrece el registrar un nombre bajo cualquier nuevo gTLD, registra nombres de marcas registradas. Sin embargo, creemos que los registrantes de nombres de dominio siguen desprotegidos respecto a los titulares de marca:

70 Como el caso finn.sexy, *vid.* Resolución número FA1405001558494 del *National Arbitration Forum URS Final Determination.* Disponible en http://domains.adrforum.com/domains/decisions/1558494F.htm. [visita: 12 de agosto de 2014].

71 Regla 1.2.7 del URS

¿Qué sucede si se bloquea un nombre de dominio registrado de buena fe? Tal y como ha sucedido en el caso de bbva.land. Afortunadamente, en este caso, el registrante de este dominio estaba construyendo la página web en donde instalaría su negocio. ¿Qué hubiera sucedido si este ya hubiera realizado inversiones para desplegar su presencia en Internet? Recordemos que el examinador analiza el asunto después de haber bloqueado el dominio.

El URS no hace referencia a ninguna indemnización en caso de que se trate de un registro de buena fe. En la mayoría de los casos, los empresarios registran sus nombres de dominio para tener presencia comercial en Internet. Igualmente, no hay que olvidar que una marca puede ser registrada bajo productos o servicios distintos y un registrante puede tener el mismo derecho e interés legítimo sobre una marca que está registrada en otra clase de la Clasificación de Niza, como se desprende del caso ya mencionado.

Sin lugar a dudas, el URS es una valiosa opción para aquellos titulares de marca cuando se enfrentan a casos claros de ciberocupación. Las primeras decisiones en virtud del URS reflejan el alto grado de exigencia respecto a las pruebas. Por lo tanto, el URS no puede ser apropiado para todos los casos de *cybersquatting*, la URDP y las leyes nacionales permanecerán disponibles para los casos en que el URS no lo permita.

Igualmente, debemos tener en cuenta que la aplicación del URS tampoco puede ser adecuada en todos los casos, pues éste solo bloquea el dominio y no ordena la transferencia del mismo al titular de la marca. Todo dependerá de la estrategia que utilice cada empresa: si desea conservar el dominio en su cartera de activos recurrirá a la UDRP, si simplemente quiere detener la conducta abusiva y no tiene interés en obtener el dominio entonces empleará el URS, tal fue el caso de facebok.pw.

"Análisis de la utilización de virus como diligencia de investigación en el Proyecto de Código Procesal Penal español"

Federico Bueno de Mata*

SUMARIO: I. Introducción: hacia un Gran Hermano mundial. II. Análisis de la regulación sobre utilización de troyanos con fines de investigación policial en el borrador de Código Procesal Penal Español. III. Reflexión final acerca de la idoneidad de la normativa en derecho español. Anexo: borrador Código Procesal Penal Español (Arts. 350 a 352).

Resumen

En este artículo analizamos la regulación otorgada en el proyecto de Código Procesal Penal español, aún pendiente de aprobación, acerca de la utilización de virus con fines investigativos. Para ello, reflexionaremos acerca de la idoneidad y necesidad de esta normativa para el esclarecimiento de determinados. Una regulación muy polémica que choca frontalmente contra una serie de derechos fundamentales y que hace qué debatamos sobre el nivel de control y espionaje que podemos llegar a sufrir por el Estado y plantearnos si realmente el fin siempre justifica los medios.

Palabras clave: Virus. Ciberdelitos. Policía. Proporcionalidad. Derechos fundamentales

Abstract

In this article we discuss the regulation given in the draft about the Spanish Code of Criminal Proceedings, pending approval, on the use of viruses for research purposes. To this end, we reflect on the necessity of this legislation to clarify certain acts. A very controversial regulation that clashes against a number of fundamental rights, and doing what we debate about the level of espionage can be suffered by the State and ask whether or not the end always justifies the means.

Keywords: Virus. Cybercrime. Police. Proporcionality. Fundamental Rights.

Recibido: 28/10/2014 • Aceptado: 30/11/2014

* Profesor Ayudante Doctor. Área de Derecho Procesal. Universidad de Salamanca. España.

I. Introducción: hacia un Gran Hermano mundial

Podemos afirmar que George Orwell y su aclamado *Best-seller* "1984" tenían razón: vivimos en un Gran Hermano planetario. Hace poco más de un año, millones de ciudadanos de distintos puntos del planeta se conmocionaban al conocer la posibilidad de que muchas parcelas de su intimidad podrían haber sido violadas a través de PRISM, un programa secreto de vigilancia electrónica a cargo de la Agencia de Seguridad Nacional (NSA) de los Estados Unidos de América, cuya confidencialidad saltó por los aires gracias a diversos datos filtrados a los periódicos *The Guardian* y *The Washington Post* por Edward Snowden[1], antiguo empleado de la Agencia Central de Inteligencia (CIA) y de la propia NSA. Desde ese momento, Snowden se ha convertido en un prófugo de la justicia estadounidense y continúa en paradero desconocido, aunque todo parece indicar que se encuentra en Rusia.

Pues bien, a partir de ese día sabemos que EE.UU. ha vulnerado constantemente los derechos fundamentales de millones de personas amparándose en sus propias leyes y obviando la jurisdicción de cualquier otro Estado del planeta Tierra, debido a que esta vigilancia tiene por objeto a personas no residentes en EE.UU. y el espectro de datos que controla es amplísimo: desde rastreo de direcciones IP hasta correos electrónicos, perfiles en redes sociales o transferencia de archivos[2].

Pensamos que esta impactante revelación, de la que muchos ingenieros informáticos siempre tuvieron sospecha, ha tenido un impacto triple en el resto de países. Por un lado, un retorno a una posición política de recelo ante la actuación del gigante americano, y por otro, el inicio de un cambio legal a nivel interno en el que muchos países están apostando por crear normativas encaminadas a favorecer el ciberespionaje y en fomentar el control ciudadano a través de técnicas más invasivas, ocasionando así un menoscabo de la libertad y la intimidad de sus ciudadanos. Por último, la sensación de oscurantismo y falta de ética trasladada a los justiciables de a pie ocasiona un evidente estado de desconfianza y genera una pregunta clara: ¿dónde está el límite?

Si estas reflexiones las trasladamos a un plano jurídico, el reto que debemos afrontar se basa en analizar las consecuencias legales que este acontecimiento puede conllevar y focalizar las distintas líneas rojas que dichos preceptos legales no pueden sobrepasar. De esta forma, si centramos nuestra atención en la

1 "Edward Snowden says motive behind leaks was to expose "surveillance state", *The Washington Post*, 9 de junio de 2013. Disponible en http://www.washingtonpost.com/politics/edward-snowden-says-motive-behind-leaks-was-to-expose-surveillance-state/2013/06/09/aa3f0804-d13b-11e2-a73e-826d299ff459_story.html?tid=pm_politics_pop (Fecha de consulta: 19 de junio de 2014).

2 GREENWALD, G., "NSA collecting phone records of millions of Verizon customers daily". The Guardian, de 5 de junio de 2013. http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (Fecha de consulta: 17 de junio de 2014).

normativa española vemos como existen nuevos proyectos de regulación procesal entre las que destaca por encima del resto el borrador del nuevo Código Procesal Penal (CPP), aún pendiente de aprobación[3].

Pues bien, si relacionamos directamente el tema del ciberesespionaje con el articulado de este futurible Código podemos ver cómo los artículos 350 a 352 del mismo contemplan una medida muy polémica, consistente en regular el *malware* y *spyware* como diligencia de investigación policial a través del uso de troyanos y distintos virus espía por parte de los Cuerpos y Fuerzas de Seguridad del Estado para perseguir distintos delitos producidos en Internet.

Muchos de los párrafos de su articulado responden a un contenido ambiguo y polémico que merece ser objeto de estudio y debate, pues debemos analizar hasta qué punto estas actuaciones, aunque gocen de autorización judicial para vulnerar distintos derechos fundamentales por razones de política criminal, podrían ser encuadrables o no dentro de lo que se denomina "*ethical hacking*[4]", ¿realmente todo vale? ¿el fin justifica los medios?, éstas y otras cuestiones serán analizadas a lo largo de este artículo desde un punto de vista procesal.

II. Análisis de la regulación sobre utilización de troyanos con fines de investigación policial en el borrador de Código Procesal Penal Español

A continuación vamos a realizar un análisis de los artículos 350 a 352 del futurible Código Procesal Penal (CPP), en los que se regula la utilización de virus con fines de investigación policial, al tiempo que iremos focalizando las sombras que surgen de su lectura e interpretación, para a su vez intentar dar algo de luz a tan polémico asunto. Para una lectura más ágil, adjuntamos como anexo a esta ponencia el contenido íntegro de los artículos objeto de estudio.

Así, siguiendo un orden cronológico empezaremos por desgranar el primer punto del artículo 350 en el que se regulan los presupuestos para adoptar esta medida. En estas primeras líneas podemos ver como el CPP, tal y como regula anteriormente, confía la instrucción del caso al Ministerio Fiscal, quién deberá "pedir razonadamente" al Tribunal de Garantías la autorización de la medida, por lo tanto será éste último el órgano encargado únicamente de supervisar y cerciorar la idoneidad de las medidas a utilizar. Posteriormente al hablar de forma abstracta de "instalación de software" para el manejo remoto del equipo vemos como no cierra de forma concreta la modalidad de virus a usar por la

3 Texto íntegro del Borrador del Código Procesal Penal disponible en: http://www.fiscal.es/cs/Satellite?c=FG_Multimedia_FA&cid=1247141143692&pagename=PFiscal%2FFG_Multimedia_FA%2FFGE_fckDescarga (Fecha de consulta: 2 de abril de 2014).

4 REYES PLATA, A., "Ethical Hacking", Subdirección de Seguridad de la Información/ UNAM-CERT, disponible en http://www.seguridad.unam.mx/ (Fecha de consulta: 22 de junio de 2014). También definiciones y principios en http://www.ethicalhacking.com/ (Fecha de consulta: 17 de junio de 2014).

policía judicial, por lo que deja en el aire la naturaleza maliciosa del virus informático, aunque al hacer referencia al control y manejo remoto todo nos lleva a pesar que se trata de un *spyware* de naturaleza *zombie*[5].

En primer lugar, debemos manifestar que partimos de un sin sentido, al pensar que hacer público un artículo que podría posteriormente materializarse en un protocolo de investigación concreto e interno de los Cuerpos y Fuerzas de Seguridad del Estado (CFSE) no deja de ser un error, si el objetivo del texto es atajar conductas criminales de "verdaderos expertos en ciberdelincuencia"…Realmente, pensamos que esta normativa, tal y como está redactada, únicamente valdría para detener e incriminar a personas que tengan un control de las TICs medio-bajo, a lo que si a esto le sumamos que, como veremos posteriormente, se podría usar esta medida para ciberdelitos dolosos mayores a 3 años y que el nuevo Código Penal español penará la exportación de *links* o la bajada de contenidos y el "mercadeo" *P2P* en ordenadores situados en España…es realmente el usuario medio el que estaría en el punto de mira.

Igualmente, partimos de que el articulado es innecesario según el enfoque que se ha dado porque ya existen otras medidas que se podrían potenciar y que no dejan de ser menos invasivas y técnicamente menos complejas que el uso de virus espía, tales como la intervención de las comunicaciones, los ciberrastreos o la figura del agente encubierto en Internet. Igualmente, dada la publicidad del borrador del CPP, las personas que se dedican a cometer delitos en la Red a gran escala se pondrán aún más sobre aviso, brindándoles un tiempo que a nivel tecnológico es inmenso y teniendo así la reforma un efecto contraproductivo.

De nuevo la justicia avanza mucho más lenta que la tecnología, y la publicación de este tipo de articulado no deja de constituir una especie de alarma para las personas que se dedican a cometer este tipo de actividades ilícitas a través de la Red. Creemos que el legislador se ha dejado llevar por la imagen idealizada[6] que el ciudadano de a pie tiene de los *hackers*…es decir, asociamos la idea del hacker con una persona solitaria y hermética que se dedica a buscar retos informáticos que superar, cuando realmente dos de los tres ejes de delitos que abarca el borrador del CPP suelen estar perpetrados en su mayoría por grupos criminales coordinados a lo largo de varios países.

Por ello, tenemos que pensar realmente en el caso de que alguien con conocimientos técnicos avanzados, es decir algún ingeniero informático, leyera

5 Vid. VELASCO NUÑEZ, E., *Delitos cometidos a través de Internet. Cuestiones procesales*, Madrid, 2010, págs. 131-137, explica lo que significa un virus con naturaleza *zombie*, en el que infectas a un terminal y puedes usarlo a tu antojo sin que la persona propietaria del mismo perciba ningún cambio.

6 Vid. "Jueces hackers: el nuevo Código Procesal Penal podría permitir que se pirateen móviles y ordenadores", Diario Crítico, Edición del 4 de junio de 2014, disponible en: http://www.diariocritico.com/nacional/troyano/pirateria/codigo-procesal-penal/436117 (Fecha de consulta: 11 de junio de 2014).

el artículo. Sin duda el profesional se pondría rápidamente en la posición de *hacker* y pensaría la forma de eludir el ataque de este tipo de virus.

Normalmente las personas que realicen este tipo de delitos a gran escala no usan su ordenador personal e incluso suelen optar ellos mismos por controlar de forma remota otro tipo de terminales[7] a través de la inclusión de *malware* en diversos equipos informáticos con el fin de crear una red *zombie* de ordenadores y un ejército de *bots* que consumen la acción y así preservar su anonimato…aún así, si esto posteriormente se demuestra mediante un perito informático veríamos como no existiría dolo en este tipo de actuaciones y su conducta podría quedar impune. Todo ello, eso sí, al margen de que los potenciales ciberdelincuentes fabriquen nuevos virus autónomos para atacar distintos bienes jurídicos a distintas escalas: desde arremeter contra cuestiones personales de usuarios hasta llegar a desmantelar la seguridad y la infraestructura del propio Estado.

Una vez expuestas nuestras dudas sobre el enfoque del texto debemos analizar si realmente esta medida es, tal y como reza el texto "*idónea y necesaria para el esclarecimiento del hecho investigado*". Todo eso dependerá de qué hechos queremos investigar con esta medida.

Pues bien, en este caso el texto ve oportuno la utilización de esta medida para tres tipos de delitos para los que realmente existen otras medidas menos invasivas para los derechos fundamentales ya reguladas en España dentro del espectro de técnicas de interceptación de comunicaciones. Igualmente, los delitos deben ser dolosos y el catálogo contemplado sería el siguiente: ciberdelitos con pena de privación de libertad superior a 3 años, infracciones cometidas en Internet a gran escala que afecten a bienes jurídicos concretos como el *grooming*, el *cyberbullying* o el *phishing* y por último, ciberdelitos realizados por organizaciones criminales encaminadas a poner en peligro las infraestructuras tecnológicas del Estado, es decir, ciberterrorismo.

Así las cosas, ¿estamos ante una normativa correcta o realmente deberíamos abogar por una modificación del articulado antes de que el mismo entre en vigor? Claramente optamos por esta segunda opción con una premisa clara: debemos prestar atención a figuras ya contempladas en nuestro derecho interno y al mismo tiempo hacia la Unión Europea para solucionar este tipo de situaciones, al poseer muchas de ellas un alto componente transfronterizo, por todo ello, pasamos a exponer a continuación los razonamientos que nos llevan a sostener esta postura.

De esta forma, si el CPP siguiera adelante y utilizásemos la inclusión de troyanos para investigar ciberdelitos dolosos con pena de privación de libertad superior a 3 años, estaríamos ante una técnica excesivamente invasiva, más

7 Así lo expone también RUIZ HERVÁS, Y., "Troyanos para la investigación policial: el fin no justifica los medios", *El Diario.es*, número del 6 de junio de 2014, http://www.eldiario.es/zonacritica/Troyanos-investigacion-policial-justifica-medios_6_140395962.html (Fecha de consulta: 23 de julio de 2014).

aún cuando el proyecto de Código Penal español prevé penas superiores a tres años para cuestiones de redirección de *links* o descargas de música. Por ello, insistimos es que esta medida acabaría atacando prioritariamente al usuario medio y nos podría llevar a casos en los que un ordenador familiar, utilizado por varios miembros de la familia, podría ser investigado de forma remota e integral, vulnerando la intimidad del resto de usuarios, hayan realizado esas descargas o no[8].

Por todo ello proponemos para este primer punto una intervención que responda a los principios de proporcionalidad y necesidad a través de la regulación genérica ya establecida para la "interceptación de comunicaciones" a través del polémico programa SITEL (Sistema Integrado de Interceptación Telefónica), utilizado por los CFSE.

En España, la intervención de las comunicaciones consiste en la restricción del derecho fundamental al secreto de las comunicaciones contenido en el art. 18.3 de la Constitución[9], efectuada por una resolución judicial motivada. En este sentido, la problemática procesal que plantea la interceptación de esta figura en España es triple, por un lado los problemas de competencia territorial, en segundo lugar el fenómeno de la interceptación de esta figura y por otro los problemas de autoría y recepción[10].

En el orden jurisdiccional penal, las infracciones penales producidas a través de comunicaciones electrónicas desde distintos dispositivos plantean la situación de que, en muchas ocasiones, entre el lugar en el que el sujeto ejecuta el comando que activa el programa y el lugar en el que se produce la ofensa al bien jurídico exista, una notable distancia geográfica, posibilitando así que el resultado ofensivo al bien jurídico no se produzca en un único lugar[11]. Por tanto necesitaríamos una reforma con carácter previo a la solución acerca de qué órgano judicial ha de asumir el conocimiento de un determinado asunto resulta obligado ver si el hecho debe entenderse ejecutado o no en los límites de la jurisdicción española siendo partidarios de la teoría que dice que el delito sería cometido en todas las jurisdicciones y que por tanto cualquiera de los órganos jurisdiccionales tendría competencia en el asunto[12].

8 En este sentido también se manifiesta TEJERINA, O., Defensora del Internauta en España en el artículo publicado en http://www.internautas.org/html/7604.html (Fecha de consulta: 19 de julio de 2014).

9 GIMENO SENDRA "La intervención de las comunicaciones" *Diario La Ley, Nº 7192*, Sección Doctrina, 9 Jun. 2009, Año XXX, Ref. D-210, Editorial LA LEY.

10 BUENO DE MATA, F. "La interceptación de los e-mails", *Revista Justicia*, 2009, págs. 5 y ss.

11 MARCHENA GÓMEZ, M. "Dimensión jurídico-penal del correo electrónico", Diario La Ley Nº 6475, 4 de Mayo de 2006, págs. 15 y ss.

12 La Sala Segunda del Tribunal Supremo, en su Acuerdo de pleno no jurisdiccional, Sala General, fechado el día 3 de marzo de 2005, proclamó que "*el delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo. En consecuencia, el Juez de*

Del mismo modo, tampoco existe una regulación sobre los datos externos de los correos electrónicos, la custodia y destrucción de los soportes magnéticos o telemáticos, el valor probatorio de la prueba inconstitucionalmente obtenida en estos casos específicos, regulación para las personas jurídicas, la ausencia del tiempo máximo de intervención[13] o una regulación específica para el programa espía utilizado por la policía judicial: SITEL[14]. Por lo que realmente sería mucho más efectivo solucionar todas estas lagunas en el próximo CPP antes de apostar por una normativa nueva.

Por supuesto, no podemos confundir SITEL con otras herramientas conocidas a nivel mundial como PRISM, pues su alcance y objeto de actuación es muy reducido, al interceptar únicamente comunicaciones electrónicas dentro de la extensión y límites territoriales establecidos para la jurisdicción española. En referencia a la laguna legal que plantea su uso, se puede constatar por declaraciones políticas que el programa nació en 2001 y no fue hasta la ley ordinaria 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (LCDCE), cuando obtuvo un manto legal tardío e insuficiente. En este sentido, la regulación se debería dar siempre por una ley orgánica, es decir por mayoría absoluta, y no una ley ordinaria, al limitar derechos fundamentales.

En segundo lugar, sobre los temas que afectan a bienes jurídicos especialmente protegidos como es la distribución de imágenes pornográficas de menores de edad o las estafas a gran escala en el comercio electrónico, creemos que también existen medidas más efectivas ya contempladas cuando el sistema informático se encuentre situado en territorio sobre el que se extienda la jurisdicción española.

Por un lado, en primer lugar para los delitos de *grooming* o *cyberbullying*, tal y como llevamos apostando años atrás[15], pensamos que la potenciación de

cualquiera de ellas que primero haya iniciado las actuaciones procesales será en principio competente para la instrucción de la causa" La solución propugnada permite optar por el doble criterio de ubicuidad, entre el lugar de ejecución y el lugar de resultado.

13 Como referencia citar que de conformidad con lo dispuesto en el art. 579.3 el plazo de duración de las intervenciones telefónicas, salvo solicitud de prórroga, no puede ser superior a tres meses.

14 Vid. Para profundizar más sobre SITEL y la interceptación de las comunicaciones BUENO DE MATA, F., MARTÍN RUANI, H. y VARGAS BASILIO, A., "Interceptación y monitoreo de correo electrónico", *Diario El Dial*, 2012, págs. 4 y ss.

15 BUENO DE MATA, F., "El agente encubierto en Internet: mentiras virtuales para alcanzar la justicia", *Los retos del Poder Judicial ante la sociedad globalizada. Actas del IV Congreso Gallego de Derecho Procesal (I Internacional) A Coruña, 2 y 3 de junio de 2011,* PÉREZ-CRUZ MARTÍN, A. (dir.), FERREIRO BAAMONDE, X. (dir). A Coruña: Universidade, 2012, págs. 295-306. Los "ciberrastreos" estaban pensados para investigar intercambio de archivos en redes P2P, como *Emule*, *Kaaza* o *Elephant*, pero ahora necesitamos otro tipo de investigación más personal y directa, valiéndonos de las ventajas aportadas por la figura de los agentes encubiertos en Internet

la figura del agente encubierto en Internet se vuelve algo preceptivo e imprescindible a nivel nacional.

La figura del agente encubierto para infiltraciones en terrenos físicos, encuentra su regulación en el art. 282 bis LECrim, gracias a una reforma de la Ley de Enjuiciamiento Criminal en materia de perfeccionamiento de la actividad investigadora relacionada con el tráfico ilegal de drogas y otras actividades ilícitas graves, efectuada por Ley Orgánica 5/ 1999, de 13 de enero. El problema es que dicho artículo establece un *numerus clausus*[16] o enumeración tasada de delitos para su uso, lo que impediría su uso en delitos cometidos en la Red. Aún así, a finales del mes de marzo de 2011 el Senado aprobó regular la figura del agente policial encubierto en Internet en investigaciones contra la pornografía infantil y la pedofilia[17].

Por todo ello, con el avance constante que tiene la tecnología, consideramos un error realizar una lista tasada de delitos a los que hacer frente con esta figura y nos decantaríamos más por establecer aquí un sistema de *numerus apertus* basado en categorías de delitos y no en figuras concretas; por lo que estaríamos hablando siempre de "compartimentos abiertos", para evitar de este modo clasificaciones a que queden rápidamente desfasadas. Así, si extrapolamos el concepto del agente encubierto en el terreno físico y lo llevamos al plano virtual, podríamos definir al agente encubierto en Internet como un empleado o funcionario público[18] que, voluntariamente, y por decisión de una autoridad judicial, se infiltra en la Red con el fin de obtener información sobre autores de determinadas prácticas ilícitas producidas a través de la Red, que causen una gran repulsa y alarma a nivel social. Cuestiones distinta sería valorar, al igual que con los virus, la técnica basada en el engaño y en la ocultación de la verdadera identidad con fines de investigación…una cuestión de *ethical hacking* que creemos plenamente justificada por la naturaleza concreta del delito a investigar y el bien jurídico lesionado relacionado con personas especialmente vulnerables como los menores de edad.

Ahora bien, dentro de este mismo segundo bloque, cuando los delitos anteriores adquieren el carácter de transfronterizos, al conllevar por su propia naturaleza una gran distancia geográfica entre el lugar de comisión y el lugar de lesión como en los casos de *phising*; optaríamos por redirigir la investigación a nivel europeo gracias al nuevo Centro Europeo Contra el Cibercrimen[19], EC3,

16 Vid. RIFÁ SOLER, J. M., se cuestiona si el listado recoge *numerus apertus o clausus*, en "El agente encubierto o infiltrado en la nueva regulación de la LECrim.", *Poder Judicial*, núm. 55, pág. 161; nosotros entendemos que con la actual redacción es una lista cerrada y tasada.

17 Vid. http://www.tecnoupdate.com.ar/2011/03/21/espana-agentes-encubiertos-en-internet-contra-la-pedofilia/ (Fecha de consulta: 13 de Abril de 2011).

18 BUENO DE MATA, F., "Un centinela virtual para investigar delitos cometidos a través de las redes sociales: ¿Deberían ampliarse las actuales funciones del agente encubierto en Internet?", *El proceso penal en la sociedad de la información: Las nuevas tecnologías para investigar probar el delito*, coord. PÉREZ GIL, J., Madrid, 2012, págs. 311 y ss.

19 Vid. https://www.europol.europa.eu/ec3 (Fecha de consulta: 3 de abril de 2014)

con sede en la Haya y que empezará a funcionar en enero de 2015 siendo dirigido por la Oficina Europea de Policía, Europol. Ahora bien, hemos de reconocer que el articulado sí contempla el recurso a los mecanismos de cooperación internacional cuando los equipos no se encuentren en España al regular que *"se instarán las medidas de cooperación judicial internacional en los términos establecidos por la Ley, los Tratados y Convenios internacionales aplicables y el derecho de la Unión Europea"*, pero pensamos que debe ser a la inversa, un texto europeo que se transpusiera a la normativa interna de los Estados.

¿Qué nos lleva recurrir a este nuevo instrumento de cooperación judicial internacional? Al encontrarnos ante delitos con un gran carácter transfronterizo y analizando el carácter bipolar de la norma española, ya que por un lado se configura como un método excesivamente lesivo para los derechos fundamentales de los potenciales investigados por un lado, pero que acota la investigación únicamente a terminales que se encuentre en territorio español por otro; pensamos que para detener las acciones delictivas a gran escala es necesario que la Comisión Europea colabore para poder ampliar la capacidad analítica y operacional en investigaciones de este tipo. En este sentido, el EC3 nace con la idea de constituir un instrumento de coordinación en el terreno de los delitos informáticos y como centro de apoyo operativo y de investigación forense a nivel europeo[20], puesto que la lesión de bienes jurídicos en ciberdelitos de tal magnitud puede producirse en multitud de Estados miembros, con distintas jurisdicciones y normativas internas que pueden obstaculizar la investigación y posterior detención de los presuntos autores.

Según sus propios promotores, el EC3 proporcionará soporte operacional a los países de la UE, dando un mayor acceso a la experiencia técnica en las investigaciones conjuntas y podrá así fomentar la puesta en común de recursos de cada Estado miembro en la prevención del cibercrimen, ésta será la única manera de desmantelar redes organizadas de este tipo, gracias a una estructura europea capaz de atajar un problema de tal envergadura.

Pues bien, tras analizar los dos primeros bloques para los que está destinada la futura normativa, solo nos atreveríamos a preservar el precepto, tras una oportuna y detallada regulación mucho más específica garantista, su aplicación en casos de ciberterrorismo tal y como pretendió en su día hacer Alemania, ya que posteriormente el Tribunal Constitucional alemán declaró inconstitucional la norma, al considerarla, tal como apunta ORTIZ PRADILLO, contraria *"al derecho fundamental a la garantía de confidencialidad e integridad de los equipos informáticos"*[21]. Únicamente apostaríamos por su mantenimiento,

20 Vid. https://www.europol.europa.eu/ec3/infographic (Fecha de consulta: 5 de abril de 2014)

21 ORTIZ PRADILLO, J. lo apunta en un artículo con gran impacto, "La policía podrá usar troyanos para investigar ordenadores y tabletas", *periódico El País*, de 3 de junio de 2014,

al ser un problema nacional ante el que la población española está especialmente sensibilizada, siempre que la misma fuera fruto de una transposición de una Directiva europea a derecho interno, pues insistimos en que estos problemas se deben resolver, dada a su trascendencia desde un punto de vista normativo e institucional superior.

En este sentido, al igual que la tecnología evoluciona de una forma vertiginosa, la capacidad de adaptación por parte de las bandas terroristas es vertiginosa. El uso de las nuevas tecnologías como instrumento para cometer atentados y como elemento de ataque es una realidad inminente con una enorme proyección de futuro, ya que, por un lado los ataques crecen desmesuradamente año a año y sus autores, en la mayor parte de los casos, son personas jóvenes con gran poder de amoldarse a los cambios tecnológicos, lo que aviva el peligro[22].

Consideraríamos actos propios de ciberterrorismo[23] el uso de las TICs como acción del delito y no como instrumento o elemento de apoyo a una infraestructura criminal. Por tanto, esta convergencia del ciberespacio con el terrorismo podría ser definida como el ataque premeditado y políticamente motivado contra información, sistemas, programas y datos informatizados relativos a la integridad y la seguridad del Estado por parte de grupos terroristas. En conclusión, optaríamos por abogar igualmente por una normativa europea para el ciberterrorismo a nivel internacional.

Por último, debemos hacer una referencia a una parte concreta del articulado centrado en los deberes de colaboración de entidades personas externas que se regulan en los artículos 351 y 352.

Así, en el artículo 351 vemos como existe una obligación por parte de los proveedores de acceso o servicios telemáticos y los titulares o responsables del sistema informático a facilitar los datos e información recogidos en su sistema que puedan ser objeto de examen y visualización. Cuestión plenamente razonable, y que compartimos, siempre que se actúe caso por caso y no se deje abierta la puerta a un filtrado de información periódica, pues entonces estaríamos repitiendo a pequeña escala el caso de la NSA.

Pero la polémica se suscita con la llegada del art. 352. 2 al regular que *"Las autoridades y los agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos*

disponible en http://sociedad.elpais.com/sociedad/2013/06/03/actualidad/1370289646_865495.html (Fecha de consulta: 3 de junio de 2014).

22 VELASCO NÚÑEZ, E. "Aspectos procesales de la investigación y de la defensa en los delitos informáticos", *La Ley*: *Revista jurídica española de doctrina, jurisprudencia y bibliografía*, ISSN 0211-2744, Nº 3, 2006, págs. 1857-1864.

23 Vid. BUENO DE MATA, F. "Ciberterrorismo: tratamiento procesal y penal del terrorismo del futuro", Estudios actuales en Derecho y ciencia política, coord. CARRIZO GONZÁLEZ-CASTELL, A., 2013, págs. 313-323

en el mismo que facilite la información que resulte necesaria para el buen fin de la diligencia". Lo que nos transporta a una situación en la que todo está permitido, un "todo vale" para que la diligencia acabe bien y en el que se ve claramente que el fin justifica los medios, ya que con la denominación "cualquier persona" se desprenden dos efectos negativos inmediatos. En primer lugar, se desvalora o se reconoce como insuficiente la capacitación técnica de la policía judicial en términos de investigación policial, cuando existen unidades concretas con miembros con años de especialización que han sido formados para tal fin y están en constante reciclaje y capacitación, por lo que a nivel publicitario y de imagen exterior no creemos que nos haga ningún bien y, en segundo lugar, ¿qué perfil tiene esa persona? Al hablarse de un cualquier no se acota la identidad de ese sujeto, ¿se está hablando de un ingeniero informático profesional? O por el contrario ¿se abre la puerta al fichaje de *hackers* que actúen sin fines éticos e incluso criminales? Preguntas retóricas que a todas luces hacen urgente la clarificación de este apartado si la norma llegara a entrar en vigor.

III. Reflexión final acerca de la idoneidad de la normativa en derecho español

Debemos dejar claro que partimos de un futurible, un Código Procesal Penal que si tenemos en cuenta la fecha en la que nos encontramos, y a sabiendas de que las próximas elecciones serán a finales del 2015, puede que no cumpla con los plazos de tramitación parlamentaria, a no ser que se opte por introducir reformas parciales que gocen de trámites más ágiles y tengan por objeto la regulación de esta diligencia de investigación.

Al margen del tema temporal y centrándonos en el análisis del borrador, vemos como por todo lo expuesto anteriormente, queda claro que no compartimos la redacción de los artículos 250 a 252 del CPP, ya que como hemos advertido, parte de un planteamiento desafortunado al ir enfocado a perfiles y tipos penales heterogéneos con un campo de actuación geográfico limitado. Así creemos que la normativa, tal y como está planteada, afectaría tanto a ciudadanos con conocimientos informáticos básicos, al imponer la medida para ciberdelitos dolosos mayores a 3 años como a cibercriminales y organizaciones internacionales encargadas de cometer delitos a gran escala en la Red, siempre que el terminal desde el que se cometieran los hechos estuviera situado en España. Igualmente existen cuestiones morales y éticas que chocan directamente con el uso de estas técnicas como son la creación de virus por parte de las propias autoridades o la contratación de *hackers* para preservar el buen fin de la diligencia…trasladando a la sociedad el mensaje de que el fin siempre justifica los medios.

Si unimos todas estas incógnitas a la creencia basada en que la autoridad judicial que permita el hipotético registro se encontraría con claros y continuos problemas de motivar la idoneidad, necesidad y proporcionalidad, cuando, como

hemos visto, existen alternativas menos lesivas para los derechos fundamentales de los investigados en la regulación nacional y que pueden resultar igual de eficaces de cara al fin perseguido, que no es otro que imputar determinados hechos delictivos a sus presuntos autores en el mundo del ciberespacio, por lo que el articulado acabaría poseyendo un corto recorrido.

De esta forma, descartamos de raíz el uso de *spyware* por parte de los CFSE para infracciones cometidas por particulares, al pensar que no se ajusta, dado el perfil criminal de los presuntos autores así como de la entidad de los delitos, a los principios de necesidad y proporcionalidad, manteniendo para estos casos lo ya regulado para la interceptación de comunicaciones en la normativa española, aunque eso sí, tratando de hacer frente a los problemas que lleva arrastrando la normativa desde hace más de una década, por lo que se solicita su urgente reforma.

En segundo lugar, para los casos de delitos en redes sociales, foros e incluso tráfico de imágenes pedófilas o estafas electrónicas, siempre que las mismas se comentan en la jurisdicción española vemos viable la potenciación de la figura del agente encubierto en Internet y no el uso de *malware*; mientras que si tienen un carácter transfronterizo lo ideal sería acudir al apoyo de fuerzas policiales europeas gracias a los mecanismos diseñados por EUROPOL y el Centro Europeo contra el Cibercrimen.

Todo esto nos lleva a demandar una Directiva europea sobre investigación policial para delitos cometidos a través de Internet, obligando en este caso a los distintos Estados Miembros a transponer la regulación a su Derecho interno e incorporar en ella las particularidades que crea oportunas, como puede ser en el caso español, dada su historia reciente, a implementar estrategias más invasivas como es el caso del uso de *malware* en casos de ciberterrorismo.

Para finalizar, debemos reconocer el carácter transgresor de la normativa al volver a agitar el debate sobre los límites entre el uso de medios de investigación basados en espionaje electrónico y los derechos fundamentales de los ciudadanos. Está claro que la justicia debe modernizarse pero no a cualquier precio, si introducimos preceptos limitativos de estos derechos nos toparemos de frente con la Carta Magna, que servirá como freno a la instauración de un estado policial y al monitorio de nuestra intimidad por los poderes públicos.

Internet es un gigante de dimensiones ingobernables, un "Goliat" ante el que no nos podemos enfrentar de forma individual, país por país, en la figura de "David". No es la hora de realizar regulaciones nacionales que permitan el ciberespionaje sino el momento de unificar esfuerzos entre los Estados de todo el mundo para impulsar regulaciones europeas y mundiales en la lucha contra los crímenes que se cometen en la Red.

ANEXO: BORRADOR CÓDIGO PROCESAL PENAL ESPAÑOL (ARTS. 350 A 352)

Artículo 350.- Presupuestos

1.- El Tribunal de Garantías podrá autorizar, a petición razonada del Ministerio Fiscal, la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que la medida resulte proporcionada para la investigación de un delito de especial gravedad y sea además idónea y necesaria para el esclarecimiento del hecho investigado, la averiguación de su autor o la localización de su paradero.

2.- La resolución judicial que autorice el registro, además de motivar la idoneidad, necesidad y proporcionalidad, deberá especificar:

a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios de almacenamiento de datos informáticos o bases de datos y datos informáticos almacenados objeto de la medida.
b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información.
d) Los agentes autorizados para la ejecución de la medida.
e) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.
f) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.

3.- Cuando los agentes que lleven a cabo el registro remoto tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo, pondrán este hecho en conocimiento del Ministerio Fiscal quien podrá solicitar del Tribunal de Garantías una ampliación de los términos del registro.

4.- El registro remoto sólo podrá ser autorizado cuando los datos se encuentren almacenados en un sistema informático o en una parte del mismo situado en territorio sobre el que se extienda la jurisdicción española. En otro caso, se instarán las medidas de cooperación judicial internacional en los términos establecidos por la Ley, los Tratados y Convenios internacionales aplicables y el derecho de la Unión Europea.

Artículo 351.- Deber de colaboración

1.- Los proveedores de acceso o servicios telemáticos y los titulares o responsables del sistema informático o base de datos objeto del registro están obligado a facilitar a los agentes investigadores la colaboración precisa para la práctica de la medida y el acceso al sistema. Asimismo, están obligados a facilitar la asistencia necesaria para que los datos e información recogidos puedan ser objeto de examen y visualización.

2.- Las autoridades y los agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria para el buen fin de la diligencia.

Artículo 352.- Forma

Las actuaciones referentes al examen y registro a distancia de equipos, dispositivos o sistemas informáticos o electrónicos se sustanciarán en pieza separada y en régimen de secreto, sin necesidad de declaración expresa, el cual tendrá una duración máxima de diez días.

Criterios básicos en Europa y propuestas respecto del tratamiento de la libertad de expresión e información en Internet*

Lorenzo Cotino Hueso**

SUMARIO: I. Premisas jurisprudenciales de las que partir. 1. La libertad de expresión e información protege la difusión de opiniones e informaciones por cualquier sujeto a través de cualquier canal, modo o medio. 2. Apoyos jurisprudenciales a la tesis de la necesidad de extender la protección especial de los medios de comunicación clásicos a los prestadores de servicios. 3. Una inercia jurisprudencial negativa: se reserva a los medios de comunicación clásicos la protección constitucional más intensa. II. Lineamientos jurisprudenciales en Europa relativos la libertad de expresión e información en Internet. 1. El caso Ahmet Yýldýrým c. Turquía de 2012, primera sentencia del TEDH que aborda frontalmente la protección de la libertad de expresión en Internet y las garantías de legalidad. 2. La preocupante sentencia del TEDH en el caso Delfi vs Estonia de 2013 y la responsabilización de los intermediarios por los contenidos que alojan. 3. Diversos criterios sobre la libertad de expresión e información por el TJUE. 4. El "olvido" de la libertad de expresión en razón del derecho al olvido. La sentencia del TJUE del caso Google vs AGPD de 2014. III. Para concluir. La necesidad que el legislador democrático asuma su papel para proteger las libertades informativas y otros derechos fundamentales en Internet.

Recibido: 16/11/2014 • Aceptado: 25/11/1014

* El presente estudio se realiza como investigador principal del Proyecto MINECO "Régimen jurídico constitucional del Gobierno 2.0-Open government. Participación y transparencia electrónicas y uso de las redes sociales por los poderes públicos" (DER2012-37844), así como Miembro del Grupo de Investigación, Derecho en Tecnologías de la Información, la Comunicación y Cyber Law (G-TICCY) de la Universidad Católica de Colombia. El presente texto trae causa de la ponencia presentada al XVIII Congreso Iberoamericano de Informática y Derecho. www.fiadi.org

** Profesor titular de Derecho Constitucional acreditado como catedrático. Universidad de Valencia. Coordinador de la Red de especialistas en Derecho de las Nuevas Tecnologías de la Información y Comunicación (TICs) www.derechotics.com

Resumen

Frente a una inercia jurisprudencial negativa, el autor reafirma que la libertad de expresión e información no queda reservada a los tradicionales medios de comunicación y aboga por el reconocimiento de la garantía institucional que tradicionalmente ha reforzado a estos medios, a los grandes prestadores e intermediarios. Se analizan las líneas jurisprudenciales y se destacan las decisiones del Tribunal Europeo de Derechos Humanos, caso Delfi vs. Estonia (2013) en materia de responsabilidad por contenidos ilícitos en Internet y la sentencia del Tribunal de Justicia de la Unión Europea, caso Google vs. España (2014) sobre el derecho al olvido; se critica que esta sentencia "olvida" la libertad de expresión e información en Internet. Ambas sentencias parecen expresar un giro hacia un Internet más controlado. Para concluir, se sostiene que el legislador no puede eludir más su responsabilidad y dejar totalmente en manos de los tribunales estas cuestiones.

Palabras clave: Jurisprudencia. Libertad de expresión. Internet. Redes sociales. Derecho al olvido. Protección de datos. Responsabilidad de intermediarios.

Abstract

Faced with negative case law inertia, the author reaffirms that freedom of speech and information is not exclusively for the traditional mass media, and advocates the acknowledgement of the institutional guarantee that traditionally has reinforced the mass media to large providers and intermediaries. Case law guidelines on decisions of the European Court of Human Rights in Delphi vs. Estonia's (2013) regarding liability for illegal Internet content, and the European Court of Justice decision in Google vs. Spain (2014) on the right to be forgotten are analyzed, and highlighted. It is criticized that this decision "forgets" the freedom of speech and information on Internet. Both decisions seem to reveal a shift to a more controlled Internet. In conclusion, it is argued that the legislature cannot avoid its responsibility and leave these issues completely in the hands of the courts.

Keywords: Case Law. Freedom of Speech. Internet. Social Networks. Right to be forgotten. Data protection. Liability of intermediaries.

I. Premisas jurisprudenciales de las que partir

1. La libertad de expresión e información protege la difusión de opiniones e informaciones por cualquier sujeto a través de cualquier canal, modo o medio

Salvando muy destacadas firmas, que por lo general hemos trabajado de forma conjunta[1], no son muchos los autores en la literatura científica española que hayan mostrado interés por las libertades en la Red[2], a diferencia de la siempre más rentable atención del fenómeno de la protección de datos.

1 Me permito recordar algunos de mis trabajos especialmente como coordinador, publicados en la materia, entre otros, "Algunas claves para el análisis constitucional futuro de las libertades públicas ante las nuevas tecnologías (con especial atención al fenómeno de los "*blogs*")", en AA.VV. *Estudios jurídicos sobre la sociedad de la información y nuevas tecnologías*, Facultad de Derecho de Burgos, Burgos, 2005, pags. 51-76. También, "Nuestros jueces y tribunales ante Internet y la libertad de expresión: el estado de la cuestión", en COTINO HUESO, Lorenzo (Coord.), *Libertad en Internet…*, cit. así como el estudio introductorio a la obra. "Nuevas tecnologías, desafíos y posibilidades para la libertad de expresión", publicación de la Ponencia en las III Jornadas de Derecho constitucional "Constitución y libertad de expresión", Fundación Giménez Abad-Cortes de Aragón- Uned, Barbastro (Huesca) 7-8 de noviembre de 2008, disponible en http://goo.gl/cBkEa (Consulta: 10 de noviembre de 2014).

He coordinado obras monográficas como COTINO HUESO, Lorenzo (Coord.), *Libertades, democracia y gobierno electrónicos*, Comares (Colección Sociedad de la Información, nº 9), Granada, 2006: *Libertad en Internet. La Red y las libertades de expresión e información*, Tirant lo Blanch, Valencia, 2007; *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías*, PUV (Publicaciones de la Universidad de Valencia), Valencia, 2011,CORREDOIRA Y ALFONSO, Loreto y COTINO HUESO Lorenzo (eds.) *Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales*, Centro de Estudios Políticos y Constitucionales, 2013.

2 En España, hay que destacar los trabajos iniciales de FERNÁNDEZ ESTÉBAN, María Luisa, *Nuevas Tecnologías, Internet y Derecho Fundamentales*, Mc-Graw Hill, 1998, así como los numerosos trabajos de BOIX PALOP, Andrés, "Pluralismo y libertad de expresión en la Red", publicado en *Revista española de Derecho constitucional*, nº 65, mayo-agosto 2002, págs. 133-180, accesible en http://www.uv.es/aboixp (Consulta: 10 de noviembre de 2014), así como en BOIX PALOP Andrés y LÓPEZ GARCÍA, Guillermo, "Derecho y cuarto poder en la era digital", en *Revista de Estudios Políticos (nueva época)*, Núm. 130, Madrid, octubre-diciembre (2005), págs. 73-108 y en "Soporte digital, autoría e industria cultural", *Revista de Estudios Políticos (nueva época)*, Núm. 131, Madrid, enero-marzo (2006), págs. 53-86. Asimismo, una monografía de la cual son editores, *La autoría en la era digital: industria cultural y medios de comunicación*, Valencia, Tirant Lo Blanch, 2006. Fue un clásico, VILLATE, Javier: "La libertad de expresión en Internet: Retos y amenazas", Versión 1.0, Borrador de trabajo sobre la libertad de expresión en la Red y los sistemas de filtrado, por Javier Villate. Documento presentado en la comparecencia de David Casacuberta, presidente de FrEE , ante la Comisión Especial del Senado sobre Internet, 16 de junio de 1998, acceso en internet. Es sencillo y muy destacable FERNÁNDEZ RODRÍGUEZ, José Julio, *Lo público y lo privado en Internet*. *Intimidad y libertad de expresión en la Red*, UNAM, Méjico, 2004. También hay que mencionar especialmente los trabajos de, CORREDOIRA y ALFONSO, Loreto *Los retos de la información en Internet. Las libertades de acceso y difusión*. Seminario Complutense de Telecomunicaciones e Información. Madrid, diciembre, 1998 y el libro colectivo, *La libertad de información. Gobierno y arquitectura de*

Frente a las negativas corrientes que luego se indican, como he sostenido en otros lugares desde hace tiempo, las libertades informativas se reconocen a toda persona (aunque no sea empresa de comunicación o periodista) que emita información veraz o exprese opiniones, así como a la colectividad que las recibe. No se trata de una afirmación nueva, puesto que lo cierto es que antes de Internet, ya se afirmaba que las libertades informativas eran de todos los ciudadanos. En aquellos tiempos estas afirmaciones, si se me permite, *salían gratis*. Así, el Tribunal Supremo de los Estados Unidos de América diría que "*la libertad de la prensa es el derecho de un solo panfleto... al igual que el de la más importante publicación metropolitana"*[3]. La sentencia Engels del Tribunal Europeo de Derechos Humanos (TEDH), de 8 de junio de 1976 afirmó que "*Está claro que la libertad de expresión garantizada por el artículo 10 [del CEDH que reconoce la libertad de expresión] es aplicable a todas las personas*" (Apartado 100). Como luego se insiste, el Tribunal de Justicia de la Unión Europea (TJUE) en 2008[4] afirmó que la importancia de la libertad de expresión impone interpretar ampliamente la noción de "periodismo" hacia "*toda persona que ejerza una actividad periodística*" (nº 58). Se señala que difundir información con ánimo de lucro no excluye que se trate de fines periodísticos, "*el soporte en el que se transmiten los datos, clásico como el papel o las ondas de radio, o electrónico como Internet, no es determinante para apreciar si se trata de una actividad "con fines exclusivamente periodísticos*" (nº 60)[5], de manera que las "actividades

Internet, Universidad Complutense, Madrid, 2001, y los trabajos de esta autora en obras que he coordinado. Destacan desde el inicio los diversos estudios de GARCÍA MORALES, María Jesús, "Nuevas tecnologías y libertad de expresión: regulación, autorregulación y filtros en Internet", en COTINO HUESO, Lorenzo (Coord.), *Libertades, democracia y gobierno electrónicos*, Comares (Colección Sociedad de la Información), Granada, 2005 y algunos trabajos en CASANOVAS, Pompeu *Internet y pluralismo jurídico: Formas emergentes de regulación*, Comares, Granada, 2003. Más recientemente, "La prohibición de la censura en la era digital", en Teoría y Realidad Constitucional, nº 31, 2013, págs. 237-276. También inicialmente bajo el enfoque penal, MORALES PRATS, Fermín y MORALES GARCÍA, Óscar, (coords.), *Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet*, de la *Revista Derecho y Proceso Penal*, Aranzadi, noviembre de 2002.

Prácticamente todos los autores citados han realizado estudios en el marco de las obras colectivas que he tenido el gusto de coordinar sobre libertad de expresión en la red y se citan en este estudio, que incluyen, además, otras veinte firmas destacadas en la materia. Asimismo, cabe destacar los estudios contenidos en la *Revista Catalana de Derecho Público* (segunda etapa de la Revista "Autonomías"), monográfico sobre "la incidencia de las TIC en el Derecho público", núm. 35, 2007, en particular, VILLAVERDE MENÉNDEZ, Enrique, "Ciberconstitucionalismo. Las TIC y los espacios virtuales de los derechos fundamentales".

3 Así, el Tribunal Supremo de los Estados Unidos de América, en el caso *Branzburg v. Hayes* de 29 de junio de 1972, ("*liberty of the press is the right of the lonely pamphleteer … as much as of the large metropolitan publisher*").

4 Sentencia del TJCE (Gran Sala) de 16 de diciembre de 2008, cuestión prejudicial asunto C 73/07.

5 En especial ver los apartados 56 a 61.

periodísticas" "*No están reservadas a las empresas de medios de comunicación y pueden ejercerse con ánimo de lucro*". (n. 61)

Según se adelantado, el TS de EE.UU. asentó con claridad la premisa de que Internet es un canal de comunicación que queda protegido por la libertad de expresión e información (*ACLU vs Reno* de 1997). Este mismo punto de partida se ha reconocido sin valor jurídico normativo en diversas declaraciones internacionales "*Los Estados miembros no han de colocar restricciones a los contenidos en Internet que vayan más allá de las aplicadas a otros medios de difusión de contenidos*" (principio nº 1 de la "Declaración sobre la libertad de comunicación en Internet", del Consejo de Europa de 28 de mayo de 2003[6]). Más recientemente, destaca la Declaración conjunta sobre libertad de expresión e Internet de 2011 por altas instituciones internacionales de libertad de expresión, incluyendo la ONU, OSCE o la OEA[7]. Su punto de partida es contundente:

> *La libertad de expresión se aplica a Internet del mismo modo que a todos los medios de comunicación. Las restricciones a la libertad de expresión en Internet solo resultan aceptables cuando cumplen con los estándares internacionales que disponen, entre otras cosas, que deberán estar previstas por la ley y perseguir una finalidad legítima reconocida por el derecho internacional y ser necesarias para alcanzar dicha finalidad". (I, principio general a).*

La premisa de que todos los ciudadanos son titulares de las libertades informativas también se ha afirmado por el Tribunal Constitucional español, aunque aún no para Internet[8]. No obstante, ha señalado que hay una protección "más intensa" de estas libertades cuando se ejercen por empresas y periodistas, por ser los agentes que cumplen una "función constitucional" a través de un "vehículo institucionalizado" (STC 165/1987 y otras)[9]. Pero esta intensidad,

6 Aprobada por el Comité de Ministros en el marco de la 840ª Reunión.

7 http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849&lID=2 (Consulta: 10 de noviembre de 2014)

8 La libertad de expresión de opiniones se reconoce a toda persona (arts. 16 y 20. 1. a) de la Constitución española). También, la libertad de información (art. 20. 1º d) se reconoce "*a cualquier otra persona que facilite la noticia veraz de un hecho y a la colectividad en cuanto receptora de aquélla*" (por todas, SSTC 6/1981, 105/1983, 168/1986, 165/1987, 6/1988, 176/1995, 4/1996).

9 Afirmó que "*la protección constitucional de la libertad de expresión [también para la libertad de información] "alcanza un máximo nivel cuando ... es ejercitada por los profesionales de la información a través del vehículo institucionalizado de formación de la opinión pública que es la prensa, entendida en su más amplia acepción*" *(STC 165/1987), donde se incluyen sus modalidades cinematográfica, radiofónica o televisiva, cuya actividad hemos calificado también como "función constitucional*"". La cita corresponde a la sentencia 176/1995, de 11 de diciembre, en ese caso respecto de la libertad de expresión, en la sentencia 154/1999, de 14 de septiembre la misma cita respecto de la libertad de información.

dijo luego, sólo es respecto del derecho a la cláusula de conciencia y al secreto profesional. Las empresas de comunicación y periodistas "en modo alguno" tienen un derecho fundamental reforzado, más allá de estas garantías especiales (como el secreto del periodista)[10].

Es, pues, capital que el punto de partida sea el reconocimiento de las libertades informativas a todo contenido veraz de interés público, aunque éste sea transmitido en Internet y pese a que no sea a través de periodistas o habituales medios de comunicación social.

2. Apoyos jurisprudenciales a la tesis de la necesidad de extender la protección especial de los medios de comunicación clásicos a los prestadores de servicios

No sólo se trata de reconocer en general a Internet y sus usuarios el ejercicio de estas libertades. Me atrevo a afirmar que la garantía institucional reconocida clásicamente a los medios de comunicación social, y que refuerza jurídicamente la posición de los medios, ya no sólo debe atribuirse a éstos, sino que también debe reconocerse especialmente a determinados prestadores de servicios de la sociedad de la información. Qué duda cabe que el buscador Google, o el servidor de vídeos Youtube o la enciclopedia interactiva Wikipedia, por citar algunos, son elementos esenciales para el acceso a la información en la actualidad. Es cierto que estos grandes prestadores de servicios, de natural tienen una posición materialmente reforzada por su enorme relevancia económica y social en el mundo moderno, pero deben contar también con el reconocimiento reforzado de una garantía institucional o la dimensión objetiva de los derechos fundamentales, lo cual en modo alguno implica la mayor libertad que pueda venir conferida por la actual falta de regulación alguna. Lo mismo, y especialmente, cabe decir de las herramientas que facilitan la interactuación y el debate entre los usuarios de Internet, especialmente las herramientas más empleadas de la llamada web 2.0. En este punto, las redes sociales, así como habituales foros o espacios colaborativos son instrumentos específicos e idóneos no sólo para el acceso a la información, sino para la generación de información y contenidos y, en fin, para el ejercicio de las libertades informativas. De este modo, debe reconocerse también a los grandes prestadores de estos servicios

10 El Tribunal Constitucional rectificó y dijo que con dicha afirmación "*en modo alguno se quiso decir que los profesionales de la información tuvieran un derecho fundamental reforzado respecto a los demás ciudadanos; sino que, al hallarse sometidos a mayores riesgos en el ejercicio de sus libertades de expresión e información, precisaban —y gozaban de— una protección específica. Protección que enlaza directamente con el reconocimiento a aquellos profesionales del derecho a la cláusula de conciencia y al secreto profesional para asegurar el modo de ejercicio de su fundamental libertad de información (STC 6/1981)*". Sentencia 199/1999, de 8 de noviembre, reiterada en sentencia 225/2002, de 9 de diciembre de 2002.

la garantía institucional, que en su caso puede reforzar las garantías en cada caso concreto.

Cabe recordar en este sentido que en España desde la STC 12/1982 (FJ 3º) se atribuye una garantía institucional a la "opinión pública libre", dado que ésta es esencial para el sistema democrático. Se afirma desde entonces que "*La preservación de esta comunicación pública libre sin la cual no hay sociedad libre ni, por tanto, soberanía popular, exige la garantía de ciertos derechos fundamentales comunes a todos los ciudadanos, y […] también una especial consideración a los medios que aseguran la comunicación social y, en razón de ello, a quienes profesionalmente los sirven*". Aunque se relativiza desde los años noventa, en razón de esta garantía o la dimensión objetiva de la libertad de expresión e información se refuerza la prevalencia de la posición de los medios de comunicación, lo cual se observa especialmente en el juicio y ponderación del interés público en el ejercicio de las libertades informativas (ver entre otras muchas las SSTC 104/1985, FJ 5º; 159/1986, FJ 6º; SSTC 171 y 172/1990 O STC 21/2000, o más recientemente la STC 9/2007, FJ 4º). Obviamente, no se trata de un efecto automático que implique una ponderación siempre favorable a los medios de comunicación, sino que la situación se analiza en cada caso concreto.

Parafraseando la referida argumentación constitucional, creo que hoy día es indiscutible que sin los prestadores de la sociedad de la información que permiten el acceso a la información y la generación de contenidos y la interactuación de los usuarios "no hay sociedad libre ni, por tanto, soberanía popular", por lo que merecen "una especial consideración a los medios que aseguran la comunicación social".

Aunque las ha ignorado por completo la sentencia definitiva, claramente contraria a las mismas, las conclusiones de 26 de junio de 2013 del Abogado General Jääskinen del caso Google vs AEPD fueron rotundas al afirmar que "*Poner contenidos a disposición del público en Internet equivale, como tal, a la libertad de expresión […] La publicación en la web es un medio para que los particulares participen en debates o difundan sus propios contenidos, o contenidos cargados por otros, en Internet*" (ap. 122). A mi juicio no hay que desdeñar tales afirmaciones, si bien que cabe puntualizar que se ejercen las libertades de expresión e información cuando se trata de contenidos de interés o relevancia pública.

3. Una inercia jurisprudencial negativa: se reserva a los medios de comunicación clásicos la protección constitucional más intensa

Desde sectores políticos y jurídicos como desde los medios de comunicación clásicos se pretende reservar sólo para estos últimos una libertad de expresión, información y de prensa reforzada y con garantías específicas (privilegios) que

no se extiendan en general a Internet[11]. Se trata de cierta inercia sociológica y jurídica en nuestros tribunales de reservar, más o menos veladamente, las libertades informativas para los medios de comunicación, digámoslo así, clásicos[12]. Así, en España el Tribunal Supremo (TS) ratificó una sanción de la AEPD (Agencia Española de Protección de Datos) por la difusión de información sobre Guardias Civiles condenados por torturas en una web de la Asociación contra la tortura, considerando tales contenidos estaban excluidos de la libre expresión e información[13]. La Sala declaró, sin más explicación, que las concretas conductas sancionadas nada tienen que ver ni con la libertad de expresión, ni con el derecho a la información, en relación con la tortura y la denuncia de tan execrable práctica (FJ 9º). En concreto, afirma el TS que "*la libertad de información alcanza su máximo nivel cuando la libertad es ejercitada por los profesionales de la información a través del vehículo institucionalizado de formación de la opinión pública, que es la prensa*" (FJ 6º).

Esta tendencia negativa encontró su máxima expresión en una muy desafortunada resolución de la AEPD, que llegó a fundamentar una sanción en que:

> *Las páginas web del imputado no pueden ser consideradas medios de comunicación social sin que quepa invocar el ejercicio y prevalencia del derecho de libertad de información que derivaría en una prevalencia general que aboliría de facto la protección de datos personales. Y que desvirtuaría el equilibrio entre derechos sostenido sobre el derecho de la sociedad a ser informada a través de los medios de comunicación y el de los ciudadanos a*

11 Así llamó la atención inicialmente en Estados Unidos de América, entre otros, SUNSTEIN, Cass R., *República.com. Internet, democracia y libertad*, Paidós, Madrid, 2003. En inglés, *Republic.com*, Princeton University Press, 2001; BALKIN, Jack M., "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society". *New York University Law Review*, Volume 79, april 2004, n. 1, págs. 1-58, disponible en http://ssrn.com/abstract=470842 (Consulta: 10 de noviembre de 2014) o RIBSTEIN, Larry Edward, "Initial Reflections on the Law and Economics of Blogging" (April 4, 2005). *U Illinois Law & Economics Research Paper* No. LE05-008. http://ssrn.com/abstract=700961 También de este autor, en "*Bloggers* and Their First Amendment Protection," vol. 57, no. 3 Otoño 2003 issue of "The Neiman Reports", The Neiman Foundation for Journalism at Harvard University. http://niemanreports.org/articles/bloggers-and-their-first-amendment-protection (Consulta: 10 de noviembre de 2014); WU, Tim, *Who Controls the Internet*, Oxford U. Press 2006, entre otros. En Reino Unido, LIPSCHULTZ, J. H., *Free expression in the age of the internet*, Westview Press, Boulder-Oxford, 2000 o recientemente, PACKARD, A., *Digital Media Law*, Willey-Blackwell, Oxford, 2010.

12 Este criterio, que se vislumbra en SSTC la 136/2004, de 13 de septiembre, FJ 5º recordando la doctrina de del vehículo utilizado para difundir la información, en particular si éste es un medio de comunicación social (SSTC 107/1988, de 8 de junio, y 15/1993, de 18 de enero; STC 54/2004, de 15 de abril, FJ 3).

13 Se trata de STS de 26 de junio de dos mil ocho, recurso: 6818/2003. Asociación contra la tortura contra las Resoluciones del Director de la Agencia de Protección de 4 de septiembre y 3 de octubre de 2000.

> *la autodeterminación informativa y privacidad sostenido sobre el derecho de protección de datos*[14].

En otras palabras: un ciudadano no puede atreverse a alegar la libertad de expresión. Eso es cosa de medios de comunicación. Esta resolución fue anulada por la Audiencia Nacional en 2012[15] por lesión de la libertad de expresión; no obstante, son varias las resoluciones con esta tendencia de la AEPD[16].

Detrás de esta corriente, tendente a la no generalización de las libertades plenamente a Internet parece latir que los grandes prestadores de servicios tienen una finalidad económica que los aleja del "mercado de las ideas", quedándose sólo en mercado. Bien se considera que los individuos a través de sus blogs, webs y especialmente en las redes sociales, no son periodistas fiables que merezcan la intensa protección constitucional. Subyace, obviamente, la realidad de la escasa fiabilidad de la información no profesional que inunda Internet, así como la frivolidad, banalidad e irresponsabilidad tan habitual de los millones de usuarios de blogs y redes sociales cuando difunden o redifunden información. También parece que tras esta corriente de reservar las libertades a los medios de comunicación social late la realidad de que es muy difícil sino imposible localizar al autor real de una información ilícita en la Red o, en su caso, perseguir efectivamente la misma.

El reflejo natural ante estas circunstancias parece ser el de mermar la protección constitucional a los usuarios de Internet a favor de los medios y periodistas más clásicos. Sin embargo, a mi juicio ello es un error importante de punto de partida, porque la extensión de la libertad de expresión e información a quien genere ideas o información de interés público en Internet no empece que vaya acompañada de las exigencias de veracidad y diligencia de la información, así como del análisis de si tal información efectivamente tiene interés público y relevancia que le lleve a gozar de una especial protección.

Aunque se han mencionado algunos supuestos, no siempre es fácil percibir directamente los efectos de esta corriente, que no son pocos. La AEPD por ejemplo, no se atreve a analizar supuestos relativos a la difusión de información por medios de comunicación convencional, reenviándolos a los tribunales civiles, en razón de la aplicación de la Ley 1/1982 sobre protección civil del derecho al honor, intimidad personal y familiar y propia imagen. Sin embargo, en casos similares de páginas web los analiza sin problema alguno imponiendo las sanciones que correspondan. De igual modo, cuando efectúa una ponderación

14 Resolución 211/2010, PS 439/2009, CITA denunciada por al U. Politécnica de Madrid por difusión de enlaces y vídeos externos en crítica por competencia desleal de algunos profesores.

15 Así en la sentencia de 11 de abril de 2012 en el P.A. 03078/2010.

16 Así lo analizo en COTINO HUESO, Lorenzo, "Datos personales y libertades informativas. Medios de comunicación social como fuentes accesibles al público (Art. 3 de la LOPD)" en TRONCOSO REIJADA, Antonio (dir.) *Comentario a la Ley Orgánica de Protección de Datos Personales*, Thomsom-Civitas, Cizur Menor, 2010, págs. 289-315 (acceso completo en internet).

del interés público de lo informado, tiende a considerarse que los blogs y webs particulares informan de cuestiones de interés sectorial que no merecen la intensa protección de las libertades[17].

Esta negativa inercia es la que, también, hace casi impensable que una autoridad administrativa pueda resolver cerrar un periódico o televisión sin una resolución judicial; mientras que la legislación permite como regla general el bloqueo o retirada de contenidos sin clara actividad judicial[18]. La AEPD resuelve la comisión de infracciones e impone sanciones efectuando ponderaciones relativas al artículo 20 de la Constitución española en supuestos de difusión de datos personales en Internet. Es más, en la instrucción de procedimientos relativos a una página web o los contenidos de una red social, la Agencia puede requerir la cesación de la difusión de datos personales, o inmovilizar directamente, en otras palabras, puede bloquear el acceso o cerrar una web (art. 49 LOPD). Se hace impensable que esto pudiera hacerlo respecto de los medios clásicos.

También, esta corriente que concentra la protección de la libertad de expresión en Internet a favor de los medios clásicos, es la que lleva a que sólo un profesional de la información cuente con el derecho a no revelar las fuentes. Así las cosas, quedaría excluida esta garantía por ejemplo a *Wikileaks* o similares, esto es, a quien revele en Internet secretos facilitados sin ser un profesional de la información. En este caso, bien es cierto, es la propia Constitución la que afirma la condición "profesional" del secreto.

Reservar de manera excluyente la protección más intensa de las libertades a los medios de comunicación clásicos es un punto de partida que amordaza la libertad de expresión e información en la Red bajo la *espada de Damocles* de severísimas sanciones administrativas o penales.

II. Lineamientos jurisprudenciales en Europa relativos la libertad de expresión e información en Internet

A diferencia de EE.UU. donde desde 1997 el TS empezó a fijar elementos básicos en la materia, los grandes tribunales europeos han intentado rehuir las cuestiones clave de libertades informativas en Internet[19]. Así, a diferencia de

17 Así lo analizo en el trabajo citado en la nota anterior.

18 La cuestión es de extraordinaria complejidad, en tanto en cuanto no está constitucionalmente clara la exigencia de resolución judicial más que en el caso del secuestro judicial. La Ley 34/2002 dispone en su artículo 8 que sólo en los casos que la Constitución o las leyes dejen clara la necesidad de actividad judicial para preservar la libertad de expresión e información, ésta será necesaria.

19 Como analicé en COTINO HUESO, Lorenzo, "Nuestros jueces y tribunales ante Internet y la libertad de expresión: el estado de la cuestión", en COTINO HUESO, Lorenzo (Coord.), *Libertad en Internet…*, cit., págs. 150 y ss. sólo se aborda incidentalmente el fenómeno de Internet respecto de la libertad de expresión en el caso Lindqvist del TJUE en 2003 (centrado en protección de datos) y la sentencia del TEDH de 18 mayo 2004, caso *Plon (société) v Francia* sobre el secuestro del libro del médico personal de Mitterrand.

Norteamérica, los tribunales supranacionales europeos hasta 2012 olvidaron prácticamente el fenómeno de Internet desde la libertad de expresión. Y cuando se ha prestado la atención en los tiempos más recientes como respecto del derecho al olvido, se ha olvidado, si se me permite, de la libertad de expresión. Bien es cierto que, a la fuerza de los años se van fijando algunas premisas importantes sobre libertad de expresión en Internet y la responsabilidad y obligaciones que implican para los prestadores. Ello ha sido así normalmente en procedimientos no centrados en la libertad de expresión, sino sobre competencia desleal, protección de la propiedad industrial e intelectual o del derecho de protección de datos. Con estos *mimbres* debe interpretarse la actual normativa y, al tiempo, muchas de estas premisas condicionan la futura normativa que –hay que esperar– se produzca. Se significan a continuación algunas líneas básicas que se deducen tanto de la jurisprudencia del TJUE cuanto del TEDH.

1. El caso Ahmet Yýldýrým c. Turquía de 2012, primera sentencia del TEDH que aborda frontalmente la protección de la libertad de expresión en Internet y las garantías de legalidad

La sentencia del TEDH de 18 de diciembre de 2012 en el asunto Ahmet Yýldýrým c. Turquía ha sido la primera de este alto tribunal que aborda centralmente la libertad de expresión en Internet[20]. A partir de ella se puede inferir, en esencia, que "*no puede ordenarse a los prestadores que bloqueen contenidos sin discriminar entre los que son lícitos y los ilícitos y para que se adopten medidas de bloqueo es necesaria una regulación legal que dé previsibilidad, certeza y garantías suficientes en la materia*".

El TEDH entiende que viola la libertad de expresión la imposición –judicial– de medidas de bloqueo de acceso a contenidos en Internet que no discriminaron contenidos del sitio de Internet implicado en un proceso penal y los de otros sitios del servicio *Google sites* con contenidos al margen de dicho proceso. El TEDH aprovecha la ocasión para fijar algunos parámetros de la regulación del bloqueo de contenidos en Internet (aps. 64 y ss.):

> *…es necesario un marco legal para garantizar tanto un control estricto sobre el alcance de las prohibiciones y con la garantía de la tutela judicial efectiva para prevenir cualquier abuso de poder [...] la revisión judicial de la*

20 El demandante tenía una web alojada en el servicio Google Sites para difundir trabajos académicos y opiniones personales. Se trataba de contenidos totalmente ajenos a un proceso penal por contenidos lesivos para la memoria de Atatürken otra página de ese servicio (Google Sites). A instancias de la autoridad turca de telecomunicaciones un tribunal resolvió el bloqueo preventivo de la web, pero para poder hacerlo efectivo se ordenó el bloqueo de los contenidos del servicio de Google Sites en su conjunto, como única vía para bloquear la página web con el contenido supuestamente delictivo.

> *medida sobre la base de una ponderación de los intereses contrapuestos ha de estar diseñada para lograr un equilibrio entre estos intereses (ap. 64).*

El TEDH admite el bloqueo judicial de contenidos, pero siempre que se cuente con un marco legal concreto, previsible por los intermediarios y afectados y diseñado para lograr un equilibrio de intereses y que regule el control judicial de las medidas. Asimismo, es preciso que la legislación imponga al juez que se adopte la medida menos restrictiva, de modo que bloquee el mínimo de contenidos posibles y, en principio, sólo se bloquee la web concreta[21].

De esta sentencia cabe subrayar que el TEDH fija unos estándares de previsibilidad, certidumbre, garantías y ponderación de todos los intereses que deberían, por ejemplo, proyectarse a la regulación de la responsabilidad por contenidos en Internet. Sin embargo, no se ha seguido este criterio en 2013.

En clara vulneración de esta jurisprudencia del TEDH precisamente para Turquía, ha sido llamativo que marzo de 2014 el presidente turco Recep Tayyip Erdogan ordenó a la Autoridad de Telecomunicaciones de Turquía bloquear *Twitter* en su país y días después *Youtube*. Se argumentó que estos prestadores no habían filtrado unos contenidos concretos que consideraba ilegales. Así pues, se censuró el todo por la ilegalidad de una parte. Esta carrera bloqueadora fue detenida primero por la justificación ordinaria que simplemente la consideró "contraria a los fundamentos del Estado de Derecho"[22]. El bloqueo fue luego considerado inconstitucional por el Tribunal Constitucional turco[23].

2. La preocupante sentencia del TEDH en el caso Delfi vs Estonia de 2013 y la responsabilización de los intermediarios por los contenidos que alojan

Es importante la sentencia del TEDH en el caso Delfi vs Estonia de 10 de octubre de 2013, de la misma se pueden derivar no pocos criterios que pueden

21 El TEDH admite que las medidas de bloqueo de acceso a contenidos en Internet puedan estar justificadas. Sin embargo, en este caso el juez no verificó si cabía una medida menos restrictiva (ap. 64); se tenía que haber elegido un método en el que sólo quedara inaccesible la web concreta del proceso penal (ap. 65), mientras que no hay muestra de que los jueces tuvieron en cuenta los intereses en juego a la hora de bloquear Google Sites, puesto que la legislación que aplicaron no contiene esta obligación (ap. 66). La aplicación de tal normativa no satisface el requisito de predictibilidad y no brinda el nivel de protección que garantiza el Estado de Derecho de una sociedad democrática. Es más, una normativa que no regula con garantías el posible bloqueo de Internet está en "conflicto directo" con la exigencia del artículo 10. 1º CEDH de que la protección de la libertad de expresión lo es "sin consideración de fronteras" (ap. 67). El bloqueo general produjo efectos arbitrarios y, dada la carencia de garantías legales, el sistema de revisión judicial es insuficiente para evitar abusos (ap. 68).

22 Así según diversas noticias periodísticas con referencia a un juzgado administrativo de Ankara tras una denuncia de la Unión de Colegios de Abogados de Turquía.

23 En todo caso, la resolución del Tribunal Constitucional turco fue bastante confusa y no estableció con claridad el final del bloqueo.

ser muy importantes para Internet. No obstante, cabe señalar que en febrero de 2014 esta sentencia ha sido remitida a la Gran Sala del TEDH que podría variar de criterio.

Delfi es un medio digital de Estonia que permite comentarios de los usuarios a sus noticias. Uno de estos comentarios, relativos a una noticia de interés público, fue considerado lesivo del honor de un importante empresario. La responsabilidad por dicho daño fue atribuida al medio digital. Cabe tener en cuenta que lo habitual en Internet, de la web 2.0 es que los usuarios generen contenidos en las plataformas al uso, y que muchas veces tales contenidos son ilícitos y no se suele poder identificar al autor. A partir de esta sentencia se pueden derivar las siguientes líneas.

Hacer responsable de los contenidos ilícitos al intermediario de Internet que los ha transmitido es una restricción de la libertad de expresión del artículo 10 CEDH, pero esta restricción puede ser admisible. Para ello, la restricción ha de estar prevista por la ley, tener una finalidad legítima y ser necesaria en una sociedad democrática.

El TEDH admite un marco legal no muy definido para la determinación de quién responde por los contenidos de Internet. Esto es así a diferencia de las más severas exigencias de legalidad para bloquear contenidos vista en la sentencia del TEDH de 2012 Ahmet Yýldýrým c. Turquía. La regulación básica de la responsabilidad por contenidos en Internet procede de una Directiva de la Unión Europea. A pesar de la gran incerteza que se produce en la materia en razón de la difusa y dispersa regulación de la responsabilidad en Internet por una Directiva de la Unión Europea, el Derecho interno y su variada interpretación judicial, el TEDH es bien permisivo y estima que se satisface el criterio de límite previsto por la ley.

El TEDH, muy posiblemente para evitar conflictos con el Derecho de la Unión Europea, *considera que la cuestión de responsabilizar por contenidos en Internet es cuestión finalmente nacional que corresponde a la regulación legal interna y su interpretación por los tribunales con un margen de apreciación importante* (aps. 71 y ss.). "*El papel del Tribunal se limita a determinar si los efectos de esta interpretación son compatibles con la Convención*" (ap. 74). Del conjunto normativo aplicable se concluye que "*un editor de medios es responsable por cualquier declaración difamatoria hechas en su publicación multimedia*" (ap. 75).

El TEDH *admite en razón del Derecho interno, se considere editor y responsable de contenidos a un medio digital que permite comentarios de los usuarios. Sin embargo, no generaliza soluciones para Internet y para otros países*. El TEDH no se atreve a asentar una doctrina importante y necesaria en Europa. Por ello, no se cuestiona si esta responsabilidad que aplica a un medio digital como editor puede proyectarse a muchos intermediarios y grandes prestadores de Internet que permiten alojar datos y contenidos por usuarios, contenidos y datos que muy habitualmente lesionan derechos de las

personas. Hay que recordar que esto es lo más habitual (ejemplo: *Google*, *Youtube*, *Facebook*, *Twitter*, *eBay*, *Tripadvisor*, etc.).

Sobre estas bases, el TEDH se centra especialmente en la ponderación entre el derecho a la vida privada y la libertad de expresión sobre los siguientes elementos: "*contribución a un debate de interés general, que tan bien conoce la interesado, el tema del informe, la conducta anterior del interesado, el método de obtención de la información y su veracidad, el contenido, la forma y las consecuencias de la publicación, y la severidad de la sanción impuesta*" (ap. 83).

Para el TEDH, *se justifica la responsabilidad del intermediario por los contenidos ilícitos que introducen sus usuarios en razón del riesgo razonable de que éstos se produzcan. En razón del principio de precaución, si hay riesgo de contenidos ilícitos, hay que poner medios y controles suficientes para evitarlos para no ser responsable (ap. 86)*[24]. La proyección de este razonamiento, a mi juicio, permite responsabilizar a casi todos los prestadores de servicios e intermediarios de Internet al uso por los contenidos que alojan y difunden, pues ciertamente ponen en riesgo cierto los derechos del artículo 18 de la Constitución española, amén de derechos y bienes como la propiedad intelectual.

Haber tomado una serie de precauciones para evitar contenidos ilícitos, que normalmente no adoptan los grandes prestadores de servicios e intermediarios de Internet, no es suficiente para eximir de responsabilidad. El TEDH no consideró suficiente para eximir de responsabilidad que el medio digital advirtiera que las opiniones no eran propias, que estaban prohibidos los comentarios insultantes, ilícitos o dañinos. Tampoco fue suficiente que la web hubiera implantado un filtro que detectara palabras malsonantes, ni que contara con un sistema de denuncia de contenidos impropios con un solo clic para que fueran revisados y retirados, ni que este sistema no fuera utilizado por el demandante. De igual modo, no sirvió para exculpar el hecho de que en ocasiones se retiraran contenidos de oficio por el medio digital (ap. 87). Todos estos sistemas *"no garantizaban una protección suficiente de los derechos de terceras personas"* sino que el medio *"no hizo tanto uso como podría haber hecho de la extensión del control a su disposición"* sobre los contenidos que introducían los usuarios (ap. 89). La empresa pudo haber puesto un sistema más robusto de identificación de los usuarios o un control inmediato de cada

24 Se estimó que dada la noticia de que se trataba el medio digital "*podría haberse dado cuenta de que podría causar reacciones negativas en contra de la compañía naviera y sus directivos y que, teniendo en cuenta la reputación general de los comentarios en el portal de noticias Delfi, se produjo un riesgo superior a la media que los comentarios negativos pueden ir más allá de los límites de la crítica aceptable y alcanzar el nivel de insulto gratuito o la incitación al odio."* En consecuencia "*se esperaba que la empresa ejerciese cierto grado de precaución […] a fin de evitar ser considerada responsable de una infracción de la reputación de otras personas*" (ap. 86).

comentario antes o después de su publicación (ap. 91). . . Tampoco fue suficiente que el medio digital retirara los contenidos ilegales inmediatamente en cuanto se lo anunció la persona afectada. La web asumió que se pudieran emitir comentarios y asumió su responsabilidad

Aunque no es *ratio decidendi*, es de interés tener en cuenta que para el TEDH, *el anonimato en Internet queda bajo la libertad de expresión* (ap. 92)[25].

Pese a que es difícil controlar la información de Internet para los intermediarios, más lo es para los individuos. El TEDH reconoce la dificultad de controlar tanta información que se genera en Internet, y que esta dificultad es "*más onerosa para la persona potencialmente lesionada, pues menos probablemente cuenta recursos para el control continuo de la Internet*" (ap. 92). Todo lo anterior, además de circunstancias como la escasa importancia de la indemnización de que se trataba, llevan al TEDH a considerar que no hubo lesión de la libertad de expresión (ap. 94).

Como se ha dicho, esta sentencia está pendiente de la revisión por el pleno. El TEDH no quiere desvincular su solución de las circunstancias concretas del supuesto. En todo caso, esta sentencia puede considerarse de modo muy negativo para la libertad de expresión e información en Internet. La sentencia deja en un enorme marco de indefinición a la web 2.0 y todos los prestadores de servicios e intermediarios que son la columna vertebral de Internet que usan los ciudadanos. El TEDH elude dar pautas claras para una indefinición que la Unión Europea no resuelve y en España y otros países genera un claro efecto amenazante para usuarios y prestadores de servicios o intermediarios. Esta situación negativa para la libertad de expresión no es exclusiva de España. Las soluciones legislativas y jurisprudenciales en los países de la UE son de lo más variadas[26]. Y la misma Comisión Europea[27] reconoce que

25 "*La Corte es consciente, en este contexto, de la importancia de los deseos de los usuarios de Internet a no revelar su identidad en el ejercicio de su libertad de expresión*".

26 Así, se llegó a condenar a prisión a tres directivos de Google Italia por un vídeo colgado por un tercero en el que se mostraba a un chico autista siendo vejado por sus compañeros, pese a que se retiró al momento de conocer el mismo. Así en aplicación de normas penales y de protección de datos (inicial sentencia de 24 de febrero de 2010 Tribunal Ordinario de Milán, Secc. 4ª penal, Associazioni Vivi-Down vs. Google Italy s.r.l., luego revocada en 2012). También cabe mencionar diversas sentencias condenatorias a Google, por sus sugerencias de búsqueda, como la sentencia de 12 de julio de 2012, la Corte de Casación francesa. En Gran Bretaña en el caso Kaschke v. Gray & Anor, [2010] EWHC 690 (QB), 29 de marzo de 2010) se ha denegado la exclusión de responsabilidad cuando hay algún género de moderación posterior de los contenidos por parte del intermediario que los aloja, ya se tratara de remover otros comentarios ofensivos o incluso la corrección tipográfica o gramatical. La sentencia del 23 de junio de 2009 del Tribunal Supremo alemán reconoció prevalencia de la libertad de comunicación (excluyendo que se tratase del privilegio de la prensa) de un portal de evaluación de maestros (*Spickmich.de*). Pero tal prevalencia se reconoció gracias a que, pese a que había anonimato, se contaba con un sistema algo robusto de identificación de usuarios y la información no era indexable para los buscadores. KLINK, Thomas, "La actual posición del TS alemán ante la libertad de expresión en la red, el caso

La Europa de Internet sigue siendo un mosaico de leyes, reglas, normas y prácticas diferentes"[28] y critica "*los costes y riesgos que entraña la fragmentación derivada de la coexistencia de 27 regímenes jurídicos nacionales*"[29], "*los proveedores intermediarios de Internet viven una situación de incertidumbre jurídica debida a la fragmentación que se observa en la UE […]. Esta fragmentación disuade a las empresas de iniciar actividades en línea o dificulta su desarrollo*[30].

3. Diversos criterios sobre la libertad de expresión e información por el TJUE

El TJUE por lo general no ha abordado de forma directa la libertad de expresión en Internet. Por lo general, el tema viene de la mano de los conflictos que genera la difusión de contenidos en la Red con la propiedad industrial e intelectual y la privacidad y la protección de datos. En todo caso, son ya diversas las afirmaciones en su jurisprudencia que afectan a las libertades informativas en la Red.

La ponderación entre la libertad de expresión y los derechos de la personalidad como la protección de datos debe realizarse bajo el principio de la proporcionalidad en sede estatal, responsabilidad básica del juez nacional. En la sentencia del TJUE de 6 de noviembre de 2003, caso *Lindqvist*, no se encuentran muchas determinaciones sobre las libertades informativas en Internet, pese a que las partes incitaron a analizar la cuestión desde la perspectiva de la libertad de expresión en Internet. Por lo que aquí interesa, la sentencia del TJUE recordó que la ponderación entre la libertad de expresión y los derechos

de "la chuleta" "spickmich.de", en COTINO HUESO, Lorenzo (editor), *Libertades de expresión e información en Internet y las redes sociales... cit.* págs. 88-98.

27 COMISIÓN EUROPEA: Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Un marco coherente para aumentar la confianza en el mercado único digital del comercio electrónico y los servicios en línea, COM (2011) 942 final Bruselas, 11.1.2012, SEC (2011) 1640 y 1641 final. Al respecto, cabe seguir los completos estudios comparados a cargo de la Comisión Europea que evidencian los problemas respecto de la responsabilidad por los contenidos en internet. VERBIEST, Thibault; SPINDLER, Gerald; RICCIO, Giovanni; Maria VAN DER PERRE, Aurélie, *Study on the liability of internet intermediaries*, (MONTERO, dir.), 12 de noviembre de 2007, Documento elaborado para la Comisión Europea: Markt/2006/09/E, acceso completo en Internet. Asimismo y más reciente, el amplio y sólido documento de trabajo adjunto a la *Comunicación* COM (2011) 942 final sobre los procedimientos de notificación y actuación sobre los contenidos ilícitos en línea organizada por intermediarios COMMISSION STAFF WORKING DOCUMENT, *Online services, including e-commerce, in the Single Market.*

28 *Ibídem*, pág. 2: "*Esta situación obstaculiza el desarrollo de los servicios en línea y merma la confianza de los usuarios reales o potenciales, tanto desde el punto de vista de la oferta como de la demanda. El desconocimiento de los derechos que les asisten y de las normas aplicables, así como de las oportunidades que ofrece la economía digital, aumenta sus dudas*".

29 *Ibídem*, pág. 3.

30 *Ibídem*, pág. 14.

de la personalidad como la protección de datos debe realizarse bajo el principio de la proporcionalidad en sede estatal, responsabilidad básica del juez nacional (aps. 85 y ss.).

La libertad de expresión la ejercen todos los que difunden contenidos en Internet, tengan o no ánimo de lucro. Como se ha adelantado, la sentencia del TJUE (Gran Sala) de 16 de diciembre de 2008, cuestión prejudicial asunto C 73/07[31] afirma que la libertad de expresión impone interpretar ampliamente la noción de "periodismo" para dotar de mayor protección a la difusión de contenidos en la Red. Ya en esta línea se había adelantado el auto de 12 de septiembre de 2007 en el mismo caso (ap. 60).

El prestador de servicios de Internet o intermediario goza de la exclusión de responsabilidad "cuando no desempeñe un papel activo que pueda darle conocimiento o control de los datos almacenados". En la sentencia del TJUE de 23 de marzo de 2010 (asuntos acumulados C-236/08 y C-238/08 Google France y Louis Vuitton) se parte de que para gozar de la exclusión de responsabilidad que confiere la Directiva 2000/31/CE de comercio electrónico[32], la actividad del prestador de servicios de la sociedad de la información tiene naturaleza "meramente técnica, automática y pasiva", lo que implica que el prestador de servicios o intermediario "*no tiene conocimiento ni control de la información transmitida o almacenada*" (ap. 113). En esta dirección, cabe mencionar diversas sentencias condenatorias a *Google*, por sus sugerencias de búsqueda, como la sentencia de 12 de julio de 2012, la Corte de Casación francesa[33]. En Gran Bretaña por ejemplo, se ha denegado la exclusión de responsabilidad cuando hay algún género de moderación posterior de los contenidos por parte del intermediario que los aloja, ya se tratara de remover otros comentarios ofensivos o incluso la corrección tipográfica o gramatical[34].

El titular de derechos de propiedad intelectual afectado puede solicitar que se prohíba la retransmisión de sus obras al tratarse de una "comunicación al público" en Internet. En este ámbito, la sentencia del TJUE asunto C-607/11 (ITV Broadcasting Ltd. y otros / TVCatchup Ltd) de 7 de marzo de 2013.

No puede obligarse a los prestadores o intermediarios de Internet que establezcan controles o filtrados técnicos de contenidos en Internet sin distinguir entre contenidos lícitos o ilícitos. Las sentencias del TJUE de 24 de noviembre de 2011, Asunto C-70/2010, Scarlet Extended vs SABAM y

31 Planteada por el Korkein hallinto-oikeus (Finlandia), en el procedimiento entre Tietosuojavaltuutettu y Satakunnan Markkinapörssi Oy, Satamedia Oy.

32 Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior.

33 http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3464 (Consulta: 10 de noviembre de 2014)

34 Kaschke v. Gray & Anor, [2010] EWHC 690 (QB), 29 de marzo de 2010). Acceso en http://www.bailii.org/ew/cases/EWHC/QB/2010/690.html (Consulta: 10 de noviembre de 2014)

Asunto C-360/10 SABAM vs Netlog de 16 de febrero de 2012 no permiten que judicialmente se impongan controles y filtrados técnicos y preventivos a prestadores de servicios y redes sociales para evitar la comisión de ilícitos de propiedad intelectual y protección de datos. El TJUE considera que deben prevalecer la libertad de expresión y la protección de los usuarios que serían controlados y rastreados, así como la libertad de empresa frente a la imposición de estos controles. Se afirma la vulneración de la libertad de información, "*dado que se corre el riesgo de que el citado sistema no distinga suficientemente entre contenidos lícitos e ilícitos, por lo que su establecimiento podría dar lugar al bloqueo de comunicaciones de contenido lícito*" (ap. 52).

Sin perjuicio de lo anterior, en razón de sentencia del TJUE de 27 de marzo de 2014[35], *sí que es posible que un juez solicite a un proveedor de acceso a Internet que bloquee el acceso de sus clientes a un sitio web que vulnera los derechos de autor*. El TJUE señala que el juez nacional que ordene la medida debe ponderar derechos y libertades e intereses en juego. Se afirma cuanto menos que las medidas de bloqueo de acceso a los usuarios "*no priven inútilmente a los usuarios de Internet de la posibilidad de acceder de forma lícita a la información disponible*" (nº 63) y que "*tanto los internautas como también el proveedor de acceso a Internet deben poder hacer valer sus derechos ante el juez*" (nº 54). No obstante, no es necesario probar que los usuarios del servicio acceden efectivamente a los contenidos ilegales.

4. El "olvido" de la libertad de expresión en razón del derecho al olvido. La sentencia del TJUE del caso Google vs AEPD de 2014

La sentencia del TJUE (Gran Sala) de 13 de mayo de 2014 en el asunto C 131/12, en el procedimiento entre *Google Spain*, S.L., *Google Inc*. vs. AEPD y Mario Costeja González[36] ha sido una de las sentencias más esperadas de este tribunal. El tema del derecho al olvido, que pasa a denominarse derecho a la supresión atrae una atención doctrina enorme[37], especialmente desde esta

35 Sentencia TJUE de 27 de marzo de 2014 asunto C 314/12 UPC Telekabel Wien GmbH / Constantin Film Verleih GmbH y Wega Filmproduktionsgesellschaft mb.

36 Cuando un internauta introducía el nombre del Sr. Costeja González en el motor de búsqueda de Google obtenía como resultado vínculos hacia dos páginas del periódico La Vanguardia, del 19 de enero y del 9 de marzo de 1998, respectivamente, en las que figuraba un anuncio de una subasta de inmuebles relacionada con un embargo por deudas a la Seguridad Social, que mencionaba el nombre. La AGPD consideró que Google debía desindexar la información relativa al Sr. Costeja. No cuestionó que la hemeroteca de la Vanguardia siguiese facilitando estos contenidos en la web.

37 Mi trabajo más reciente sobre la cuestión es "El conflicto entre las libertades de expresión e información en internet y el derecho a la protección de datos. El derecho al olvido y sus retos: "un falso derecho, a juzgar por un falso tribunal", en BEL Ignacio y CORREDOIRA Loreto, *Derecho de la información. El ejercicio del derecho a la información y su jurisprudencia*, Centro de Estudios Políticos y Constitucionales, Madrid, 2014. Acceso provisional en http://goo.gl/

sentencia. Ha sido especialmente llamativo que casi mediara un año entre las conclusiones de junio de 2013 y la sentencia definitiva, así como la radical diferencia entre unas y otra.

Pese a que no se ha seguido las mismas, fueron bien importantes las proclamaciones de la libertad de expresión e información en Internet del Abogado General Jääskinen de 25 de junio de 2013. En esencia, las conclusiones iban en la línea de que el buscador Google es esencial para el ejercicio del derecho fundamental de acceso a la información en el Europa y que, por tanto, no puede desvirtuarse el papel de intermediario de Google haciéndole censurar el contenido[38]. Asimismo, el derecho fundamental de acceso a la información quedaría "comprometido" si la información fuera una versión modulada o dulcificada ("*bowdlerizada*"[39]) al gusto del usuario.

1hxOdR (Consulta: 10 de noviembre de 2014) En cualquier caso destaca SIMÓN CASTELLANO, Pere; "El régimen constitucional del derecho al olvido en Internet", *Neutralidad en la Red y otros retos para el futuro de Internet. Actas del VII Congreso Internacional Internet, Derecho y Política*, Universitat Oberta de Catalunya, Huygens Editorial, Barcelona, 2011, págs. 391-406. Especialmente su obra monográfica, *El régimen constitucional del derecho al olvido digital*, Tirant lo Blanch, 2012 (Premio AGPD). También y más reciente, "El carácter relativo del derecho al olvido en la red y su relación con otros derechos, garantías e intereses legítimos", en COTINO HUESO, L. (editor), *Libertades de expresión e información en Internet y las redes sociales… cit.* págs. 24 y ss. Además, entre otros muchos, LUCAS MORILLO DE LA CUEVA, Pablo; "La distancia y el olvido. A propósito del derecho a la autodeterminación informativa", *Revista de jurisprudencia el Derecho*, octubre de 2012; TRONCOSO REIGADA, Antonio; "El derecho al olvido en Internet a la luz de la propuesta de Reglamento General de Protección de Datos Personales", *Datospersonales.org – Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, nº59, 2012 ; RALLO LOMBARTE, Artemi; "El derecho al olvido y su protección. A partir de la protección de datos", *Revista Telos*, Fundación Telefónica, nº octubre-diciembre 2010, http://goo.gl/ueTEX3 (Consulta: 10 de noviembre de 2014). ORZA LINARES, Ramón María (2013): "El derecho al olvido en Internet: algunos intentos para su regulación legal", en CORREDOIRA Y ALFONSO L. y COTINO HUESO L. (Dirs.), *Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales*, Centro de Estudios Políticos y Constitucionales, págs. 475-499. En la misma obra, CERNADA BADÍA, Rosa (2013): "El derecho al olvido judicial en la Red", págs. 521-541.

38 "*[E]l proveedor de servicios [en este caso el buscador Google] necesitaría ponerse en la posición del editor de la página web fuente y comprobar si la difusión de los datos personales en la página web podría considerarse legal y legítima a los efectos de la Directiva. Dicho de otro modo, el proveedor de servicios necesitaría abandonar su función de intermediario entre usuario y editor y asumir la responsabilidad por el contenido de la página web fuente y, cuando resultase necesario, censurar el contenido evitando o limitando el acceso a éste*". (ap. 109) Y ello supondría una restricción de la libertad de expresión e información del prestador o intermediario, del editor (creador del contenido conflictivo) y, sobre todo, del derecho de acceso a la información de los usuarios de Internet. Ver los apartados 120 y ss.

39 Nota original en las conclusiones: "Thomas Bowdler (1754–1825) publicó una versión aséptica de la obra de William Shakespeare que intentaba ser más adecuada para las mujeres y los niños del s. XIX que la original".

Sin embargo, la sentencia, al igual que la sentencia del TJUE (Gran Sala) de 8 de abril de 2014[40] que declara que la Directiva 2006/24/CE de retención de datos de las comunicaciones es contraria a la vida privada y protección de datos, parecen asentar una dirección firme en la protección de estos derechos. No obstante, la sentencia que ahora se expone, lo hace quizá en excesiva medida a costa de las libertades informativas en Internet.

Los elementos básicos de una sentencia poco centrada en la libertad de información:

1º Google realiza un "tratamiento de datos personales" en el sentido de la Directiva cuando indexa contenido y ofrece resultados:

> *el gestor de un motor de búsqueda "recoge" tales datos que "extrae", "registra" y "organiza" posteriormente en el marco de sus programas de indexación, "conserva" en sus servidores y, en su caso, "comunica" y "facilita el acceso" a sus usuarios en forma de listas de resultados de sus búsquedas", (ap. 28). Google es responsable de este tratamiento, pese a que no controle la información de origen de las páginas web que indexa (ap. 34). Debe entenderse a partir de estas afirmaciones, que otros prestadores de servicios de Internet también serán responsables de tratamientos de datos en tanto en cuanto su servicio permita acceder a información estructurada de una persona, de modo que se pueda "establecer un perfil más o menos detallado*.

Así pues, cabe tener en cuenta otros servicios búsqueda o estructuración de contenidos en Internet, como, entre otros muchos, los propios de las redes sociales, quedarán sujetos a las consecuencias de esta sentencia.

2º A Google le es de aplicación la normativa de la Unión Europea y por tanto está sometido a la legislación sobre protección de datos española (aps. 50 y ss.). Así se entiende en razón del criterio interpretativo favorable a aplicar las garantías del Derecho de la Unión Europea (aps. 54 y 58). Se considera en concreto que la publicidad está "indisociablemente ligada" al servicio de búsqueda de Google y que una oficina de publicidad en un Estado miembro es criterio suficiente para aplicar el Derecho europeo (aps. 55, 56). No queda claro qué sucede en el caso de que el prestador de servicios de que se trate no tenga oficina comercial en el Estado miembro. No obstante, en razón del principio de eficacia de las garantías de la norma europea, muy posiblemente se considere también la sujeción al Derecho europeo cuando los servicios vayan destinados al continente, por ejemplo.

40 Asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland Ltd (C-293/12), Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl y otros (C-594/12) / Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Irlanda y el Attorney General.

3º Ni el interés económico de Google, ni el general interés de los usuarios a acceder información de otros justifica suficientemente la grave afección a la privacidad y protección de datos que implica el buscador de Google. Así, "*estos derechos prevalecen, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en encontrar la mencionada información en una búsqueda que verse sobre el nombre de esa persona*" (ap. 97, ídem en 81 o 99). Sólo "*en supuestos específicos, de la naturaleza de la información de que se trate y del carácter sensible para la vida privada de la persona afectada y del interés del público en disponer de esta información, que puede variar, en particular, en función del papel que esta persona desempeñe en la vida pública*" (ap. 81).

Será Google primero y las autoridades de protección de datos o los tribunales después quienes deberán llevar a cabo la ponderación concreta de si procede la desindexación solicitada.

4º Los ciudadanos pueden dirigirse a Google, allí donde esta compañía tenga establecimiento –aunque sólo sea para contratar publicidad– para solicitar la retirada de determinados resultados. Se puede solicitar –y ordenar– la desindexación sin que sea necesario haber acudido previamente a solicitar la retirada de contenidos en la web de origen. Es más, la información puede ser legítima en la web de origen pero no en Google, puesto que la difusión por Google "*puede constituir una injerencia mayor en el derecho fundamental al respeto de la vida privada del interesado que la publicación por el editor de esta página web*". (ap. 87).

5º El tiempo puede hacer que deban desindexarse informaciones: "*incluso un tratamiento inicialmente lícito de datos exactos puede devenir, con el tiempo, incompatible con dicha Directiva cuando estos datos ya no sean necesarios en relación con los fines para los que se recogieron o trataron*" (ap. 93). En este sentido el TJUE recuerda que "*cada tratamiento de datos personales debe ser legítimo, en virtud del artículo 7, durante todo el período en el que se efectúa*", (ap. 95).

A mi juicio, la sentencia adolece de una perspectiva general de la libertad de información. La clave de la sentencia es que las libertades informativas no se aprecian en perspectiva general o institucional a la hora de ponderarlas con la privacidad y la protección de datos. No se percibe la magnitud de la afección a las libertades informativas que se produce al imponer obligaciones a un prestador de servicios de Internet que es esencial para el acceso a la información en el mundo. Asimismo, el interés de los usuarios de Internet en disponer de información no es considerado un contenido de la libertad información, de manera que el acceso a la información queda desvalorizado en la ponderación con los

derechos de vida privada y protección de datos. Ello es importante también cuando se trate de ponderar con otros derechos e intereses en juego. De igual modo, el TJUE tampoco parece tener en cuenta el efecto que produce que el acceso efectivo a la información en Internet, instrumentado esencialmente a través de Google –y otros buscadores– quede condicionado a los criterios privados, ya sean los criterios de los afectados por la información que solicitan la retirada masiva de contenidos, ya sea de Google a la hora de estimar o no las solicitudes de retirada.

III. Para concluir. La necesidad de que el legislador democrático asuma su papel para proteger las libertades informativas y otros derechos fundamentales en Internet

No es escasa la normativa española o europea vinculada a las nuevas tecnologías, como la relativa a comercio electrónico, telecomunicaciones, prestadores de servicios de la sociedad de la información, protección de datos, propiedad intelectual, delitos informáticos, etc. Sin embargo, el conjunto normativo hace auténticas aguas a la hora de fijar no pocos elementos esenciales del ejercicio de la libertad de expresión e información por los grandes y pequeños prestadores de servicios en Internet, así como cientos de millones de usuarios de Internet en todo el mundo. *Sólo* se trata de la actividad cotidiana de unos cuatrocientos millones de europeos y unos treinta y cinco millones de personas en España[41], además de todo el entramado empresarial y social que implican los prestadores de servicios e intermediarios europeos o extranjeros.

Aquí se ha sostenido que los grandes prestadores de servicios e intermediarios de Internet deben contar con una especial protección constitucional, bajo los mismos fundamentos que ésta intensa protección se ha otorgado a los medios de comunicación clásicos. Ello no debe traducirse en la habitual desregularización de la prensa que se ha dado históricamente en España.

La jurisprudencia y los altos tribunales españoles o supranacionales son esenciales para perfilar muchos problemas que genera Internet para las libertades informativas. No en vano, dado el escaso activismo asumido por los tribunales durante décadas, se hace precisa la actuación legislativa respecto de muchos aspectos.

Lo idóneo es una regulación europea que imponga criterios de homogeneización y marcos nítidos de solución de conflictos. No obstante, es en sede nacional donde deben resolverse y ponderarse los conflictos concretos de los derechos fundamentales con otros derechos, bienes e intereses. La pereza y elusión de responsabilidades es también nacional y hay que asir las riendas y marcar algunas pautas en España, especialmente ante el palmario retraso en la toma de decisiones en la UE.

41 Datos sobre acceso a Internet de forma sencilla en www.internetworldstats.com

No está de más proclamar legalmente que toda la información y expresión de interés o relevancia pública en Internet goza de protección constitucional, aunque no proceda de un clásico "medio de comunicación social"; pueden resultar útiles algunas pautas para determinar qué información tiene interés público con independencia de su origen o algunos requisitos o garantías de la veracidad y diligencia tanto respecto de los contenidos, como de quiénes son sus autores. Asimismo es de interés que la legislación parta de que los grandes prestadores o intermediarios son agentes, instrumentos y vehículos esenciales de las libertades informativas en el mundo actual, lo cual debe tenerse bien presente en cualquier regulación de su régimen jurídico o en la imposición de deberes o restricciones. Y la legislación no puede desconocer que *el tamaño importa*, es posible delimitar jurídicamente obligaciones concretas para los grandes prestadores que equilibren el desarrollo de la sociedad de la información con los derechos personales. Esta adecuación al presente también ha de serlo a la web 3.0, el Internet de las máquinas. Y, por ejemplo, no sabemos si las máquinas, esto es, las personas jurídicas o físicas para las que operan, están protegidas por las libertades informativas cuando generan, difunden y redifunden de forma automatizada informaciones de mayor o menor interés público, así como cuando personalizan y restringen el acceso a tales contenidos[42], como los buscadores o la personalización masiva de contenidos[43]. Es bien posible atribuir la protección constitucional de las libertades informativas al tiempo de exigir para ello condiciones de diseño por defecto de los servicios o aplicaciones.

También, cabe afirmar y perfilar las garantías del ejercicio de las libertades en Internet por usuarios e intermediarios y el alcance concreto de algunas de ellas, como el derecho a no revelar las fuentes, o el derecho de réplica y el derecho de rectificación. Falta una meridiana claridad respecto de las facultades administrativas de control de contenidos en Internet, las posibilidades de ponderación de derechos en estos supuestos. De la misma manera, es preciso fijar las garantías judiciales al respecto del control de contenidos en Internet. También, dado que los poderes públicos cada día generan más contenidos en la Red, cabe aclarar la más que dudosa titularidad de las libertades informativas por los poderes públicos; hay que dotar de soporte legal y configurar la discrecionalidad administrativa para difundir contenidos. También cabe hacer

42 Al respecto, de interés, WU Tim, "Free Speech for Computers?", *New York Times*, 19 de junio de 2012, http://goo.gl/nTZPX (Consulta: 10 de noviembre de 2014). El autor es básicamente contrario a conferir especial protección constitucional al discurso de las máquinas. Otra reflexión por firma autorizada al respecto, y en línea contraria del anterior, en "Freedom of Speech and Information Produced Using Computer Algorithms" VOLOKH, Eugene, 21 de junio de 2012, en http://goo.gl/68NPI (Consulta: 10 de noviembre de 2014)

43 Al respecto, recientemente, mi trabajo "La selección y personalización de noticias por el usuario de nuevas tecnologías", en CORREDOIRA Y ALFONSO, Loreto y COTINO HUESO Lorenzo (eds.) *Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales*, cit., págs. 41-56.

referencia a cuestiones como las facultades administrativas de control y moderación de los espacios de interactuación con los ciudadanos en Internet, así como elementos sobre responsabilidad por la información administrativa y garantías ciudadanas ante la misma.

Por cuanto a los conflictos de las libertades informativas en Internet con otros derechos, bienes e intereses, amén de proyectar los generales criterios a las peculiaridades de la Red, la legislación puede tener en cuenta y explicitar determinados elementos contextuales, el ámbito y alcance real de la difusión de los datos en la Red, la naturaleza del medio o modo de comunicación en la Red y el contexto en el que se produce. La necesaria regulación legal no debe caer en la tendencia, habitual en Europa y España, de contemplar el fenómeno de la privacidad sólo desde este derecho fundamental, sin percibir que la difusión de datos en Internet no sólo es un tratamiento a efectos de normativa de datos, sino que, al mismo tiempo en muchos casos, es el ejercicio de la libertad de expresión e información. En la ponderación que se efectúe, no hay que perder de vista el grave riesgo que implica el muy severo marco jurídico administrativo y penal de la protección de datos. El futuro Reglamento europeo de protección de datos que se está ultimando no añade reglas claras a este respecto y remite las cuestiones a cada Estado miembro[44]. Hoy día la legislación española tan siquiera contempla el posible conflicto protección de datos y libertad de expresión y se aplica directamente la Constitución y los criterios jurisprudenciales oportunos.

El recientemente consagrado derecho al olvido, reconocido ahora frente a Google, se puede extender a muchos otros intermediarios y prestadores de servicios de Internet, como las redes sociales, medios digitales en general y hemerotecas digitales en particular. Habrá que determinar respecto de qué tipo de sujetos es exigible. Asimismo, hoy por hoy la noción misma de la desindexación, la utilización del *robot .txt*[45] y otros medios para resolver estos conflictos literalmente no existen en el ordenamiento jurídico[46].

44 Cuanto menos se tiene en cuenta el potencial conflicto entre la privacidad y protección de datos y la libertad de expresión, por ejemplo en el artículo 80. 1º de la Propuesta de Reglamento en la versión del Parlamento de 12 de marzo de 2014, cuando se deja en manos de los Estados miembros las excepciones al derecho de protección de datos *"en lo referente al tratamiento de los datos personales efectuado exclusivamente con fines periodísticos o de expresión literaria o artística, para conciliar el derecho a la protección de los datos de carácter personal con las normas que rigen la libertad de expresión."*

45 Para explicarlo en términos sencillos, el administrador de una web puede de modo muy sencillo indicar qué contenidos de la misma no deben indexados por los buscadores tipo Google. Para una información http://goo.gl/m8YUEx (Consulta: 10 de noviembre de 2014)

46 Sobre el tema me ocupé en "La colisión del derecho a la protección de datos personales y las libertades informativas en la red: pautas generales y particulares de solución", en COTINO HUESO, L. (editor), *Libertades de expresión e información en Internet y las redes sociales... cit.*, págs. 386-401 Acceso completo en Internet.

Es preciso que los prestadores de servicios e intermediarios que tengan que hacer efectivo el derecho al olvido tengan algunas guías y criterios para efectuar una ponderación de la procedencia de la retirada o desindexación de contenidos. Sería idóneo que tales criterios vengan fijados por una ley o normativa similar europea y no se dejen a la autorregulación y a la práctica que adopte Google y otros. Como se señalaba con razón en las conclusiones del caso Google vs AEPD, es necesaria una "protección legal adecuada" de las relaciones privadas para que el prestador o intermediario no censuren y lesionen la libertad de expresión del generador de contenidos[47]. Es más, las mismas autoridades de protección de datos deberían contar con el apoyo de una fuente de legitimidad democrática –como es la ley– y no los meros criterios que vayan discrecionalmente desarrollando para vigilar el alcance de este derecho al olvido en su relación con las libertades informativas. La ley puede regular procedimientos, órganos, plazos así como establecer las bases y remitir a normas reglamentarias más técnicas para determinados sectores de la sociedad de la información.

Como se ha insistido, especialmente al hacer referencia a la sentencia Delfi, la actual incertidumbre sobre la responsabilidad en Internet incentiva la autocensura, la censura colateral. El prestador o intermediario queda en una posición amenazada porque debe vigilar todos los contenidos y ha de establecer sistemas de control de acceso y moderación previos. Además, tiene que retirar cualquier contenido dudoso al momento de una simple comunicación por un sujeto privado.

Una futura legislación puede precisar e imponer mecanismos ágiles y efectivos de contacto con el prestador o intermediario que facilita los contenidos ilegales. Asimismo se puede fijar la revisión periódica o automática de contenidos integrados por terceros en plataformas de Internet. Es muy importante regular, y no dejar a una autorregulación que no llega, que haya procedimientos o mecanismos para establecer con la industria las configuración por defecto de los servicios de la sociedad de la información, la identificación más o menos robusta de los usuarios según los tipos de servicios o contenidos, la necesidad de plantillas efectivas y garantistas de comunicación de ilícitos y, en su caso, de solicitud de retirada de contenidos. En cualquier caso, la imposición de estas cargas a los prestadores debe ser proporcional y ponderada para no implicar efectos colaterales contrarios a las libertades informativas. El futuro reglamento de protección de datos de la Unión Europea establece importantes mecanismos de garantía a través de la evaluación de impacto de privacidad u obligaciones

47 Ap. 134: "*Ello traería consigo una interferencia en la libertad de expresión del editor de la página web, que no disfrutaría de una protección legal adecuada en tal situación, dado que cualquier "procedimiento de detección y retirada" que no esté regulado es una cuestión privada entre el interesado y el proveedor de servicios de motor de búsqueda. Equivaldría a una censura del contenido publicado realizada por un tercero*".

de configuración por defecto. Será necesario perfilar el alcance de estas obligaciones para muchos prestadores o intermediarios de la información en Internet.

No hay que temer la especialización o sectorialización del régimen jurídico. Internet es como la calle y no todo lo que puede haber en la vía pública merece una regulación idéntica, sino una adecuación y contextualización. A la vista de la experiencia y sin perjuicio del dinamismo de la Red, es bien posible describir funcionalidades y servicios para aplicarles regímenes jurídicos singulares. Baste apuntar que la normativa hoy día desconoce que existen buscadores, redes sociales, lugares de comercio masivo, grandes centros de consejos y opiniones para los usuarios, lugares que facilitan el acceso a contenidos concretos, servicios de almacenamiento masivo por usuarios, etc.

En el ámbito de la responsabilidad por contenidos es posible fijar algunos criterios generales como puedan serlo la voluntariedad y conocimiento más o menos directo en la confección del servicio o web y sus posibles usos, o del contenido ilícito concreto, la estructura más o menos automatizada de una agregación, sindicación o redifusión de contenidos, más o menos selectiva de los mismos; la diligencia en la selección de contenidos o en la confección técnica de la selección; la significación y magnitud de los contenidos conflictivos en el marco de la cantidad de los contenidos seleccionados; la participación real en la generación de contenidos los mismos; los indicios que llevan a pensar en el conocimiento material de los contenidos y su posibilidad de control; el hecho de que esos contenidos estén más o menos difundidos en otros sitios; el nivel de acceso y relevancia en la Red de quien los difunde; el contexto y naturaleza propio del sitio web, servicio y aplicación en el marco de los usos de Internet (no es lo mismo insultar en una cantina a las dos de la madrugada que en mitad de una clase de la universidad); la posibilidad de respuesta del afectado en el medio que es la Red y las garantías reales que tiene el afectado de proteger sus intereses en cada ámbito.

Todo esto y mucho más se podía pedir a nuestros legisladores, con la casi certeza de que, si se me permite, esta *carta a los Reyes*, caerá en saco roto. Me atrevo a compartir cierta desesperanza respecto de la adecuación del Derecho a las nuevas, y no tan nuevas, tecnologías que con gran acierto Rodríguez ha verbalizado:

> *En la medida en que cada vez mayor número de ciudadanos acudirán a Internet para confiarle más y más facetas de su existencia, estos problemas no harán sino incrementarse y resultar más patentes.*
>
> *Por otra parte, todo parece indicar que en una buena porción de importantes cuestiones el ciberespacio y el Derecho seguirán sus respectivas órbitas tranquilamente, desconocidos el uno para el otro. Puede que de modo eventual esas "órbitas" se alineen en algún punto, pero esto no será lo frecuente. […] La rápida evolución de Internet contrasta con la lentísima*

evolución de la creación del derecho, y nada hace pensar que ambos rasgos vayan a cambiar[48].

48 RODRÍGUEZ GARCÍA, Luis Fernando, "Políticas de la Federal Communications Commission en materia de neutralidad de la red", en COTINO HUESO, L. (editor), *Libertades de expresión e información en Internet… cit.* págs. 99-113.

Responsabilidades civiles de los proveedores de servicio de Internet (ISP). En especial de los buscadores

Horacio Fernández Delpech*

SUMARIO: I. Introducción. II. Libertad de contenidos de Internet. III. Doctrina de las responsabilidades ulteriores. IV. Legislaciones europeas y norteamericana. V. Nueva legislación brasilera y chilena. VI. La sentencia del Tribunal de Justicia de la Unión Europea del 13 de mayo 2014. VII. El régimen de responsabilidad en Argentina. Criterios de atribución de responsabilidad. VIII. La jurisprudencia argentina. Los casos de las modelos. IX. Sentencia de la Corte Suprema en el caso de Rodríguez, María Belén c/GOOGLE INC s/daños y perjuicios. X. Intentos de dictar normativa en Argentina. XI. Conclusión final.

Resumen

El tema de la responsabilidad civil de los proveedores de servicio de Internet, en particular de los buscadores, es importante debido a la ausencia de regulación específica en algunos países, especialmente en América Latina. El autor analiza las normas del Derecho europeo y estadounidense que regulan esta materia, así como las reglas generales sobre responsabilidad establecidas en el Código Civil argentino, aplicadas en algunos casos por los jueces de este país, para concluir y reafirmar que el criterio adecuado al establecer la responsabilidad de los buscadores debe basarse en el sistema de responsabilidad subjetiva.

Palabras clave: Responsabilidad civil. Proveedores de servicio de Internet. Buscadores. Responsabilidad subjetiva

Recibido: 18/11/2014 • Aceptado: 26/11/1014

* Abogado especialista en Propiedad Intelectual y Derecho Informático. Primer Presidente y actualmente Presidente Honorario de la Asociación de Derecho Informático de Argentina. Profesor en las Universidades del Salvador, Austral y Universidad Católica de Argentina y en los postgrados internacionales de las Universidades de Georgetown y Nueva York, (EE.UU.) y Deusto de España. Autor de numerosas publicaciones y libros entre ellos: "Internet: Su problemática Jurídica", "Protección Jurídica del Software", "Manual de los Derechos de Autor", "Esquemas de Derecho Laboral y de Derecho Informático", "Manual de Derecho Informático".

Abstract

The liability of Internet Service Providers, including search engines, has become a highly important issue due to lack of specific regulation in some countries, especially in Latin America. The author analyzes the rules of European and US law governing this matter, as well as the general rules of liability in the Argentine Civil Law, applied in some cases by the judges of this country, to conclude and reaffirm that proper standard to establish the liability of search engines must be based on the system of fault liability.

Keywords: Liability. Internet Service Providers. Search Engines. Fault Liability

I. Introducción

La temática de las responsabilidades civiles que pueden resultar para los ISP (*Internet Service Provider*), y en particular entre ellos para los buscadores, por sus actividades en Internet, es de trascendental importancia, tanto por la falta de una legislación a su respecto en casi toda América Latina, así como por una serie de causas judiciales que se están tramitando en la Republica Argentina, entre las cuales una de ellas ha obtenido recientemente Sentencia de la Corte Suprema de Justicia de la Nación.

Creo que importante primero precisar qué se entiende actualmente por ISP, o *Internet Servicie Provider*, en la usual terminología anglosajona.

Tal como lo he analizado en otras oportunidades[1], además de los usuarios de Internet, que son aquellas personas que acceden a un sitio de la Red para buscar información o utilizar alguna de las diferentes aplicaciones que la Red brinda, y de los proveedores de contenido, que son todos aquellos autores, editores o simplemente usuarios que proveen información a los sitios de Internet[2], existen los Proveedores de Servicio de Internet (*Internet Service Providers*), que son quienes posibilitan la conexión entre el usuario y los contenidos incorporados al sito y que conforme la actual doctrina internacional podemos dividirlos en:

- **Los proveedores de acceso. *Internet Access Providers*** (IAP) Son quienes brindan a los usuarios individuales el servicio de conexión a Internet, a través de un servidor de gran poder conectado a la Red (nodo), a fin de poder llegar así a los diferentes sitios de la Red. Por su parte, el proveedor de contenido, creador de una página o sitio, requiere también los servicios

1 FERNÁNDEZ DELPECH, Horacio: *Manual de Derecho Informático*. Editorial Abeldó Perrot de Buenos Aires, año 2014.

2 La web 2.0 que caracteriza a la época actual es una red dinámica en donde impera la interoperabilidad entre los usuarios que hoy en día pueden interactuar y colaborar con el creador de contenidos, generando ellos nuevos contenidos y creando así comunidades virtuales.

de estos proveedores de acceso a fin de poder incorporar su sitio a la red.

- **Los proveedores de alojamiento. *Hosting Service Providers*** (HSP) Son quienes brindan el servicio de alojamiento de páginas web en su propio servidor, así como otros servicios adicionales.
- **Los proveedores de Red. *Networks Service Providers*** (NSP). Son quienes brindan una estructura técnica (líneas telefónicas, de cable o por antena), a fin de que el usuario se conecte a través del proveedor de acceso con la página o sitio almacenada por el proveedor de alojamiento. De esta forma se completa el circuito en el que el usuario individual accede a los contenidos incorporados por el proveedor de contenidos.
  Es de resaltar que muchas veces existen empresas que brindan conjuntamente los servicios de proveedor de acceso a usuarios y proveedor de alojamiento, e incluso actúan en algunos casos también como proveedores de Red.
- **Los proveedores de servicios de aplicaciones. *Aplication Service Provider*** (ASP). Sus funciones consisten fundamentalmente en habilitar software, u otras aplicaciones informáticas en Internet, de manera que puedan ser utilizadas por los clientes sin necesidad de instalarlas en sus computadores. Es decir, el cliente accede a las aplicaciones utilizando únicamente su *browser*. La información se almacena en un *data center* que tiene todas las características de seguridad necesarias. Este servicio básico se complementa con otros servicios adicionales, como la administración de infraestructura (bases de datos, computadores centrales, usuarios, etc.), el manejo de respaldos y recuperación, la ejecución de procesos, y todos aquellos servicios que garanticen una explotación cómoda, continua y segura. Este sujeto tiene una gran similitud con el proveedor de *cloud computing*.

Pero ya hace algunos años aparece un quinto sujeto, al que se lo comienza a incluir entre los ISP, y nos referimos a los Proveedores de Localización (LSP), y para expresarlo más claramente, estamos hablando de los buscadores de Internet, que son quienes nos facilitan hoy en día la búsqueda y conexión con determinados sitios. En España, la Ley 34/2002 sobre Servicios de la Sociedad de la Información y el Comercio Electrónico (LSSICE)[3], ya en su redacción del año 2002 incluyó a los Proveedores de Localización entre los ISP.

Lo que voy a intentar tratar ahora es analizar cuáles son las responsabilidades civiles que les pueden caber a estos proveedores de servicio de Internet, y en particular a los LSP (proveedores de localización o buscadores) por los contenidos que transmiten, o por los resultados de las búsquedas de los usuarios,

3 Ley 34/2002, de los servicios de la sociedad de la información y comercio electrónico. Publicada en el Boletín Oficial del Estado núm. 166, de12 de julio de 2002.

cuando tanto esa transmisión o ese resultado de búsqueda contiene contenidos nocivos, ilícitos o que causan daño.

II. Libertad de contenidos en Internet

Internet nace como un ámbito de plena libertad en donde pareciera que todo es válido y en donde cualquier intento de filtrar, impedir o castigar por contenidos violatorios de la moral o de la ley no es aceptado. En todas partes del mundo existe desde hace ya años esa conciencia de plena libertad en Internet, fundamentalmente garantizando de esta forma la plena libertad de expresión.

La Constitución de la República Argentina garantiza ampliamente la libertad de expresión y, tanto los Convenios Internacionales suscriptos por la Argentina, como la jurisprudencia de nuestra Corte Suprema, establecen una prohibición a la censura previa de los contenidos, aun cuando con ellos se cometiera un delito.

Pero el derecho a la libertad de expresión no es un derecho absoluto, y tiene ciertas restricciones cuando se trata de contenidos ilícitos o prohibidos por la ley. Tanto la doctrina como la jurisprudencia nacional e internacional han admitido el establecimiento de restricciones sobre el derecho de libertad de expresión con el fin de proteger a la comunidad de ciertas manifestaciones ofensivas y para prevenir el ejercicio abusivo de ese derecho.

Pero esas restricciones a la libertad de expresión no pueden consistir en censurar previamente el contenido, pero sí en establecer su prohibición o ilicitud, y en caso de darse el supuesto, de juzgar con posterioridad al acto la responsabilidad que puede caber.

Igual situación se da en los contenidos que causan un daño, en los cuales es válido pensar en el juzgamiento con posterioridad al acto de la responsabilidad que puede caber.

En estos casos debemos ver cuál es la responsabilidad que puede tener cada uno de los actores que intervienen en la incorporación y transmisión de ese contenido que pueden resultar responsables con posterioridad al acto, en lo que ha dado en llamarse "*responsabilidad ulterior*".

En la República Argentina, el artículo 14 de la Constitución Nacional consagra el derecho a publicar las ideas por la prensa sin censura previa, garantizando así ampliamente la libertad de expresión.

Asimismo existen normas legales que hacen extensiva dicha garantía constitucional a Internet[4], y, tanto los Convenios Internacionales suscriptos por la Argentina, como la jurisprudencia de nuestra Corte Suprema, establecen una

4 Y es así como primero el Decreto 1279/97 establece que el servicio de Internet se considera comprendido dentro de la garantía constitucional de la libertad de expresión, y luego la Ley 26032/2005 dispone que la búsqueda, recepción y difusión de información e ideas por medio del servicio de Internet se considera comprendida dentro de la garantía constitucional que ampara la libertad de expresión.

prohibición a la censura previa de los contenidos, aún cuando con ellos se cometiera un delito.

Destaco que el concepto de "idea" de nuestra Carta Magna se ha hecho extensiva, tanto en la doctrina como en la jurisprudencia argentina (al igual que en la totalidad de los documentos internacionales), a las informaciones e ideas de todo tipo.

La Corte Suprema ha establecido que:

> *…no todo lo que se difunde por la prensa o se emite en programas radiales o televisivos o por cualquier otro medio goza del amparo otorgado por la prohibición a la censura previa, sino aquello que por su contenido encuadra en la noción de información o difusión de ideas*[5].

La jurisprudencia argentina ha sido muy fiel a este principio y ha establecido que no corresponde la censura previa ni aún en el caso de que la publicación implique la comisión de un delito, estableciendo claramente que en ese supuesto sólo es posible juzgar las responsabilidades con posterioridad al acto, pudiendo imponerse incluso penas en caso de delito. (caso Verbitzky)

III. Doctrina de las responsabilidades ulteriores

Pero el derecho a la libertad de expresión no es un derecho absoluto, y tiene ciertas restricciones cuando se trata de contenidos ilícitos, prohibidos por la ley, o que causan daño.

Tanto la doctrina como la jurisprudencia nacional e internacional han admitido el establecimiento de restricciones sobre el derecho de libertad de expresión con el fin de proteger a la comunidad de ciertas manifestaciones ofensivas y para prevenir el ejercicio abusivo de ese derecho.

Pero esas restricciones a la libertad de expresión no pueden consistir en censurar previamente el contenido, pero sí en establecer su prohibición o ilicitud, y en caso de darse el supuesto, de juzgar con posterioridad al acto la responsabilidad que puede caber. En estos casos, el autor de la incorporación de ese contenido puede resultar responsable con posterioridad al acto, en lo que como ya he adelantado se ha dado en llamar "*la doctrina de las responsabilidades ulteriores*".

Hasta hace no muchos años eran escasas las situaciones en que se debía juzgar responsabilidades de este tipo. En una web en que el usuario solamente bajaba contenidos de Internet, los problemas eran menores, pero ya desde comienzos del nuevo siglo, Internet se transforma en algo mucho más activo. La nueva Internet 2.0, es una Internet interactiva donde todos ingresamos contenidos que a veces rozan derechos, cuando no los afectan. Entonces nos

5 Fallos 315:1943. Año 1992, ED 149,245.

encontramos frente a un choque de derechos y nos preguntamos: ¿podemos censurar esos contenidos?

La apología del delito, la propagación de injurias y calumnias, las propagandas discriminatorias, la violación y afectación de la intimidad y de la privacidad de las personas, las violaciones a los derechos propiedad intelectual, entre otras cuestiones, son ahora situaciones frecuentes en Internet y requieren entonces una respuesta de los regímenes jurídicos mas allá de ese principio de la libertad en Internet.

Como dijera, nuestra Constitución e incluso normas internacionales impiden la censura previa. Pero necesitamos encontrar un equilibrio, ya que la libertad de unos termina donde comienza la libertad de otros.

La doctrina de las responsabilidades ulteriores podría resumirla indicando que implica que cada uno puede escribir, publicar, subir o transmitir contenidos sobre la base de la libertad de expresión garantizada por la Constitución, y si estos contenidos resultaren ser difamatorios, ofensivos o lesivos a los derechos de otro o configuren un ilícito, será posteriormente la Justicia quien determine la responsabilidad de la persona y en su caso, el resarcimiento económico por los daños y perjuicios ocasionados.

Esta doctrina que fue formulada, para la prensa escrita, por la Convención Americana sobre Derechos Humanos (Artículo 13)[6] y otros Convenios Internacionales, y que tuvo acogida en numerosos fallos de la Corte Suprema de Justicia de Argentina, así como en la principal jurisprudencia americana, creo que sin duda es plenamente aplicable a Internet.

Internet es libre, pero ello no se puede traducir una total impunidad para quien viola la ley o causa daños a terceros.

Con relación a lo estipulado en el referido, la Comisión Interamericana de Derechos Humanos, ha dicho también:

> *La Convención permite la imposición de restricciones sobre el derecho de libertad de expresión con el fin de proteger a la comunidad de ciertas manifestaciones ofensivas y para prevenir el ejercicio abusivo de ese derecho. El artículo 13 autoriza algunas restricciones al ejercicio de este derecho, y estipula los límites permisibles y los requisitos necesarios para poner en*

6 Párrafo 1 y 2 del artículo 13 de la Convención Americana sobre Derechos Humanos. Pacto de San José de Costa Rica

1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar:

a) el respeto a los derechos o a la reputación de los demás, o

b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas.

> *práctica estas limitaciones. El principio estipulado en ese artículo es claro en el sentido de que la censura previa es incompatible con el pleno goce de los derechos protegidos por el mismo. La excepción es la norma contenida en el párrafo 4, que permite la censura de los "espectáculos públicos" para la protección de la moralidad de los menores*.

La única restricción autorizada por el artículo 13 es la imposición de responsabilidad ulterior. Además, cualquier acción de este tipo debe estar establecida previamente por la ley y sólo puede imponerse en la medida necesaria para asegurar: a) el respeto de los derechos o la reputación de los demás, o b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas.

IV. Legislaciones europeas y norteamericana

La *Multimedia Act*, dictada en Alemania en el año 1997, establece diferentes tipos de responsabilidades según sea la clase de ISP de que se trate, distinguiendo para ello a tres tipos de proveedores: *Information Providers*, *Hosting Providers* y *Access Providers*.

Con relación al *Information Provider*, se establece la plena responsabilidad por los contenidos que incorporan al sito; mientras que con relación a los *Access Providers* y *Hosting Service Providers* se determina que son responsables sólo si tienen conocimiento de los contenidos, teniendo en cuenta si tomaron las medidas técnicas adecuadas frente a tal conocimiento.

La Directiva europea 2000/31 CE sobre comercio electrónico[7], establece en su artículo 15.1:

> *Los Estados miembros no impondrán a los prestadores de servicios una obligación general de supervisar los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas, respecto de los servicios contemplados en los arts. 12, 13 Y 14*"

Establece también la Directiva en su artículo 12 la falta de responsabilidad de los ISP, al disponer: "*No serán responsables por los datos transmitidos a menos que: hayan originado o modificado ellos mismos los datos o hayan seleccionado a éstos o a sus destinatarios*".

Con total acierto Miguel Peguera Poch, comentando la Directiva 2000/31/CE, nos dice:

7 Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior.

> …El hecho de que los contenidos que el ISP transmite o almacena hayan sido proporcionados por terceros, esto es, que sean contenidos ajenos, resulta esencial desde la perspectiva de la exención de responsabilidad. Así, cuando el prestador de servicios coloca en la red o transmite contenidos propios, la exención de responsabilidad pierde su razón de ser. En efecto, la exención se funda en que el prestador del servicio intermediario no ha tenido parte ni en la creación ni en la decisión de transmitir o de hacer accesibles los contenidos ilícitos y potencialmente dañinos: ha sido un tercero quien lo ha hecho. A ello se añade la idea de que no le es técnicamente posible, o bien le resulta excesivamente costoso, supervisar lo que circula por sus redes o se aloja en su servidores, con lo que normalmente ni siquiera tendrá conocimiento de los contenidos concretos, y aún menos de su carácter lícito o ilícito[8].

Se completa este principio de la irresponsabilidad de los ISP con lo dispuesto en el artículo 13 de la Directiva europea sobre la memoria tampón o caching[9] y en el artículo 14 sobre los supuestos de *hosting*.

En España, la LSSICE trata detalladamente el tema refiriéndose en los artículos 13 a 17 a la responsabilidad de los prestadores de los servicios de la sociedad de la información, distinguiendo entre ellos a:

- los operadores de redes y proveedores de acceso a una red de telecomunicaciones;
- los prestadores de servicios que realizan copia temporal de los datos solicitados por los usuarios;
- prestadores de servicios de alojamiento o almacenamiento de datos;
- prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda. Resalto que este apartado de la ley española incorpora entre los ISP a los intermediarios de localización.

Todos estos son, en la terminología habitual y que referimos en el comienzo del este trabajo, proveedores de servicio de Internet.

En los tres primeros casos, la ley española exime de responsabilidad a estos prestadores, salvo excepciones como que hayan originado la transmisión, modificado los datos o seleccionado éstos o a los destinatarios de dichos datos.

En el cuarto caso, de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda, y que incluye a los proveedores de localización (buscadores de Internet), la ley es más rigurosa y establece clara y expresamente:

8 Miguel Peguera Poch en la obra: “La Responsabilidad Jurídica de los Prestadores de Servicios de la Sociedad de la Información” - Pamplona. Aranzadi.

9 Este artículo 13 de la Directiva europea, que es del año 2000, tuvo especialmente en cuenta lo dispuesto por los Convenios Internet de la OMPI de 1996.

> *Los prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que:*
>
> - *a) No tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o*
> - *b) Si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.*
>
> *Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.*

En los Estados Unidos de América, la temática de la libertad de los contenidos en Internet y la responsabilidad de los proveedores de servicio ha sido objeto de un amplio debate.

En 1996 se dictó en el marco de la ley de telecomunicaciones, la *Communications Decency Act* (CDA), que fue ratificada como ley federal el 8 de febrero de 1996. Esta ley establecía responsabilidades penales a quienes transmitiesen vía Internet material obsceno o indecente destinado a menores.

De inmediato fue impugnada judicialmente por la Asociación de Libertades Civiles (*American Civil Liberties Union*), sosteniendo que la ley era inconstitucional por violar la libertad de expresión consagrada por la Constitución de los Estados Unidos de América, obteniéndose que en el Distrito de Filadelfia se decretase la no aplicación de la normativa del acta.

La fiscal de Reno también recurrió contra esta ley, y el caso llegó a la Corte Suprema, donde el 26 de junio de 1997, en un fallo no unánime (7 votos contra 2), con fundamento en la Primera Enmienda de la Constitución, se declaró su inconstitucionalidad[10].

Se consideró allí que la ley, al imponer restricciones a la difusión por Internet de material sexual, vulneraba el derecho a la libre expresión e implicaba una censura ilegal.

Se expresó también en el fallo:

> *...a pesar de la legitimidad y la importancia de la meta legislativa de proteger a la niñez de los materiales peligrosos, coincidimos en que el estatuto*

10 Janet Reno, Fiscal General de los Estados Unidos de América, et al, apelantes c/ *American Civil Liberties Union*, et al No. 96-511 - CS Estados Unidos de América - (1997 U.S LEXIS 4037)

> *limita la libertad de expresión y en que el Gobierno no tiene la potestad para discriminar a los adultos con materiales que no sean aptos para niños.*

Como consecuencia del citado fallo, el entonces Presidente Clinton se refirió públicamente al tema, propiciando la necesidad de encontrar una solución técnica que permitiese proteger a los menores de edad, sin que ello violase la libertad de expresión.

El Congreso de los EEUU, por iniciativa de la Senadora Patty Murray promulgó entonces en octubre de 1998, la Ley para la Protección o Seguridad en Línea de la Privacidad de los Menores.

Allí se contempla el uso de programas filtro o de selección de contenidos por parte de los padres, estableciendo que los operadores de sitios deben exhibir notas al respecto.

Desde entonces, la jurisprudencia ha eximido de responsabilidad a los ISP. Tal como sucedió en los casos "Lunney vs. Prodigy Service" (de diciembre de 1999) y "Ben Ezra, Weinstein & Co. Inc. vs American OnLine" (de marzo de 2000), donde se determinó que las empresas demandadas que eran proveedores de servicio no eran responsables, ya que sólo tenían calidad de distribuidores o editores secundarios.

Finalmente, la *Digital Millennium Copyright Act (DMCA)*, aprobada en EE.UU en octubre de 1998, modificó la *Copyright Act* en diversos puntos, figurando entre ellos la incorporación de la Sección 512 que regula la limitación de la responsabilidad en línea de los servidores de Internet (ISP).

La normativa libera de responsabilidad a los ISP por:

- la mera transmisión de contenidos (*transient host*).
- el almacenamiento de contenidos, de manera que permita al servidor reducir tanto el tiempo de transmisión a sus usuarios como su ancho de banda (*system o proxy caching*).
- el almacenamiento de contenidos en sistemas o redes bajo la dirección de los usuarios (*hosting*)
- el uso de mecanismos de localización de la información a través de los cuales se dirige a los usuarios a contenidos infractores.

Por otra parte, establece un detallado sistema de "*notice and take down*" (detección y retirada), para hacer posible que los titulares de derechos de autor identifiquen las infracciones que se cometen a sus obras a través de Internet y lo notifiquen a los servidores afectados para que el material, supuestamente infractor, sea retirado o su acceso bloqueado.

La DMCA establece consecuentemente que la responsabilidad de los ISP se genera únicamente cuando la incorporación del contenido es manifiesta o habiendo sido notificados que existen contenidos violatorios de la ley, no toman de inmediato las medidas necesarias para su retiro.

Si bien la normativa de la DMCA esta referida a violaciones a los derechos de *copyright*, estas normas también han sido aplicadas a otros contenidos ilícitos o que causan daño a terceros.

Vemos cómo este tema ha sido tratado en dos sistemas jurídicos, con dos soluciones parecidas pero no iguales.

- En la ley española, se establece que el sitio web o el buscador es responsable recién cuando tiene conocimiento efectivo de la infracción, y que este conocimiento efectivo existe cuando un órgano competente haya declarado la ilicitud del acto. Así es como en España, y en Europa en general, el buscador sería responsable subjetivamente –salvo que le demostremos culpa directa– sólo cuando un órgano competente le ordene bajar ese contenido porque es ilícito o es inmoral o causa un daño y si no cumple, entonces sería responsable. Hacemos presente que conforme reciente jurisprudencia española si bien el párrafo segundo de la ley hace mención a que se entenderá que existe ese conocimiento cuando un órgano competente lo haya declarado, la coletilla final de la norma, que indica la posibilidad de "*otros medios de conocimiento efectivo que pudieran establecerse*", ha permitido al Tribunal Supremo señalar en otros casos que tanto la comunicación remitida por el tercero afectado como la propia naturaleza de los contenidos pueden servir como medio de alcanzar ese conocimiento efectivo y por lo tanto romper la exención de responsabilidad

- En EE.UU. la situación es distinta, la responsabilidad es más amplia. En este país funciona el sistema del *notice and take down*, establecido primero por la *Digital Millenium* para la propiedad intelectual y que se ha ampliado después a los ISP y buscadores de Internet directa o indirectamente:
  - "Yo le aviso que esto es una infracción; desde este momento usted es responsable si un juez lo condena".
  - Para que nazca la responsabilidad, en EE.UU. no se necesita la decisión judicial que ordene bajar el contenido, sino que basta que el afectado lo solicite, y no se efectúe de inmediato la bajada del contenido.

V. Nueva legislación brasilera y chilena

En abril de 2014, Brasil dictó la Ley 12965, Marco Civil de Internet, en la que se establece entre otras cosas que los ISP no son responsables civilmente por daños provenientes de contenidos generados por terceros, y sólo podrán ser responsabilizados por contenidos que transmiten si hay una resolución judicial que ordena la baja y ellos no la cumplen. De esa manera, se busca evitar que las empresas tengan la potestad de definir por sí mismas cuándo un material debe ser retirado.

Por su parte, la Ley 17336 de Propiedad Intelectual de Chile, en su modificacion dispuesta por la Ley Nº 20.435, contempla la responsabilidad de los ISP pero con relacion solo a las violaciones a la propiedad intelectual. Establece asi la ley que los ISP están exentos de responsabilidad si eliminan los contenidos infractores tan pronto tengan conocimiento de ello. Con la nueva ley, se considera que los prestadores de servicios de Internet conocen de la existencia de los contenidos que transmiten o alojan una vez que reciben una notificación judicial al respecto.

VI. La sentencia del Tribunal de Justicia de la Unión Europea del 13 de mayo de 2014[11]

Si bien referido específicamente a los datos personales, la Gran Sala del Tribunal de Justicia de la Unión Europea, dictó recientemente este importante fallo, en el cual establece que conforme la Directiva 95/46/CE sobre protección de datos, debe interpretarse que la actividad de un motor de búsqueda, que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por ultimo ponerla a disposición de los internautas, debe calificarse como tratamiento de datos personales.

Asimismo que cuando esa información contiene datos personales, el motor de búsqueda debe considerarse responsable de dicho tratamiento, pudiendo en estos casos el afectado pedir la eliminación de dicho dato.

De acuerdo a este controvertido fallo, cualquier persona que se sienta afectada por cuanto sus datos personales aparecen mencionados en un buscador, como resultado de la indexación de una noticia sobre su persona, tiene el derecho a exigir directamente al buscador, la supresión de ese dato, sin necesidad de cumplir con ningún requisito previo, siempre que alegue que el dato sobre su persona le produce perjuicio y ya no sea pertinente por el tiempo transcurrido, respaldando así el derecho a la autodeterminación informativa y el derecho al olvido[12].

Si bien este fallo es mencionado frecuentemente como referido al derecho al olvido, creo que el mismo es más amplio y tiene alcances mayores.

El derecho al olvido es materia de tratamiento en las diversas leyes de protección de datos personales en cuanto a los datos de informaciones crediticias, estableciéndose en esas leyes de protección de datos de diversos países, que los datos de incumplimientos financieros deben ser eliminados de las bases de datos transcurrido cierto tiempo, que es diferente si la deuda ha sido abonado a

11 Tribunal de Justicia Unión Europea, Gran Sala, 13/05/2014. - Google Spain, S.L., y Google Inc., c. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González.

12 Sobre este tema me referí ampliamente en una nota publicada en la edición del Diario La Ley de Buenos Aires, del 9 de junio de 2014.

no. Nuestra Ley 25326 de Protección de Datos Personales[13], establece el derecho al olvido en el artículo 26.4, al establecer:

> *Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hace constar dicho hecho*.

Este es el derecho al olvido que tratan las leyes y podríamos llamarlo el derecho al olvido de los incumplimientos financieros. Ahora bien, ya hace tiempo que se está hablando también del derecho a olvido en Internet, que incluiría toda clase datos. El fallo Tribunal Europeo si bien fue la consecuencia de un pedido de eliminación de datos de incumplimiento financiero, o sea un derecho al olvido financiero, por las conclusiones a que arriba y la terminología utilizada, podría decirse también que está admitiendo el derecho al olvido en Internet de otros datos, de carácter general, financieros o no financieros, en situaciones que el dato de una persona que conste en Internet, sea transcripto por el buscador, le produzca perjuicio por no ser pertinentes y por el termino transcurrido.

Hago presente que como consecuencia de este fallo, Google ha implementado en Europa un formulario para que cualquier persona que se considere afectada e incluida en la doctrina del fallo, pueda pedir la eliminación de los datos que se refieren a su persona y que considere que sean inadecuados, no pertinentes y excesivos en relación con los fines del tratamiento, o que no estén actualizados o que se conserven durante un período superior al necesario (derecho al olvido).

En el ámbito de la ciudad de Buenos Aires, y siguiendo la idea del fallo europeo, ante un amparo presentado, el juez Marcelo López Alfonsín, titular del Juzgado 18 en lo Contencioso, Administrativo y Tributario, ha dictado recientemente un fallo en el que ordena a la Dirección General de Defensa y Protección del Consumidor del Gobierno de la Ciudad Autónoma de Buenos Aires a adoptar, en un plazo de 180 días, las medidas necesarias a fin de exigir a los proveedores de servicios de búsqueda y enlaces o motores de búsqueda en Internet domiciliados en la ciudad de Buenos Aires, que incorporen de manera obligatoria un protocolo interno de protección al derecho a la intimidad de los usuarios de Internet.

Este protocolo interno, de implementarse, debiera permitir a los habitantes de la ciudad de Buenos Aires, exigirle a los buscadores Google o Yahoo la eliminación de *links* o resultados de búsquedas que lleven a contenidos que consideran que afectan su derecho de intimidad, privacidad, seguridad o dignidad; para ello, el peticionante deberá aportar pruebas de que esto es así, y si el buscador no acepta la petición, deberá el interesado recurrirá la justicia

13 Ley 25326 de Protección de los Datos Personales. Sancionada: octubre 4 de 2000. Promulgada parcialmente: octubre 30 de 2000.

VII. El régimen de responsabilidad en Argentina. Criterios de atribución de responsabilidad

En el Derecho argentino tenemos dos tipos de responsabilidad: la contractual, derivada del incumplimiento de un contrato, y la extracontractual, que se origina por haber producido un daño sin que exista un nexo contractual.

En estos casos de perjuicios a terceros por páginas de Internet o a través de buscadores, tenemos evidentemente que encontrar la solución en la responsabilidad extracontractual. Y para que se dé esa responsabilidad, tendremos que determinar primero la existencia del daño material o moral medible y resarcible en dinero. Después debe existir una relación causal entre el daño y el hecho que dio lugar al mismo. Acá ya es más difícil: ¿existe la relación causal? Sí, ¿pero en el buscador? Y, yo creo que también podría existir esa relación de causalidad. El hecho cuestionado debe ser antijurídico, si no hay antijuridicidad no puede darse la responsabilidad extracontractual.

Pero sentada la existencia de una responsabilidad extracontractual, debemos determinar el segundo factor de atribución de responsabilidad. Se trata de determinar si se trata de una responsabilidad subjetiva o estamos frente a una responsabilidad objetiva.

La responsabilidad subjetiva está regulada en los artículos 512 y 1109 del Código Civil que establecen fundamentalmente que "*La culpa del deudor en el cumplimiento de la obligación consiste en la omisión de aquellas diligencias que exigiere la naturaleza de la obligación, y que correspondiesen a las circunstancias de las personas, del tiempo y del lugar*", y que "*Todo el que ejecuta un hecho, que por su culpa o negligencia ocasiona un daño a otro, está obligado a la reparación del perjuicio…*"

La responsabilidad objetiva está regulada en los artículos 1113, 1071, 1071 bis, y complementarios del Código Civil.

> *Artículo 1113. "La obligación del que ha causado un daño se extiende a los daños que causaren los que están bajo su dependencia, o por las cosas de que se sirve, o que tiene a su cuidado. En los supuestos de daños causados con las cosas, el dueño o guardián, para eximirse de responsabilidad, deberá demostrar que de su parte no hubo culpa; pero si el daño hubiere sido causado por el riesgo o vicio de la cosa, sólo se eximirá total o parcialmente de responsabilidad acreditando la culpa de la víctima o de un tercero por quien no debe responder. Si la cosa hubiese sido usada contra la voluntad expresa o presunta del dueño o guardián, no será responsable".*

El texto originario de la norma regulaba dos supuestos específicos de responsabilidad: la responsabilidad genérica del principal por los daños que causaren los que están bajo su dependencia, y la responsabilidad del guardián por las cosas de que se sirve o que tiene a su cuidado.

La reforma de 1968 del Código Civil por Ley 17711 agregó la responsabilidad de los daños causados con cosas y la responsabilidad de los daños causados por el riesgo o vicio de la cosa.

Podría resumir diciendo entonces que en nuestro sistema jurídico argentino, tenemos dos factores de atribución de responsabilidad extracontractual: la responsabilidad subjetiva, clásica, tradicional, y la nueva responsabilidad que está avanzando poco a poco, que es la responsabilidad objetiva. ¿Dónde vamos a encontrarla? ¿Podemos decir que es subjetiva, que es objetiva? La primera es la que surge de la culpa en el daño, el que causó un daño debe resarcirlo. Esa es la responsabilidad tradicional, que podríamos endilgarle quizás al ISP, incluyendo al buscador, si le demostramos la culpa o la intencionalidad. Por otro lado, la responsabilidad objetiva –que tiene muchos defensores– es la responsabilidad sin culpa, que se crea por otros motivos, que se crea para tener respuesta ante el daño, para que ciertos actores respondan aún sin haber cometido culpa. ¿Por qué así? Porque se ejerce una actividad riesgosa o peligrosa.

Discrepo con la opinión de importantes juristas, como el Dr. Horacio Granero, que atribuye responsabilidad objetiva a los motores de búsqueda por los daños que se causen, por considerar a las actividades relacionadas con Internet como actividades riesgosas[14].

Yo creo que la responsabilidad objetiva no puede ser atribuida a Internet, porque no puede decirse que Internet sea una actividad riesgosa o peligrosa.

Me inclino rotundamente por la exclusión de Internet de este tipo de responsabilidad. Creo que Internet no es lo mismo que el fabricante de un arma o el propietario de una plataforma petrolera. Si creáramos una responsabilidad objetiva sobre Internet, además de equivocar en su origen, la estaríamos destruyendo. Sería la destrucción de un medio que ha beneficiado enormemente al mundo; el acceso al conocimiento y a la información que nos ha dado Internet no puede ser desconocido.

El concepto de actividad peligrosa o riesgosa es por su naturaleza un concepto relativo y depende del estado de avance de la ciencia y de la técnica en un sector determinado; lo que lleva a calificar de peligrosas a actividades que antes no lo eran o viceversa.

Debemos tener en cuenta que la utilización de la informática en el mundo actual ha dado lugar a múltiples usos, de los cuales algunos pueden implicar actividades peligrosas pero no así otros. Pareciera que la utilización de la informática en el manejo de los bancos de datos podría considerarse una actividad peligrosa, así como también el desarrollo de determinado software

14 El Dr. Horacio Granero sostuvo esta posición en la exposición que como amigo del Tribunal formuló en la audiencia pública convocada por la Corte Suprema en el caso de María Belén Rodríguez

destinado a actividades industriales que son en sí peligrosas, como podría ser el destinado a centrales nucleares, etc.

Bustamante Alsina, nos dice que los sistemas automatizados de información que emplean la informática, no son cosas peligrosas que dañen por sí mismas, sino instrumentos que el hombre maneja o acciona a su voluntad.

También se ha dicho que "*No hay cosas peligrosas o no peligrosas en sí, sino que la tal peligrosidad depende de una situación jurídica integrada por la cosa y la particular circunstancia en que se originó el daño*"[15].

Tradicionalmente se ha considerado que la responsabilidad objetiva debe estar asociada con actividades que son potencialmente peligrosas y que tienen una alta probabilidad de daño. Tal el caso, entre otros, de la energía eléctrica, la producción o tratamiento de explosivos o materiales radioactivos.

Creo que cuando se trata de perjuicios que son causados por la cosa interviniente en forma directa, y esa cosa es un elemento de potencial peligro, podría regir el sistema de responsabilidad objetiva del artículo 1113 2º párrafo del Código Civil, pero cuando la cosa no interviene autónomamente en la producción del daño, sino respondiendo al accionar del operador, debe ser aplicado un criterio de atribución de responsabilidad subjetiva conforme al artículo 1109 del Código Civil.

¿Cuál es la naturaleza del ISP? ¿Son editores de la información? Yo creo que no, ni el que transmite técnicamente la información ni el buscador que me lleva a ella editaron la información, ellos no crean el link, se crea automáticamente con la indexación que realiza el algoritmo creado. Son sólo distribuidores de información, reitero, no le podemos atribuir entonces una responsabilidad objetiva. Pero sí una responsabilidad subjetiva, en la medida que le podamos probar que ellos conocían el hecho, que fueron partícipes, que tuvieron culpa, que hubo negligencia de su parte.

Opino que en el estado actual de la tecnología, pese a que algunos fallos dicen lo contrario, no podemos decir que los buscadores sean *per se* culpables por los contenidos que indexan. Su culpabilidad puede surgir en el momento que son advertidos de la circunstancia dañina, que es más o menos lo que han dicho los últimos fallos y el fallo de la Corte Suprema que luego comentaremos. La posición internacional dice que son meros distribuidores de información, tienen responsabilidades subjetivas por las infracciones de terceros, porque hay un daño, una causalidad, y hay una acción dolosa o culposa. Tenemos que probarle la culpa por lo menos, la negligencia. ¿Cuándo nace esa responsabilidad? Por las infracciones propias serían responsables plenamente. Entonces yo diría que si los buscadores no crean la información, no tienen plena responsabilidad, sino indirecta, secundaria, que surge por la responsabilidad de un tercero.

15 BOFFI BOGGERO, Luis María, *Tratado de las obligaciones*, Ed. Astrea, 1985, t. 6, p. 103.

VIII. La jurisprudencia argentina. Los casos de las modelos

En materia jurisprudencial, un caso interesante en Argentina es el conocido como ***los juicios de las modelos***.

Hace algunos años, numerosas modelos argentinas y personas vinculadas al espectáculo, advirtieron que colocando sus nombres en los buscadores Google y Yahoo, se obtenían referencias que las vinculaban con sitios pornográficos y de prostitución, así como se difundían sus fotografías en los buscadores de imagen. Esto provocó que muchas de estas modelos, considerándose afectadas moralmente, promovieran juicios de daños y perjuicios contra los buscadores Google y Yahoo, juicios a los que se los llamo "*los juicios de las modelos*".

Se trata de más de 100 causas judiciales que tramitan ante los tribunales argentinos, en las cuales las modelos demandan daños y perjuicios a Google de Argentina y a Yahoo Inc., por considerarse afectadas moralmente por citas en los buscadores referidos, que las vinculaban con la prostitución. También se reclama por el uso indebido de la imagen.

En esos casos, recién tenemos unas pocas sentencias de primera y segunda instancia, que no son coincidentes entre sí, y un reciente fallo de la Corte Suprema de Justicia de la Nación.

El primer caso fue el de una integrante del grupo musical "Bandana", Virginia Da Cunha, quien en el año 2009 obtuvo a su favor la primera sentencia dictada en la República Argentina en relación con esta temática conforme el fallo dictado por la Dra. Virginia Simari, titular del Juzgado Nacional de Primera Instancia en lo Civil 75. El fundamento del fallo condenando a Google y a Yahoo fue la responsabilidad tanto objetiva como subjetiva. Posteriormente la Cámara Civil, revocó dicho decisorio, con voto dividido y rechazo la demanda. El expediente se encuentra en la Corte Suprema de Justicia de la Nación vía recurso extraordinario.

El segundo de los casos fue dictado en la causa promovida por la modelo Belén Rodríguez[16] contra los mismos buscadores. En este fallo en ambas instancias se hizo también lugar a la demanda pero condenando sobre la base de un criterio de atribución de responsabilidad subjetiva, lo que llevó al recurso extraordinario ante la Corte Suprema, quien con fecha 28 de octubre de 2014 dicto sentencia, revocando la sentencia de Cámara y rechazando la demanda, en un fallo que por su importancia comentaremos en el próximo apartado.

El tercero de los mencionados casos, el fallo de Paola Krum[17] dictado por la Sala J de la Cámara Civil, que luego de un minucioso y pormenorizado análisis del caso establece:

16 Rodríguez, María Belén c/GOOGLE INC s/daños y perjuicios.

17 Krim, Andrea Paola c/ Yahoo de Argentina S. R. L. y otros/ daños y perjuicios

> *Las accionadas son titulares de sus propias páginas web o sitios y por ende responsables de los contenidos que ellos introducen o reproducen, sean por medios automatizados o no.*
>
> *c. La actividad que desarrollan los buscadores es una actividad riesgosa". Al respecto sostuvo la magistrada que "…Resulta evidente que esta interpretación abarca no sólo a la actividad propia de las demandadas y a las cosas de las que se sirve, de las que son propietarias y/o guardianes, sino también quedan incluidas en lo que Pizarro llama "los otros posibles sujetos pasivos" en relación a los sitios de terceros que son el ámbito donde se genera el daño primigenio, luego multiplicado, potenciado y concretado en una magnitud casi inimaginable..."*

Como corolario, en este punto en el que se fijaba una responsabilidad objetiva de los buscadores por ser una actividad riesgosa, la magistrada agregó que las demandadas también habían incurrido en responsabilidad subjetiva porque ninguna había cumplido en forma completa e inmediata con las medidas cautelares dictadas luego de iniciados los juicios y que ordenaban el bloqueo de los contenidos que afectaban a las modelos actora en los juicios.

Vemos que en este fallo se admite tanto la responsabilidad objetiva como la responsabilidad subjetiva, admitiéndose que ambas se pueden dar simultáneamente.

Finalmente, la Sala L de la Cámara Civil, en noviembre de 2013 en autos "Solaro Maxwell, María Soledad c/ Yahoo de Argentina SRL y otros/ daños y perjuicios" dictó un fallo en el cual condenó a las demandadas Yahoo y Google, ya que coincidió con lo resuelto por la Dra. Mattera en el fallo de Paola Krum de la Sala J, estableciendo en consecuencia que la responsabilidad de las accionados, como titulares o guardadores de los buscadores en Internet, no era subjetiva, sino que:

> *se trata de una actividad riesgosa y que debe analizarse desde la órbita de la responsabilidad objetiva por el riesgo que dicha actividad genera (art. 1.113 Cód. Civil). Ello por cuanto si bien los contenidos de los sitios son cargados por terceros, lo cierto es que la finalidad de los buscadores es facilitar su llegada a sus usuarios mediante su indexación.*

Conforme a esta responsabilidad objetiva condenó a las demandadas.

Creo que el camino que vamos haciendo es ése, pero que la jurisprudencia argentina está marcando que la responsabilidad parte recién desde el momento en que el buscador es noticiado de la infracción. Creo que no podemos llevar a condenarlo de por sí, porque el responsable es el sitio y no el buscador.

IX. La sentencia de la Corte Suprema en el caso Rodríguez, María Belén c/GOOGLE INC s/daños y perjuicios

Como lo comentara en el párrafo anterior, el 28 de octubre de 2014, la Corte Suprema de Justicia de la Nación, dictó un fallo en el que revocó la sentencia que había dado lugar a una indemnización de daños y perjuicios a favor de la modelo María Belén Rodríguez. El fallo fue dictado con una disidencia parcial de los Dres. Ricardo Lorenzetti y Juan Carlos Maqueda.

En este caso, la referida modelo había promovido demanda de daños y perjuicios contra Google Inc., demanda que, luego amplió contra Yahoo de Argentina SRL, fundamentándose en lo substancial en que se había procedido al uso comercial y no autorizado de su imagen y que se habían avasallado sus derechos personalísimos al habérsela vinculado a determinadas páginas de Internet de contenido erótico y/o pornográfico.

En primera instancia en un meduloso fallo, la jueza analizó minuciosamente los hechos, así como toda la doctrina nacional e internacional, fallando a favor de la actora y condenando a los demandados. Entre otros argumentos se expresa:

> *Así, la conducta culpable de las demandadas, nacida –reitero– a partir de la notificación fehaciente de la afectación a los derechos personalísimos de la actora, engendra la obligación de reparar el daño causado. Tienen pues responsabilidad directa por violación al principio legal del "alteran non laedere" que el Código Civil prevé en el art. 1109, debiendo responder por las consecuencias dañosas, en tanto medie adecuado nexo de causalidad entre ésta y los daños probados (cfr. arts. 901, 905, 906, 1067, 1068, 1069 y cc del Código Civil).*

Esta sentencia fue apelada y la Sala A de la Cámara Civil la modificó levemente, ya que rechazó la demanda contra Yahoo y mantuvo la condena contra Google Inc., si bien redujo el monto de la condena. La sentencia encuadró la responsabilidad de los llamados "motores de búsqueda" en el ámbito de la responsabilidad subjetiva, descartando que pudiera aplicarse la responsabilidad objetiva del artículo 1113 del Código Civil.

Tanto la parte actora y Google interpusieron sendos recursos extraordinarios que fueron concedidos en cuanto estaba en juego la inteligencia de derechos de raigambre constitucional.

Substanciada una audiencia pública de carácter informativo los días 21 y 29 de mayo de 2014, en la cual expusieron las representaciones letradas de cada una de las partes y los amigos del tribunal, el 28 de octubre de 2014 la Corte dictó su fallo en el que revocó la sentencia y rechazó la demanda.

Trataré de resumir brevemente, y en algunos casos transcribir, los fundamentos de este importante y meduloso fallo

- Que en este caso se encuentran en conflicto dos derechos fundamentales: por un lado, la libertad de expresión e información y, por el otro, el derecho al honor y a la imagen.
- Que la libertad de expresión, que es totalmente aplicable a Internet y a los motores de búsqueda, comprende el derecho a transmitir ideas, hechos y opiniones difundidas a través de Internet, conforme lo establece expresamente el artículo 1 de la Ley 26.032, en concordancia con lo establecido por la Relatoría para la Libertad de Expresión de la Organización de los Estados Americanos y el artículo 13 de la Convención Americana sobre Derechos Humanos.
- Que el derecho al honor se refiere a la participación que tiene el individuo dentro de la comunidad amparando a la persona frente a expresiones o mensajes que lo hagan desmerecedor en la consideración ajena al ir en su descrédito.
- Que el derecho a la imagen integra el derecho a la privacidad que tutela el artículo 19 de la Constitución Nacional
- Que resulta indudable la importancia que desempeñan los motores de búsqueda en el funcionamiento de Internet.
- Que no corresponde juzgar la eventual responsabilidad de los "motores de búsqueda" de acuerdo con las normas que establecen una responsabilidad objetiva, desinteresada de la idea de culpa. Que corresponde hacerlo, en cambio, a la luz de la responsabilidad subjetiva. Afirmando el fallo que la pretensión de aplicar responsabilidad objetiva en este tema, es de una llamativa insustancialidad.
- La libertad de expresión seria mellada de admitirse una responsabilidad objetiva que -por definición- prescinde de toda idea de culpa y, consiguientemente, de juicio de reproche a aquél a quien se endilga responsabilidad.
- Que en muchos países se afirma que los "buscadores" no tienen una obligación general de "monitorear" los contenidos que se suben a la Red y que se concluye en ellos que los "buscadores" son, en principio, irresponsables por esos contenidos que no han creado, mencionando a su respecto la Directiva europea 2000/31 CE, las legislaciones de Chile, Brasil, España, Estados Unidos.
- Que, sin embargo, hay casos en que el buscador puede llegar a responder por un contenido que le es ajeno: eso sucederá cuando haya tomado ***efectivo conocimiento*** de la ilicitud de ese contenido, si tal conocimiento no fue seguido de un actuar diligente.
- Luego la Corte afirma que a los efectos del efectivo conocimiento requerido para la responsabilidad subjetiva, cabe preguntarse si es suficiente que el damnificado curse una notificación privada al

"buscador" o si, por el contrario, es exigible la comunicación de una autoridad competente.

- *Afirmando que en ausencia de una regulación legal específica, conviene sentar una regla que distinga nítidamente los casos en que el daño es manifiesto y grosero, a diferencia de otros en que es opinable, dudoso o exige un esclarecimiento, lo que registra antecedentes en alguna legislación (artículo 16 del decreto-ley 7 de 2004 de Portugal). Son manifiestas las ilicitudes respecto de contenidos dañosos, como pornografía infantil, datos que faciliten la comisión de delitos, que instruyan acerca de éstos, que pongan en peligro la vida o la integridad física de alguna o muchas personas, que hagan apología del genocidio, del racismo o de otra discriminación con manifiesta perversidad o incitación a la violencia, que desbaraten o adviertan acerca de investigaciones judiciales en curso y que deban quedar secretas, como también los que importen lesiones contumeliosas al honor, montajes de imágenes notoriamente falsos o que, en forma clara e indiscutible, importen violaciones graves a la privacidad exhibiendo imágenes de actos que por su naturaleza deben ser incuestionablemente privados, aunque no sean necesariamente de contenido sexual. La naturaleza ilícita -civil o penal- de estos contenidos es palmaria y resulta directamente de consultar la página señalada en una comunicación fehaciente del damnificado o, según el caso, de cualquier persona, sin requerir ninguna otra valoración ni esclarecimiento. En estos casos es suficiente la notificación directa del afectado.*
- *Por el contrario, en los casos en que el contenido dañoso que importe eventuales lesiones al honor o de otra naturaleza, pero que exijan un esclarecimiento que deba debatirse o precisarse en sede judicial o administrativa para su efectiva determinación, cabe entender que no puede exigirse al "buscador" que supla la función de la autoridad competente ni menos aún la de los jueces. Por tales razones, en estos casos corresponde exigir la notificación judicial o administrativa competente, no bastando la simple comunicación del particular que se considere perjudicado y menos la de cualquier persona interesada.*
- Con relación al reclamo por el uso comercial y no autorizado de su imagen, (se refiere el tribunal a las *thumbnails* o imágenes en miniatura en los buscadores), interpretando el artículo 31 de la Ley de propiedad intelectual, establece que no constituye violación del derecho a la imagen la reproducción con fines de enlace de las imágenes de la modelo, por lo que revoca lo decidido en la alzada y

rechaza la demanda a este respecto. Aquí es en donde surge el voto en disidencia de los Dres. Lorenzetti y Maqueda.

- Con relación a la posibilidad de establecer una condena que obligue a Google a fijar filtros o bloqueos de vinculaciones para el futuro, el fallo, mencionando la doctrina de las responsabilidades ulteriores, desarrollada en el artículo 13 inc. a de la Convención Americana sobre Derechos Humanos, así como la propia doctrina de la Corte que ha establecido que toda restricción, sanción o limitación a la libertad de expresión debe ser de interpretación restrictiva, al igual que la doctrina la Corte Suprema de los Estados Unidos, decidió que cualquier sistema de restricciones previas tiene una fuerte presunción de inconstitucionalidad por lo que rechazó el agravio de la demandada. (La sentencia de Cámara había dejado sin efecto el pronunciamiento de primera instancia que había decidido disponer la eliminación definitiva de las vinculaciones del nombre, la imagen y las fotografías de la actora con sitios y actividades de contenido sexual, erótico y/o pornográfico a través de Google).

Que pese a que la Corte en el fallo admite la responsabilidad subjetiva de los motores de búsqueda a partir de la notificación judicial o administrativa competente (cuando el daño sin ser manifiesto o grosero es opinable, dudoso o exige un esclarecimiento), e incluso en algunos casos ante la simple intimación personal del afectado (cuando el daño es manifiesto o grosero), no se condena a los buscadores, ya que la sentencia de Cámara apelada había dado por acreditado que no hubo intimación previa al juicio y cuando se ordenó la medida cautelar de bloqueo los buscadores la cumplieron, dice la Corte*:*

> *…no se ha acreditado que las demandadas, frente a una notificación puntual de la actora que haya dado cuenta de la existencia de contenidos lesivos para sus derechos en determinados sitios, hayan omitido bloquearlos, con lo cual no se encuentra probada su negligencia en los términos del arto 1109 del Código Civil.*

La Corte fundó su revocatoria y rechazo de la demanda en esta circunstancia de falta de culpa o negligencia de las demandadas, afirmado por la Cámara y consentido por la actora.

Creo que el fallo en lo principal es correcto y coincide con mi opinión reiterada sobre el tema desde hace años en diversas publicaciones, libros y ponencias internacionales[18], ya que parte de la base que los buscadores, no son los creadores de los contenidos y que consecuentemente solo serían responsables por su

18 Además de mis libros ya mencionados, ponencia presentada en el XVII Congreso Iberoamericano de Derecho e Informática, celebrado en septiembre de 2014, en San José de Costa Rica.

obrar culposo o negligente cuando han sido intimados por el afectado o por una orden judicial, basándose en un factor de atribución de responsabilidad subjetiva, rechazando en forma total la posibilidad de que exista una responsabilidad objetiva de los buscadores. En este caso, la Corte consideró que no había obrar negligente, ya que tomó en cuenta lo que la Cámara estableció en ese sentido y que no fue motivo del recurso extraordinario.

Creo también que con iguales fundamentos se hubiera podido condenar si se hubiera acreditado el incumplimiento de las demandadas ante una intimación sin éxito, o las demandadas no hubieran cumplido con el bloqueo ordenado en una medida cautelar. Distinta será la situación de otros juicios similares pero en donde las demandadas fueron intimadas a bloquear contenidos o la Justicia, en medida cautelar, así lo dispuso, y los buscadores fueron en principio renuentes al bloqueo.

Sin duda este fallo será un importante precedente para futuras decisiones y ha marcado claramente la preeminencia que la Corte da a la libertad de expresión frente a los derechos personalísimos, estableciendo la inexistencia de responsabilidad objetiva y admitiendo en cambio la posibilidad de responsabilidad subjetiva cuando existe culpa, con las fórmulas apropiadas y al estilo del sistema norteamericano del *notice and take down*, para la notificación al buscador y el consecuente nacimiento de su responsabilidad.

X. Intentos de dictar normativa en Argentina

Desde hace algunos años varios fueron los intentos de dictar una normativa relacionada con la responsabilidad de los ISP, pero el 22 de febrero de 2011, el diputado Federico Pinedo presentó un proyecto que reingresado en el Parlamento en el 2013, regula la actividad desarrollada por los ISP y que tomo estado parlamentario.

El proyecto consta de 10 artículos en los cuales se recogen principios de legislación extranjera y de la jurisprudencia local e internacional.

En particular, el proyecto establece que los buscadores de Internet o las redes sociales deben responder por contenidos publicados por terceros cuando dichos contenidos violentan derechos personalísimos tales como el honor, la imagen o la intimidad. El proyecto establece que la responsabilidad nace cuando el ISP tiene el conocimiento efectivo de que la información almacenada viola normas legales o derechos de terceros, considerando que “tiene conocimiento efectivo” desde el momento en que es notificado del dictado de alguna orden judicial que ordene la baja o bloqueo del contenido.

En consecuencia, el Proyecto Pinedo considera que no puede imputarse responsabilidad objetiva fundando la responsabilidad en un criterio de atribución de responsabilidad subjetiva. Este proyecto aun no ha sido tratado por el Parlamento.

XI. Conclusión final

Como antes dijera, en nuestro sistema jurídico argentino, tenemos dos factores de atribución de responsabilidad extracontractual: la responsabilidad subjetiva, clásica, tradicional, y la nueva responsabilidad que está avanzando poco a poco, que es la responsabilidad objetiva**.**

¿Dónde debemos buscar las responsabilidades de los proveedores de servicio de Internet frente a la incorporación de contenidos ilícitos o que causan daño o a la incorporación ilícita de contenidos? ¿Se trata de una responsabilidad subjetiva u objetiva?

La primera es la que surge de la culpa en el daño, el que causó un daño debe resarcirlo. Esa es la responsabilidad tradicional, que podríamos endilgarle quizás al buscador si le demostramos la culpa o la intencionalidad.

Su fundamento lo encontramos en los arts. 512 y 1109 del Código Civil que establecen fundamentalmente:

> *La culpa del deudor en el cumplimiento de la obligación consiste en la omisión de aquellas diligencias que exigiere la naturaleza de la obligación, y que correspondiesen a las circunstancias de las personas, del tiempo y del lugar"*, y que *"Todo el que ejecuta un hecho, que por su culpa o negligencia ocasiona un daño a otro, está obligado a la reparación del perjuicio…*

Por otro lado tenemos la responsabilidad objetiva –que tiene muchos defensores– que es la responsabilidad sin culpa, que se crea por otros motivos, que aparece para tener respuesta ante el daño, para que ciertos actores respondan aún sin haber cometido culpa. ¿Por qué así? Porque se ejerce una actividad riesgosa o peligrosa.

Más allá de lo que estableció la Corte en el fallo reciente antes comentado, y que sin duda será un antecedente de gran importancia para futuros fallos, e incluso para cualquier proyecto normativo, personalmente creo, y así siempre lo he afirmado[19], que la responsabilidad objetiva no puede ser atribuida a Internet, porque no puede decirse que Internet sea una actividad riesgosa o peligrosa.

Me inclino rotundamente por la exclusión de Internet de este tipo de responsabilidad. Creo que Internet no es lo mismo que el fabricante de un arma o el propietario de una plataforma petrolera. Si creáramos una responsabilidad objetiva sobre Internet, además de equivocar en su origen, la estaríamos destruyendo. Sería la destrucción de un medio que ha beneficiado enormemente al mundo; el acceso al conocimiento y a la información que nos ha dado Internet no puede ser desconocido.

El concepto de actividad peligrosa o riesgosa es por su naturaleza un concepto relativo y depende del estado de avance de la ciencia y de la técnica en un

19 Horacio FERNÁNDEZ DELPECH. *Manual de Derecho Informático*. Abeledo Perrot. 2014 y Internet Su problemática Jurídica, Lexis Nexis 2004

sector determinado; lo que lleva a calificar de peligrosas a actividades que antes no lo eran o viceversa.

Se debe tener en cuenta que la utilización de la informática en el mundo actual ha dado lugar a múltiples usos, de los cuales algunos pocos pueden implicar actividades peligrosas pero no así otros. Pareciera, y así lo ha considerado la jurisprudencia en algún caso, que la utilización de la informática en el manejo de los bancos de datos podría considerarse una actividad peligrosa[20], así como también el desarrollo de determinados software destinado a actividades industriales que son en si peligrosas, como podría ser el destinado a centrales nucleares, etc.

Bustamante Alsina, nos dice que los sistemas automatizados de información que emplean la informática, no son cosas peligrosas que dañen por sí mismas, sino instrumentos que el hombre maneja o acciona a su voluntad.

Reitero que se ha dicho que "*No hay cosas peligrosas o no peligrosas en sí, sino que la tal peligrosidad depende de una situación jurídica integrada por la cosa y la particular circunstancia en que se originó el daño*[21].

Tradicionalmente se ha considerado que la responsabilidad objetiva debe estar asociada con actividades que son potencialmente peligrosas y que tienen una alta probabilidad de daño. Tal el caso de la energía eléctrica, la producción o tratamiento de explosivos o materiales radioactivos.

Se ha dicho también con acierto:

> *…la aplicabilidad del artículo 1113 requiere, en cualquier hipótesis, que la cosa tenga una intervención activa en la producción del daño. La caracterización de este concepto ha dado lugar a arduas discusiones doctrinarias en Francia; pero es de entender que la intervención de la cosa es activa cuando tiene acción nociva, o sea, cuando ella causa el daño; en tanto –por lo contrario- su intervención es pasiva cuando no causa el daño, el cual no nace de la cosa de que se trata"*[22].

Creo que cuando se trata de perjuicios que son causados por la cosa interviniente en forma directa, y esa cosa es un elemento de potencial peligro, podría regir el sistema de responsabilidad objetiva del artículo 1113 2º párrafo

20 "*resulta evidente que un Banco de Datos conforma un instrumento riesgoso de por sí (riesgo de la cosa) que hace plenamente aplicable la responsabilidad del dueño o guardián por vicio o riesgo de la cosa (art. 1113, Cód. Civil) que solo puede quedar neutralizada si éste último acredita, sin asomo de duda, la culpa de la víctima o de un tercero por el que no debe responder, o alguna circunstancia de caso fortuito o fuerza mayor que en el caso, no aparecen*". "Gutiérrez, Vicente Juan Carlos Demetrio c/Banco de la Provincia de Buenos Aires y otro s/daños y perjuicios" - CNCIV - SALA K - 22/10/2002.

21 BOFFI BOGGERO, Luis María, *Tratado de las obligaciones*, Ed. Astrea, 1985, t. 6, p. 103

22 ALTERINI – AMEAL – LÓPEZ CABANA; *Derecho de las Obligaciones Civiles y Comerciales*. Ed. Abeledo-Perrot, Buenos Aires, 2006. P. 719.

del Código Civil, pero cuando la cosa no interviene autónomamente en la producción del daño, sino respondiendo al accionar del operador, debe ser aplicado un criterio de atribución de responsabilidad subjetiva conforme al artículo 1109 del Código Civil.

¿Cuál es la naturaleza del ISP? ¿Son editores de la información? Estimo que no, ni el que transmite técnicamente la información ni el buscador que me lleva a ella editaron la información. Ellos no crean el *link*, se crea automáticamente con la indexación que realiza el algoritmo creado. Son sólo distribuidores de información, reitero, no le podemos atribuir entonces una responsabilidad objetiva. Pero sí una responsabilidad subjetiva, en la medida que le podamos probar que ellos conocían el hecho, que fueron partícipes, que tuvieron culpa, que hubo negligencia de su parte.

Sentado este criterio de atribución de responsabilidad subjetiva, debemos ver ahora en qué casos se da la misma.

En primer término considero que los ISP son plenamente responsables con relación a los contenidos propios, generándose en ese supuesto su plena responsabilidad, tanto por transmitir como por alojar estos contenidos que le pertenecen. Pero con relación a los contenidos que le son ajenos y que son fundamentalmente los que transmite o aloja, creo que cualquiera sea la postura adoptada, éste tipo de proveedores sólo podría tener una responsabilidad subjetiva, que surgiría de su culpa o negligencia manifiesta.

También sería responsable cuando se le comunicó la existencia de un contenido ilícito y no tomó las medidas necesarias para evitar que el ilícito se continúe cometiendo.

Podemos afirmar que coincidimos con el consenso doctrinario hoy en día existente en cuanto que sólo cabe hacer responsable a los ISP incluyendo dentro de ellos a los buscadores en dos situaciones:

- Cuando la incorporación ilícita del contenido es manifiesta y no pudo ser ignorada por el proveedor;
- Cuando la incorporación ilícita del contenido no es manifiesta, pero el proveedor ha sido notificado de la existencia de esos contenidos y no toma de inmediato las medidas necesarias para retirar dicho contenido.

Coincido acá con el criterio de la Corte Suprema en el sentido que si el daño es manifiesto y grosero, bastaría con una simple notificación del afectado, mientras que cuando es opinable, dudoso o exige un esclarecimiento, corresponde exigir la notificación judicial o administrativa competente, no bastando la simple comunicación del particular que se considere perjudicado y menos la de cualquier persona interesada, mi pregunta acá sería cuál es el tribunal administrativo competente y me surge la idea que podría ser la Dirección Nacional de Protección de Datos Personales.

Fuera de estos casos creo que no existe responsabilidad de los ISP ya que razones tecnológicas generalmente les impiden ejercer un control permanente de los contenidos de terceros que transmiten o alojan, como también porque aceptar su responsabilidad y consecuentemente para evitarla, obligarlos a eliminar o bloquear contenidos que cree ilícitos, implicaría ni mas ni menos que legalizar la privatización de la censura, toda vez que los ISP, fuera de los casos de contenidos manifiestamente ilícitos, serían quienes disciernen si un contenido es lícito o ilícito, si es nocivo o no.

RESEÑA LEGISLATIVA

Comentarios a la Ley de Infogobierno

Gustavo A. Amoni Reverón*

SUMARIO: I. Aspectos formales: La ley en cifras. 1. Conformación de la Ley. 2. Aspectos organizacionales: Instituciones, sistemas y subsistemas. 3. Principios. 4. Derechos. 5. Tributos: 3 tasas y 3 contribuciones especiales. 6. Infracciones administrativas. II. Implicaciones en el ejercicio de las funciones del Poder Público y del Poder Popular. 1. Objeto y finalidades de la ley y ámbito de aplicación. 2. Ámbito de aplicación. Omisiones de las misiones. 3. Ampliación expresa de la actuación del Poder Público y del Poder Popular por medio de las tecnologías de información.

I. Aspectos formales: La ley en cifras

1. Conformación de la ley

La Ley de Infogobierno fue publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 40.274, el 17 de octubre de 2013, con *vacatio legis* de 10 meses a partir de su publicación, conforme a lo previsto en la disposición final tercera, entrando en vigencia el 17 de agosto de 2014.

Está conformada por 6 títulos, 10 capítulos, 84 artículos, 4 disposiciones transitorias, 2 disposiciones derogatorias y 3 disposiciones finales.

2. Aspectos organizacionales: instituciones, sistemas y subsistemas

Mediante la Ley de Infogobierno se crean 2 instituciones administrativas: un órgano, el Consejo Nacional para el Uso de las Tecnologías de Información (artículo 37) y un ente, la Comisión Nacional de las Tecnologías de Información (artículo 40).

Recibido: 15/7/2013 • Aceptado: 26/8/2014

* Abogado *Summa Cum Laude* de la Universidad de Carabobo. Especialista *Cum Laude* en Derecho Administrativo de la Universidad Católica "Andrés Bello". Profesor de la especialidad en Derecho Administrativo de la Universidad Católica "Andrés Bello".

1 Numeral 6 del artículo 3 de la Ley de Infogobierno: "*Garantizar la transparencia de la gestión pública, facilitando el acceso de las personas a la información pública*".

Además, se instaura un sistema; se trata del Sistema Nacional de Seguridad Informática (numeral 1 del artículo 55) o Sistema Nacional de Protección y Seguridad Informática (artículo 57), cuyo desarrollo es competencia de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), órgano creado mediante el Decreto con Fuerza de Ley de Mensajes de Datos y Firmas Electrónicas N° 1.204, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 37.184, el 10 de febrero de 2001.

Dicho sistema está constituido por 4 subsistemas (artículo 57): (1) El Subsistema de Criptografía Nacional, (2) el Subsistema Nacional de Gestión de Incidentes Telemáticos, (3) el Subsistema Nacional de Informática Forense y, (4) el Subsistema Nacional de Protección de Datos.

3. Principios

La ley establece 11 principios: (1) de acceso por múltiples medios a la actuación del Poder Público (artículo 7); (2) de legalidad en la actuación electrónica (artículo 9); (3) de conservación de comunicaciones, documentos y actuaciones electrónicas del Poder Público y del Poder Popular (artículo 10); (4) de transparencia en la información pública y las actuaciones del Poder Público y Poder Popular (artículo 13); (5) de accesibilidad de las personas, en igualdad de condiciones, a las tecnologías de información (artículo 14); (6) de fomento del conocimiento de las tecnologías de información (artículo 16); (7) de proporcionalidad en la seguridad de acuerdo con la naturaleza de los trámites y actuaciones a realizar ante el Poder Público y el Poder Popular (artículo 22); (8) de aseguramiento de la información, documentos y comunicaciones electrónicas en las actuaciones electrónicas que realicen el Poder Público y el Poder Popular (artículo 23); (9) de coordinación de los proyectos y acciones que desarrollen el Poder Público y el Poder Popular, a fin de consolidar el uso de las tecnologías de información libres en la gestión pública; (10) de colaboración entre el Poder Público y el Poder Popular para alcanzar la consolidación del uso de las tecnologías de información libres en el Estado; y (11) de unidad orgánica lo que implica que los procesos soportados en las tecnologías de información en el Poder Público y el Poder Popular sean interoperables, a fin de apoyar la función y gestión pública que prestan (artículo 30).

4. Derechos

La ley prevé 36 derechos. (1) derecho a relacionarse con el Poder Público mediante tecnologías de información, de forma no exclusiva y excluyente, (artículos 6, 7 y 33), y en consecuencia, tendrán derecho, usando tecnologías de información, a (artículo 8): (2) dirigir peticiones, (3) cumplir con las obligaciones pecuniarias, (4) recibir notificaciones, (5) acceder a la información pública, (6) acceder a los expedientes, (7) conocer y presentar los documentos electrónicos

emanados de los órganos y entes del Poder Público y el Poder Popular, (8) utilizar y presentar ante el Poder Público y demás personas naturales y jurídicas, los documentos electrónicos emitidos por este (disposición final segunda), (9) obtener copias de los documentos electrónicos que formen parte de procedimientos en los cuales se tenga la condición de interesado o interesada, (10) disponer de mecanismos que permitan el ejercicio de la contraloría social, y (11) utilizar las tecnologías de información libres como medio de participación y organización del Poder Popular.

Así mismo, la ley prevé el derecho: (12) al expediente y documentos electrónicos (artículos 11, 26 y disposición final segunda) del Poder Público y del Poder Popular, en este último caso, sobre la base de la normativa especial que se dicte; (13) de las personas con discapacidad o en cualquier otra condición de vulnerabilidad a contar con acceso electrónico adecuado a sus capacidades (artículo 15); (14) a recibir formación, a fin de garantizar la apropiación social del conocimiento (artículo 17); (15) a contar con información íntegra, veraz, oportuna, actual y con el mismo valor que la impresa, en los portales de internet de los órganos y entes del Poder Público y el Poder Popular (artículos 18 y 19); (16) a contar con servicios accesibles, sencillos, expeditos, confiables, pertinentes y auditables, prestados por el Poder Público y el Poder Popular a través de los portales de Internet (artículo 19); (17) a participar en la promoción, colaboración, creación y optimización de los servicios y uso de las tecnologías de información libres (artículo 20); (18) a ejercer contraloría social mediante los servicios prestados por el Poder Público y el Poder Popular (artículo 21); (19) al uso de firma digital o firma electrónica certificada en la actuación del Poder Público (artículo 24); (20) A la protección de datos personales (artículo 25); (21) a la validez de las impresiones de documentos electrónicos con código unívoco cuando sea necesaria la presentación de documentos en papel (artículo 27); (22) a la interoperabilidad en el ámbito del Poder Público y del Poder Popular (artículos 30 y 32); a consultar por medios electrónicos, la veracidad y existencia de los documentos electrónicos, circunstancias o requisitos que posean y sean necesarios para realizar una determinada solicitud, trámite o servicio (artículo 31); (32) de acceder a los archivos y registros del Poder Público y Poder Popular, salvo que se trate de información sobre el honor, vida privada, intimidad, propia imagen, confidencialidad y reputación de las personas, la seguridad y defensa de la Nación (artículo 74); (33) de conocer el uso que le dará el Poder Público y el Poder Popular a la información personal (artículo 75); (34) a la inexigibilidad de consignar documentos en formato físico que contengan datos o información que se intercambien electrónicamente (artículo 76); (35) a la protección de la información que repose en los archivos o registros electrónicos del Poder Público y el Poder Popular; y (36) de los niños, niñas y adolescentes que los datos personales no sean divulgados, cedidos, traspasados, ni compartidos con ninguna persona natural o jurídica, sin el previo consentimiento de su representante legal, salvo cuando el menor de edad sea emancipado, en la investigación de

hechos punibles, por una orden judicial, o cuando así lo determine la ley (artículo 79).

5. Tributos: tres tasas y tres contribuciones especiales

Se crean tres (3) contribuciones especiales, dos de ellas deducibles del impuesto sobre la renta. La tercera (artículo 60) es aplicable a las personas jurídicas cuyo objeto sea la importación, distribución y comercialización de software privativo al Poder Público, actividad por la que pagarán a la Comisión Nacional de Tecnologías de Información el 2,5% de la utilidad neta del ejercicio. Mientras que la segunda (artículo 61), se dirige a toda persona que preste servicios de software privativos al Poder Público, por lo que pagará una contribución del 1,5% de la utilidad neta del ejercicio, a la Comisión Nacional de Tecnologías de Información. La tercera corresponde a los órganos y entes del Poder Público y del Poder Popular que sea autorizado a adquirir, usar y actualizar un software privativo, por lo cual debe pagar una contribución especial al Fondo Nacional de Ciencia, Tecnología e Innovación equivalente entre el 5 y el 10 % del valor de adquisición del software privativo y de los gastos asociados al soporte y uso del software privativo.

Adicionalmente, se crean tres tasas: (1) tasa de 50 unidades tributarias por "*certificación del cumplimiento de las disposiciones de la presente Ley y demás normativa aplicable de los programas informáticos por equipos de computación según su tipo o modelo*" que debe pagar el Poder Público ante la Comisión Nacional de las Tecnologías de Información. En consecuencia, los órganos del Poder Popular quedan excluidos de este pago (artículo 62); (2) tasa de 300 unidades tributarias por certificación y homologación de los equipos o aplicaciones con soporte criptográfico, salvo que se trate de aplicaciones y equipos con soporte criptográfico libre los cuales quedan exentos de pago (artículo 63); y, (3) tasa de 15 a 30 unidades tributarias por la tramitación de la solicitud de acreditación o renovación como unidad de servicios de verificación y certificación que realicen las personas naturales o jurídicas ante la Comisión Nacional de las Tecnologías de Información (artículo 64).

6. Infracciones administrativas

La ley tipifica diecinueve (19) infracciones administrativas. La ejecución de trece (13) de ellas será sancionada por la Comisión Nacional de las Tecnologías de Información, previo procedimiento administrativo, con multa comprendida entre 50 y 500 unidades tributarias.

Tales infracciones son: (1) omitir la elaboración, presentación o implementación del Plan Institucional de Tecnologías de Información; (2) ordenar o autorizar el desarrollo, adquisición, implementación y uso de programas, equipos o servicios de tecnologías de información que no cumplan con las condiciones y

términos de la Ley, salvo autorización; (3) incumplir las normas instruccionales, normas técnicas y estándares dictados por la autoridad competente; (4) omitir registrar ante la autoridad competente los programas informáticos que utilicen o posean y demás requisitos de ley; (5) omitir el uso de certificados y firmas electrónicas; (6) usar equipos o aplicaciones con soporte criptográfico sin la correspondiente aprobación, certificación y homologación de la autoridad competente; (7) alterar un dato, información o documento suministrado por los servicios de información; (8) emplear los datos, información o documentos obtenidos, para fines no autorizados; (9) negar, obstaculizar o retrasar la prestación de un servicio de información; (10) negar o suministrar en forma completa o inexacta información sobre el uso de las tecnologías de información, seguridad informática o interoperabilidad; (11) exigir la consignación, en formato físico, de documentos que contengan datos de autoría, información o documentos que se intercambien electrónicamente; (12) incumplir los niveles de calidad establecidos para la prestación de los servicios de información; (13) celebrar acuerdos de intercambio de datos sin autorización.

Aunado a las infracciones enumeradas, la Contraloría General de la República, de manera exclusiva y excluyente, inhabilitará al servidor público: (14) cuando niegue, obstruya o retrase, de manera injustificada, la prestación de un servicio de información que haya sido ordenado por la autoridad competente; y (15) cuando adquiera un software privativo sin haber sido autorizado expresamente.

Por último, la Comisión Nacional de las Tecnologías de Información revocará las acreditaciones de las unidades de servicios de verificación y certificación, así como las certificaciones que se otorguen, siempre que: (16) se incumplan las condiciones establecidas en la norma instruccional correspondiente para el otorgamiento de la acreditación o certificación; (17) se suministren datos falsos para obtener la acreditación; (18) en la fiscalización, inspección o auditoría de un programa informático, equipo de computación o servicio de información, se hayan incumplido los procedimientos debidos; (19) se haya certificado un programa informático, equipo de computación o servicio de información en contravención con la ley.

II. Implicaciones en el ejercicio de las funciones del Poder Público y del Poder Popular

1. Objeto y finalidades de la ley y ámbito de aplicación

Conforme al artículo 1, la Ley de Infogobierno tiene por objeto establecer los principios, bases y lineamientos que rigen el uso de las tecnologías de información en el Poder Público y el Poder Popular, mas no regula en detalle el uso de las tecnologías de información en el ámbito público y popular, sino que pretende establecer los fundamentos del uso de las tecnologías informáticas, lo

cual deberá ser complementado con el resto del ordenamiento jurídico mientras se dictan las normas especiales que habrán de regir cada materia.

En concreto, el artículo 1 prevé que la Ley de Infogobierno busca mejorar la gestión pública y los servicios que se prestan a las personas, destacando su aplicación en el ejercicio de la función administrativa, principalmente en cuanto a la actividad prestacional o de servicio público, lo cual se ratifica en el numeral 2 del artículo 3 *eiusdem* donde se estatuyen como otro de los fines de la ley:

> *Establecer las condiciones necesarias y oportunas que propicien la mejora continua de los servicios que el Poder Público presta a las personas, contribuyendo así en la efectividad, eficiencia y eficacia en la prestación de los servicios públicos.*

Sobre la base de lo anteriormente expuesto, pareciera estar excluido el ejercicio de las otras funciones del Poder Público: legislativa, judicial, ciudadana y electoral, por usar la división quíntuple constitucional. Este criterio se reitera cuando el mismo artículo prevé que la ley persigue mejorar la gestión pública impulsando la transparencia del sector público[1], la participación y el ejercicio pleno del derecho de soberanía, referencias claras a la actividad administrativa, como se puede desprende del propio título de la ley que alude al gobierno, esto es, a la Administración.

No obstante, el primer párrafo del artículo citado es diáfano cuando prevé el uso de las tecnologías de información en el Poder Público y el Poder Popular, sin discriminar su aplicación exclusiva en sede administrativa.

Conclusión que ratifica el artículo 3 cuando prevé como fines de la ley:

> *Facilitar el establecimiento de relaciones entre el Poder Público y las personas a través de las tecnologías de información*" (numeral 1) y
>
> *Garantizar el ejercicio de los derechos y el cumplimiento de los deberes de las personas, a través de las tecnologías de información*" (numeral 4)

Estas normas de importancia capital porque vienen a disipar cualquier duda respecto de la aplicación de la ley, descartando que solo se dirija al ejercicio de la función administrativa por lo que no puede negarse su implementación en toda la actividad pública: administrativa, judicial, legislativa, electoral y ciudadana.

Además, esta conclusión se refuerza cuando la ley establece, como parte de su objeto, promover el desarrollo de las tecnologías de información libres en el Estado, haciendo alusión al Estado y no a una función específica, la administrativa, apuntando tácitamente a todas las funciones del Poder Público, como se verá en el epígrafe siguiente. Pero tal referencia es únicamente en cuanto al uso de tecnologías libres, con miras a garantizar la independencia tecnológica, la apropiación social del conocimiento, así como la seguridad y defensa de la Nación, lo cual tiene como antecedente el Decreto N° 3.390

publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 38.095 de fecha 28 de diciembre de 2004, mediante el cual se dispone que la Administración Pública, Nacional empleará prioritariamente Software Libre desarrollado con Estándares Abiertos en sus sistemas, proyectos y servicios informáticos, sin vigencia a partir de la disposición derogatoria primera de la Ley de Infogobierno.

En consecuencia, la ley es aplicable a los órganos y entes que ejercen el Poder Público y al Poder Popular, aclarando el artículo 2 de la Ley de Infogobierno, quiénes están sujetos a la ley.

2. Ámbito de aplicación. Omisión de las misiones

En el título anterior, se veía como el artículo 1 de la Ley de Infogobierno se dirige al Poder Público y al Poder Popular. De ahí que deba precisarse qué significan ambas instituciones.

En cuanto al Poder Público, Brewer-Carías[2], considera que es la potestad o situación jurídica general de índole constitucional en la que se encuentran los sujetos de derecho que actúan, conformando el Estado, para materializar sus fines.

En este sentido, el artículo 5 de la Constitución de la República Bolivariana de Venezuela prevé que el Poder Público es ejercido por órganos, entre los que se distribuye desde la óptica político-territorial y funcional, de acuerdo con el artículo 136 *eiusdem*. Así, el Poder Público lo ejercen el Poder Municipal, el Poder Estadal y el Poder Nacional. Mientras que el Poder Público Nacional se divide en Legislativo, Ejecutivo, Judicial, Ciudadano y Electoral; a la vez que los Poderes Públicos Estadal y Municipal cuentan con sus respectivos Poderes Públicos Ejecutivo y Legislativo por ello debe concluirse que el Poder Público implica el ejercicio de distintas funciones[3], mas no de una en especial.

Por su parte, el Poder Popular está definido en el numeral 13 del artículo 5 de la Ley de Infogobierno, repitiendo la definición del artículo 2 de la Ley Orgánica del Poder Popular (LOPP):

> Es el ejercicio pleno de la soberanía por parte del pueblo en lo político, económico, social, cultural, ambiental, internacional, y en todo ámbito del desenvolvimiento y desarrollo de la sociedad, a través de diversas y disímiles formas de organización, que edifican el estado comunal.

2 (Disponible en: http://www.allanbrewercarias.com/Content/449725d9-f1cb-474b-8ab2-41efb849fea3/Content/I.2.61%20BASES%20CONSTITUCIONALES%20DEL%20DA%201982.pdf).

3 En este sentido: Gómez Tapia, J. "Mecanismos constitucionales de control del poder del Estado" en: *Una visión global del México Actual*, De la Rosa Pérez, A. (Coord.), México: Universidad Autónoma del Estado de Hidalgo, 2006, p. 11; y, p. Muro Ruiz, E. *Algunos elementos de técnica legislativa*, México: Universidad Nacional Autónoma de México, 2006, p. 219

Conforme a la ley especial, se ejerce mediante organizaciones[4], expresiones[5] e instancias[6], destacando entre estas últimas los consejos comunales, las comunas, ciudades comunales, federaciones comunales y confederaciones comunales.

Sus funciones radican en ejercer las competencias y atribuciones descentralizadas y transferidas desde la República, los estados y municipios como son la gestión, administración, control de servicios y ejecución de obras atribuidos a aquéllos por la Constitución de la República, para mejorar la eficiencia y los resultados en beneficio del colectivo[7].

Así mismo, los gobiernos de las comunas podrán transferir la gestión, la administración y la prestación de servicios a las diferentes organizaciones del Poder Popular[8].

Conforme a lo expuesto, se incluyen todos los sujetos de derecho que ejercen funciones públicas, y en ese sentido, el artículo 2 de la Ley de Infogobierno prevé que están sometidos a su aplicación los órganos y entes que ejercen el Poder Público Nacional, Estadal, en los distritos metropolitanos, municipios y en las demás entidades locales previstas en la Ley Orgánica del Poder Público Municipal, y en las dependencias federales.

No obstante, del listado citado hasta ahora quedan excluidas las misiones, previstas como una institución diferenciada de los órganos y entes de la Administración Pública, según los artículos 15 y 131 del Decreto con Rango,

4 Artículo 9 LOPP. "*Las organizaciones del Poder Popular son las diversas formas del pueblo organizado, constituidas desde la localidad o de sus referentes cotidianos por iniciativa popular, que integran a ciudadanos y ciudadanas con objetivos e intereses comunes, en función de superar dificultades y promover el bienestar colectivo, para que las personas involucradas asuman sus derechos, deberes y desarrollen niveles superiores de conciencia política. Las organizaciones del Poder Popular actuarán democráticamente y procurarán el consenso popular entre sus integrantes*". Ejemplo de ellas son los Comité de Tierras Urbanas previstos en el artículo 10 del Decreto con Rango, Valor y Fuerza de Ley Especial de Regularización Integral de la Tenencia de la Tierra de los Asentamientos Urbanos o Periurbanos, publicado en la Gaceta Oficial N° 39.668 del 6 de mayo de 2011; así como los Consejos Educativos, definidos en el artículo 3 de la Resolución N° 58 del Ministerio del Poder Popular para la Educación, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 40.029 del 16 de octubre de 2012.

5 Artículo 10 LOPP. "*Las expresiones organizativas del Poder Popular son integraciones de ciudadanos y ciudadanas con objetivos e intereses comunes, constituidas desde la localidad, de sus referentes cotidianos de ubicación o espacios sociales de desenvolvimiento, que de manera transitoria y en base a los principios de solidaridad y cooperación, procuran el interés colectivo*".

6 Artículo 8 LOPP. "*A los efectos de la presente Ley se entiende por… 9. Instancias del Poder Popular: Constituidas por los diferentes sistemas de agregación comunal y sus articulaciones, para ampliar y fortalecer la acción del autogobierno comunal: consejos comunales, comunas, ciudades comunales, federaciones comunales, confederaciones comunales y las que, de conformidad con la Constitución de la República, la ley que regule la materia y su reglamento, surjan de la iniciativa popular*".

7 Artículo 27 de la LOPP.

8 Artículo 28 de la LOPP.

Valor y Fuerza de Ley Orgánica de la Administración Pública (DLOAP), publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 5.890 Extraordinario, el 31 de julio de 2008.

Inclusive, en el artículo 6 de la Ley de Infogobierno, en análisis, se incluyen expresamente los institutos públicos nacionales, estadales, de los distritos metropolitanos y municipales; el Banco Central de Venezuela; las universidades públicas, así como cualquier otra institución del sector universitario de naturaleza pública; enumeración de la que tampoco consta la inclusión de las misiones.

Adicionalmente, el mismo artículo 6 incluye en el ámbito de aplicación de la ley a las demás personas de derecho público nacionales, estadales, distritales y municipales, así como a las sociedades de cualquier naturaleza, las fundaciones, empresas, asociaciones civiles y las demás creadas con fondos públicos o dirigidas por las personas a las que se refiere este artículo, en las que ellas designen sus autoridades, o cuando los aportes presupuestarios o contribuciones en un ejercicio efectuados por las personas referidas en el presente artículo representen el cincuenta o más de su presupuesto.

Como se advierte de la norma citada, al incluirse a las "demás personas de derecho público" se abre una opción para incorporar las misiones; no obstante, el DLOAP no prevé si tendrán personalidad jurídica como los entes, o si no la tendrán, como los órganos. Por esta razón quedarían cubiertas por la previsión anterior, en caso de contar con personalidad jurídica, al ser en consecuencia, un ente público.

Conforme a lo precisado hasta el momento, las misiones serían las únicas figuras jurídicas excluidas de la Ley de Infogobierno; sin embargo, hay al menos dos razones para considerar lo contrario. La primera radica en que el artículo 2 que se está comentando, luego de completar la lista referente al ámbito de aplicación incluyendo las organizaciones y expresiones organizativas del Poder Popular, y las personas naturales o jurídicas, en cuanto les sea aplicable, en los términos establecidos en dicha Ley, incluye "*las demás que establezca la Ley*", expresión suficientemente amplia para incluir las misiones, con lo que no sería posible dejar aspectos de la actuación pública exentas de la aplicación de la normativa de infogobierno. Por su parte, la segunda razón que justifica la aplicación de ley analizada es que normalmente las misiones creadas hasta el momento funcionan bajo la figura de fundaciones[9], entes que están expresamente incluidos entre los sujetos de la ley.

9 Ej. Decreto N° 498 emanado de la Presidencia de la República el 15 de octubre de 2013, publicado en la Gaceta Oficial N° 40.280 del 25 de octubre de 2013, en el que autoriza la creación de la "Fundación Misión José Gregorio Hernández"; "Fundación Misión Hábitat" (cuya creación fue autorizada por el artículo 4 del Decreto N° 4.230 del 23 de enero de 2006, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 38.367 del 27 de ese mes y año, y cuyos Estatutos Sociales fueron protocolizados el 28 de marzo de 2006 ante el Registro Inmobiliario del Primer Circuito del Municipio Baruta del Estado Bolivariano de Miranda, bajo el N° 44,

En definitiva, a modo de cierre de este apartado y atendiendo a lo expuesto en el anterior, la Ley de Infogobierno se aplica al Estado, esto es, a los órganos y entes (donde se incluyen las misiones) que ejercen las distintas funciones del Poder Público, así como también al Poder Popular, de modo que las previsiones normativas que contiene superan el ámbito de la Administración Pública, permeando diáfanamente en la actividad administrativa de los órganos que ejercen las demás funciones del Poder Público así como también de quienes ejercen el Poder Popular, e inclusive se afirma su implementación en el ejercicio de las demás funciones públicas, vale decir, en el ejercicio de la jurisdicción y de la legislación.

3. Ampliación expresa de la actuación del Poder Público y del Poder Popular por medio de las tecnologías de información

Antes de la entrada en vigencia de la Ley de Infogobierno, el Decreto Ley Sobre Mensajes de Datos y Firmas Electrónicas (DLMDFE) ya permitía el uso de las tecnologías de información y comunicación en el ámbito público, otorgando y reconociendo validez y eficacia a los instrumentos tecnológicos previstos en él, siempre que pudieran ser atribuidos "…*a personas naturales o jurídicas, públicas o privadas*…" (artículo 1°), donde quedan incluidos los órganos, entes y misiones del Poder Público así como los sujetos del Poder Popular.

En este sentido, el artículo 6° del DLMDFE establece que la observancia de las solemnidades o formalidades exigidas por las leyes para la formación de determinados actos o negocios jurídicos podrán realizarse utilizando los mecanismos descritos en él, mientras que el artículo 3° contempla que el Estado adoptará las medidas que fueren necesarias para que los organismos públicos puedan desarrollar sus funciones, utilizando las referidas herramientas tecnológicas.

Pero la normativa citada expresa en términos generales el uso de las tecnologías de información en el ámbito público y privado, debiendo acudirse a las normas concretas sobre su utilización, como son las referentes a las firmas electrónicas y mensajes de datos, principalmente, por constituir medios indispensables para documentar y autenticar la actuación pública.

Tomo 22, Protocolo Primero, modificados según Acta de Reforma de fecha 23 de abril de 2007 en el referido Registro Inmobiliario anotada bajo el N° 12, Tomo 5, Protocolo Primero; la "Fundación Misión Identidad", adscrita al Ministerio del Poder Popular para Relaciones Interiores y Justicia, autorizada su creación mediante decreto N° 3.654 dictado por el Presidente de la República en Consejo de Ministros del 9 de mayo de 2005, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 38.188 del 17 de mayo de 2005 y debidamente protocolizada en el Registro Inmobiliario del Segundo Circuito del Municipio Libertador del Distrito Capital, en fecha 6 de junio de 2005, bajo el N° 23, Tomo 27, Protocolo Primero, publicada en la Gaceta Oficial N° 38.202 de la misma fecha; y la "Fundación Misión Che Guevara" autorizada mediante el Decreto N° 6.316 de fecha 12 de agosto de 2008 y publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 38.995 del 15 de ese mismo mes y año.

Por ende, conforme al artículo 8 del DLMDFE "*Cuando la ley requiera que la información conste por escrito, ese requisito quedará satisfecho con relación a un Mensaje de Datos, si la información que éste contiene es accesible para su ulterior consulta*", mientras que el artículo 1° del DLMDFE otorga y reconoce eficacia y valor jurídico "*…al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material…*".

A partir de tales normas es válido, desde la óptica jurídica, generar escritos público electrónicos, pero estos equivaldrían a una hoja sin firmar; por ello, el referido instrumento jurídico también le reconoce valor en Derecho a la firma electrónica, estableciendo 4 formas de firmas (firma simple, concordada, avanzada y certificada) autorizando su uso el artículo 6º, para ejecutar cualquier acto o negocio jurídico para el cual la ley exija la firma autógrafa, tanto por parte de personas naturales como jurídicas, privadas y públicas. No obstante, le Ley de Infogobierno limita al uso de la firma electrónica en el ejercicio del Poder Público al uso restrictivo de la firma digital o firma electrónica certificada, (artículo 24) llegando a sancionar con multa de 50 a 500 unidades tributarias al empleado público que en sus actuaciones electrónicas, omita el uso de certificados y firmas electrónicas (numeral 5 del artículo 81).

Toda esta actividad pública informática del DLMDFE dispone inclusive de base constitucional. Al respecto, el artículo 110 de la Constitución reconoce los servicios de información como instrumentos fundamentales para el desarrollo económico, social y político del país.

Regulación, que en materia administrativa encuentra respaldo en los Decretos Leyes de la Administración Pública (DLOAP) y de Simplificación de Trámites Administrativos (DLSTA), que prevén el uso de las tecnologías de la información en el ejercicio de la actividad administrativa.

Normas complementadas con el Decreto Nº 825 del 22 de mayo de 2000 sobre Internet como prioridad, que prevé que la Administración Pública deberá utilizar preferentemente Internet para el intercambio de información con los particulares; con la Providencia Administrativa Nº 004-10, emanada de la Superintendencia de Servicios de Certificación Electrónica (Suscerte) el 12 de marzo de 2010, que exhorta a todos los entes, órganos y demás Instituciones de la Administración Pública, a propiciar el uso de Certificados Electrónicos y Firmas Electrónicas en la emisión de actos administrativos de efectos particulares, así como en la recepción de solicitudes y procesos ante la Administración Pública, efectuados a través de las tecnología de información y comunicación; y, en el aparte N° 7 de la Carta Iberoamericana de Gobierno Electrónico, que consagra el derecho de los ciudadanos a relacionarse electrónicamente con la Administración Pública.

Incluso, más cercano a la entrada en vigencia de la Ley de Infogobierno, el Decreto con Rango, Valor y Fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes

del Estado[10], también conocido como Decreto Ley de Interoperabilidad (DLI), igualmente contempla el uso de las tecnologías informáticas por parte de los órganos del Poder Público Nacional, Estadal y Municipal y las personas de derecho público nacionales, estadales, distritales y municipales.

De modo que el DLI consagra expresamente lo que ya era posible con el DLMDFE, la sustanciación electrónica de expedientes administrativos (artículo 49[11]). Potestad reiterada en la Ley de Infogobierno, en el numeral 8 del artículo 3, cuando establece como uno de sus fines: "*Contribuir en los modos de organización y funcionamiento del Poder Público, apoyando la simplificación de los trámites y procedimientos administrativos que éstos realizan*" y al mismo tiempo, ampliada a cualquier otro tipo de expediente, inclusive judicial, al no discriminar al respecto cuando consagra el derecho al expediente y a los documentos electrónicos (artículos 11, 26 y disposición final segunda) del Poder Público, donde no hay razón para excluir a los tribunales.

Esto es así aunque no exista una declaración expresa de su uso en el proceso jurisdiccional, puesto que los derechos que contempla la ley no están limitados al ámbito administrativo. Derivado de ello, cuando la Ley de Infogobierno reconoce el derecho a relacionarse con el Poder Público mediante tecnologías de información (artículos 6, 7 y 33), así como lo prevé el DLMDFE, puede entenderse que se trata de procedimientos administrativos o procesos jurisdiccionales accesibles, sencillos, expeditos, confiables, pertinentes y auditables, prestados por el Poder Público a través de los portales de internet que todos deben tener (artículo 19), con el mismo valor jurídico que la información que conste en papel[12], y que en el caso de la Administración ya tenía consagración legal[13].

En consecuencia, la informatización de la actividad administrativa se ve aún más reforzada con la Ley de Infogobierno, al consagrarse el derecho a consultar

10 Decreto N° 9.051, publicado en la Gaceta Oficial N° 39.945 del 15 de junio de 2012.

11 "*Los órganos y entes del Estado podrán sustanciar sus actuaciones administrativas, total o parcialmente, por medios electrónicos. Serán aplicables a los expedientes administrativos electrónicos, todas las normas sobre procedimiento administrativo, en la medida en que no sean incompatibles con la naturaleza del medio empleado.Los funcionarios públicos están obligados a aceptar de los ciudadanos, la consignación de documentos en físico para su incorporación en un expediente electrónico. En tales casos, se procederá a la digitalización de los documentos para su incorporación al expediente electrónico, en los términos establecidos en el presente Decreto con Rango, Valor y Fuerza de Ley.El expediente administrativo electrónico que resulte de la sustanciación electrónica tendrá la misma validez jurídica y probatoria que el expediente físico*".

12 Artículo 18 "*Los órganos y entes del Poder Público y el Poder Popular, en el ejercicio de sus competencias, deben contar con un portal de internet... La información contenida en los portales de internet tiene el mismo carácter oficial que la información impresa que emitan*".

13 Artículo 11 "*… Cada órgano y ente de la Administración Pública deberá establecer y mantener una página en Internet, que contendrá entre otras, la información que se considere relevante, los datos correspondientes a su misión, organización, procedimiento, normativa que lo regula, servicios que presta, documentos de interés para las personas, ubicación de sus dependencias e información de contactos*".

por medios electrónicos la veracidad y existencia de los documentos electrónicos, circunstancias o requisitos que posean y sean necesarios para realizar una determinada solicitud, trámite o servicio (artículo 31)[14]; dirigir peticiones; recibir notificaciones electrónicas; acceder a los expedientes y archivos electrónicos[15]; así como presentar, utilizar y copiar los documentos emanados de los órganos y entes del Poder Público y el Poder Popular; combinar el uso de documentos en papel, electrónicos y mensajes de datos reiterando la validez de las impresiones de documentos electrónicos con código unívoco cuando sea necesaria la presentación de documentos en papel (artículo 27)[16]; y hasta efectuar pagos electrónicos[17].

Asimismo, no se advierten obstáculos insalvables para que esta normativa también sirva de fundamento para su implementación en el terreno procesal, de modo que la presentación de la demanda al igual que cualquier otro documento, la realización de notificaciones y citaciones, aunado a la conformación del expediente, todo en formato electrónico, pudiera ser realidad, como se desprende

14 *Idem*.

15 La disposición final segunda de la Ley de Infogobierno, al igual que lo hace el artículo 51 del DLI, le impone al Poder Público el deber de digitalizar sus archivos físicos y de firmar los mensajes de datos que resulten de esta digitalización por una persona autorizada, con el fin de certificar dichas copias electrónicamente. Por esta razón, las páginas de Internet oficiales en las que se registran actos jurídicos públicos, bien sea leyes, actos administrativos o decisiones judiciales, deberán incorporar una copia digital firmada electrónicamente por un empleado encargado al efecto a fin de darle pleno valor jurídico en cumplimiento de la ley.

16 Esta norma ya estaba prevista en el artículo 53 del DLI: "*Cuando los datos de autoría, información o documentos emanados de los órganos y entes del Estado se encuentren contenidos en un mensaje de dato, sea porque estos han sido digitalizados o han sido tramitados en formato electrónico, y la ley exija que deben constar por escrito; tal requisito quedará satisfecho, cuando el mensaje de dato correspondiente se presente en formato impreso y contenga el código unívoco que lo identifique y permita su recuperación en el repositorio digital institucional correspondiente*".

17 La Ley de Infogobierno también permite cumplir con obligaciones pecuniarias por lo que el pago de tasas administrativas quedaría cubierto; situación que ya era posible a la luz de las leyes vigentes antes de esta, independientemente de que se trate del pago de tasas en efectivo o mediante timbres fiscales. En el primer caso, bastaría una transferencia electrónica en la cuenta dispuesta por la Administración al efecto, de conformidad con los artículos 21 y 22 del Decreto con Fuerza de Ley de Simplificación de Trámites Administrativos, de plena concordancia con lo sugerido en el aparte 9.b de la Carta Iberoamericana de Gobierno Electrónico. Para lo cual, la Administración debe contar con las herramientas necesarias para tramitar y comprobar dicho pago. Al tiempo que en el segundo caso, la LTF (parágrafo único del artículo 1) faculta a la Administración para que elabore las planillas necesarias para lograr la recaudación de tasas y contribuciones de su competencia y mandar a efectuar el enteramiento mediante el pago en las oficinas receptoras de fondos nacionales "…cuando no sean utilizables los timbres móviles." Por esta razón, ante la imposibilidad de inutilizar timbres fiscales tangibles en la emisión de un acto administrativo electrónico, el órgano o ente competente deberá elaborar las planillas electrónicas necesarias para dicho pago, el cual, podría materializarse mediante una transferencia bancaria electrónica.

de algunas experiencias jurisprudenciales patrias sobre el tema, anteriores a la entrada en vigencia de la Ley de Infogobierno[18].

Por último, es insoslayable tener claro que el uso de las tecnologías de información, como las denomina la Ley de Infogobierno, o de información y comunicación, como también se les conoce, supone ampliar y facilitar el ejercicio de derechos e intereses, y por ello es válidamente operante en conjunto con las normas especiales que rigen los procedimientos administrativos y procesos jurisdiccionales.

Lo que no puede pretenderse, y esto lo aclara expresamente La ley de Infogobierno, es restringir o discriminar a las personas, restringiendo derechos legales de aplicación preferente, como los previstos en la Ley Orgánica de Procedimientos Administrativos o en las leyes orgánicas procesales, imponiéndose como único medio de acceso al Poder Público y al Poder Popular, el uso de la tecnología informática, "*por lo que, el acceso a la prestación de*

18 En cuanto a la presentación de **demandas y escritos recursivos electrónicos**, Ver: A. *Sala Constitucional* (Sentencia N° 523 del 9 de abril de 2001, sentencia N° 408 del 4 de abril de 2011, sentencia N° 1603 del 5 de diciembre de 2012, sentencia N° 1736 del 17 de diciembre de 2012, sentencia N° 1549 del 11 de noviembre de 2013, sentencia N° 299 del 16 de abril de 2013, sentencia N° 418 del 26 de abril de 2013, sentencia N° 633 del 30 de mayo de 2013, sentencia N° 640 del 30 de mayo de 2013, sentencia N° 916 del 15 de julio de 2013, sentencia N° 957 del 16 de julio de 2013, sentencia N° 987 del 16 de julio de 2013, sentencia N° 1122 del 8 de agosto de 2013 y sentencia N° 1635 del 19 de noviembre de 2013), B. *Sala Electoral* (sentencia N° 76 del 13 de junio de 2001 y sentencia N° 203 del 14 de noviembre de 2012) y C. *Sala de Casación Social* (sentencia N° 1092 del 13 de noviembre de 2013). Respecto de las **citaciones y notificaciones electrónicas**, ver: *Decisiones judiciales. A. Sala Constitucional (*Sentencia N° 7 del 1° de febrero de 2000, sentencia N° 1.336 del 3 agosto de 2001, sentencia N° 2535 del 5 de agosto de 2005, sentencia N° 1533 del 16 de noviembre de 2012, sentencia N° 993 del 16 de julio de 2013, sentencia N° 1122 del 8 de agosto de 2013 y sentencia N° 1777 del 16 de diciembre de 2013); B. *Sala Político Administrativa (*Sentencia Nº 1121 del 10 de agosto de 2011 y sentencia N° 327 del 12 marzo de 2014); y C. *Juzgado de Sustanciación de la Sala Político Administrativa* (auto N° 339 del 7 de agosto de 2012). Por último, en lo que concierne a las **pruebas electrónicas**, ver: A. *Sala de Casación Social* (Sentencia N° 203 del 5 de abril 2005, sentencia N° 198 del 7 de febrero de 2006, sentencia N° 687 del 4 de abril de 2006, sentencia N° 2028 del 12 de diciembre de 2006, sentencia N° 245 del 6 de marzo de 2008, sentencia N° 808 del 11 de junio de 2008, sentencia N° 264 del 5 de marzo de 2007, sentencia N° 1443 del 5 de octubre de 2009, sentencia N° 1092 del 8 de agosto de 2010, sentencia N° 1044 del 4 de octubre de 2010, sentencia N° 970 del 5 de agosto de 2011, sentencia N° 1354 del 4 de diciembre de 2012, sentencia N° 396 del 11 de junio de 2013, sentencia N° 640 del 8 de agosto de 2013 y sentencia N° 788 del 26 de septiembre de 2013); B. *Sala Político Administrativa* (a. *Actos jurídicos privados:* Sentencia N° 157 del 13 de febrero de 2008, sentencia N° 460 de 5 de octubre de 2011 y b. *Actos administrativos:* Sentencia N° 1.011 del 8 de julio de 2009, sentencia N° 1.437 del 8 de octubre de 2009, sentencia N° 100 del 3 de enero de 2010, sentencia N° 1.801 del 15 de diciembre de 2011, sentencia N° 103 del 29 de enero de 2014); C. *Sala de Casación Civil* (Sentencia N° 769 del 24 de octubre de 2007, sentencia N° 460 del 5 de octubre de 2011, sentencia N° 274 del 30 de mayo de 2013, sentencia N° 550 del 24 de septiembre de 2013 y sentencia N° 609 del 11 de octubre de 2013); y, D. *Sala Constitucional* (Sentencia N° 2.370 del 19 de diciembre de 2007).

los servicios públicos, como a cualquier actuación del Poder Público, debe ser garantizada por cualquier medio existente" (artículo 7).

Derivando la obligación para el Estado de revisar aquellos procedimientos administrativos que en la actualidad solamente pueden completarse o al menos iniciarse, por medio de las tecnologías de información, los cuales pasan a ser ilegales desde la entrada en vigencia de la Ley de Infogobierno, el 17 de agosto de 2014, salvo disposición legal en contrario.

LEGISLACIÓN

Gaceta Oficial de la República Bolivariana de Venezuela
N° 40.274 del 17 de octubre de 2013

LA ASAMBLEA NACIONAL DE LA REPÚBLICA
BOLIVARIANA DE VENEZUELA

DECRETA

La siguiente;

LEY DE INFOGOBIERNO

Título I
Disposiciones Fundamentales

Capítulo I
Normas generales

Objeto de la ley

Artículo 1 Esta Ley tiene por objeto establecer los principios, bases y lineamientos que rigen el uso de las tecnologías de información en el Poder Público y el Poder Popular, para mejorar la gestión pública y los servicios que se prestan a las personas; impulsando la transparencia del sector público; la participación y el ejercicio pleno del derecho de soberanía; así como, promover el desarrollo de las tecnologías de información libres en el Estado; garantizar la independencia tecnológica; la apropiación social del conocimiento; así como la seguridad y defensa de la Nación.

Ámbito de aplicación

Artículo 2 Están sometidos a la aplicación de la presente Ley:

1. Los órganos y entes que ejercen el Poder Público Nacional.
2. Los órganos y entes que ejercen el Poder Público Estadal.
3. Los órganos y entes que ejercen el Poder Público en los distritos metropolitanos.
4. Los órganos y entes que ejercen el Poder Público Municipal y en las demás entidades locales previstas en la Ley Orgánica del Poder Público Municipal.

;

5. Los órganos y entes que ejercen el Poder Público en las dependencias federales.

6. Los institutos públicos nacionales, estadales, de los distritos metropolitanos y municipales.

7. El Banco Central de Venezuela.

8. Las universidades públicas, así como cualquier otra institución del sector universitario de naturaleza pública.

9. Las demás personas de derecho público nacionales, estadales, distritales y municipales.

10. Las sociedades de cualquier naturaleza, las fundaciones, empresas, asociaciones civiles y las demás creadas con fondos públicos o dirigidas por las personas a las que se refiere este artículo, en las que ellas designen sus autoridades, o cuando los aportes presupuestarios o contribuciones en un ejercicio efectuados por las personas referidas en el presente artículo representen el cincuenta o más de su presupuesto.

11. Las organizaciones y expresiones organizativas del Poder Popular.

12. Las personas naturales o jurídicas, en cuanto les sea aplicable, en los términos establecidos en esta Ley.

13. Las demás que establezca la Ley.

Finalidad de la ley

Artículo 3 Esta Ley tiene como fines;

1. Facilitar el establecimiento de relaciones entre el Poder Público y las personas a través de las tecnologías de información.

2. Establecer las condiciones necesarias y oportunas que propicien la mejora continua de los servicios que el Poder Público presta a las personas, contribuyendo así en la efectividad, eficiencia y eficacia en la prestación de los servicios públicos.

3. Univerzalizar el acceso de las personas a las tecnologías de información libres y garantizar su apropiación para beneficio de la sociedad.

4. Garantizar el ejercicio de los derechos y el cumplimiento de los deberes de las personas, a través de las tecnologías de información.

5. Promover el empoderamiento del Poder Popular a través de la generación de medios de participación y organización de las personas, haciendo uso de las tecnologías de información.

6. Garantizar la transparencia de la gestión pública, facilitando el acceso de las personas a la información pública.

7. Apoyar el fortalecimiento de la democracia participativa y protagónica en la gestión pública y el ejercicio de la contraloría social.

8. Contribuir en los modos de organización y funcionamiento del Poder Público, apoyando la simplificación de los trámites y procedimientos administrativos que éstos realizan.

9. Establecer los principios para la normalización y estandarización en el uso de las tecnologías de información, a los sujetos sometidos a la aplicación de esta Ley.

10. Promover la adquisición, desarrollo, investigación, creación, diseño, formación, socialización, uso e implementación de las tecnologías de información libres a los sujetos sometidos a la aplicación de esta Ley.

11. Establecer las bases para el Sistema Nacional de Protección y Seguridad de la Información, en los términos establecidos en la presente Ley y por otros instrumentos legales que regulen la materia.

12. Fomentar la independencia tecnológica y con ello fortalecer el ejercicio de la soberanía nacional, sobre la base del conocimiento y uso de las tecnologías de información libres en el Estado.

Interés público y carácter estratégico

Artículo 4 Son de interés público y estratégico las tecnologías de información, en especial las tecnologías de información libres, como instrumento para garantizar la efectividad, transparencia, eficacia y eficiencia de la gestión pública; profundizar la participación de la ciudadanía en los asuntos públicos; el empoderamiento del Poder Popular y contribuir corresponsablemente en la consolidación de la seguridad, defensa y soberanía nacional.

Definiciones

Artículo 5 A los efectos de la presente Ley, se entenderá por:

1. **Actuación electrónica**: Capaz de producir efectos jurídicos.
2. **Acceso abierto**: Característica de los documentos públicos que se refiere a su disponibilidad gratuita en la internet pública, que permite a cualquier usuario leer, descargar, copiar, distribuir, imprimir, buscar o añadir un enlace al texto completo de esos artículos, rastrearlos para su indización, incorporarlos como datos en un software, o utilizarlos para cualquier otro propósito que sea legal, sin barreras financieras, legales o técnicas, aparte

de las que son inseparables del acceso mismo a la internet. La única limitación en cuanto a reproducción y distribución, y el único papel del copyright en cuanto a los derechos patrimoniales en este ámbito, debe ser dar a los autores el control sobre la integridad de sus trabajos y el derecho a ser adecuadamente reconocidos y citados.

3. **Código fuente**: Texto escrito en un lenguaje de programación específico, contentivo de un conjunto de instrucciones que se puede compilar para generar un programa que se ejecuta en un computador, es el conjunto de líneas de texto escritas en un lenguaje de programación específico, que al ser procesadas por los compiladores e interpretadores adecuados, generan exactamente dicho programa que es ejecutado por el computador.
4. **Conocimiento libre**: Es todo aquel conocimiento que puede ser aprendido, interpretado, aplicado, enseñado y compartido libremente y sin restricciones, pudiendo ser utilizado para la resolución de problemas o como punto de partida para la generación de nuevos conocimientos.
5. **Criptografía**: Rama inicial de las matemáticas y en la actualidad también de la informática, que hace uso de métodos y técnicas con el objeto principal de hacer ilegible, cifrar y proteger un mensaje o archivo por medio de un algoritmo, usando una o más claves.
6. **Documento electrónico**: Documento digitalizado que contiene un dato, diseños o información acerca de un hecho o acto, capaz de causar efectos jurídicos.
7. **Estándares abiertos**: Especificaciones técnicas, publicadas y controladas por alguna organización que se encarga de su desarrollo, aceptadas por la industria de las tecnologías de información, y que están a disposición de cualquier usuario para ser implementadas.
8. **Hardware libre**: Dispositivos de hardware, componentes electrónicos o mecánicos diseñados para su uso en cualquier área científico técnica, cuyas especificaciones y diagramas esquemáticos son de acceso público, garantizando el total acceso al conocimiento de su funcionamiento y fabricación, y que reconociendo los derechos de autor, no están sometidos a normativas legales del sistema de patentes de apropiación privativa, otorgándose las mismas libertades contempladas en el software libre para su uso con cualquier propósito y en cualquier área de aplicación, libertad de modificación y

adaptación a necesidades específicas, y la libertad para su redistribución.

9. **Informática forense**: también llamado computo forense, computación forense, análisis forense digital o examen forense digital es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.
10. **Infraestructuras críticas**: Infraestructuras críticas también conocidas como estratégicas, son aquéllas que proporcionan servicios esenciales y cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre tales servicios.
11. **Interoperabilidad**: Capacidad que tienen las organizaciones dispares y diversas para intercambiar, transferir y utilizar, de manera uniforme y eficiente datos, información y documentos por medios electrónicos, entre sus sistemas de información.
12. **Normas instruccionales**: Todas aquellas providencias administrativas de efectos generales, instructivos o circulares, de carácter obligatorio, dictados con el fin de garantizar el efectivo uso de las tecnologías de información y la seguridad informática, en los términos establecidos en esta Ley.
13. **Poder Popular**: Es el ejercicio pleno de la soberanía por parte del pueblo en lo político, económico, social, cultural, ambiental, internacional, y en todo ámbito del desenvolvimiento y desarrollo de la sociedad, a través de diversas y disímiles formas de organización, que edifican el estado comunal.
14. **Prospectiva tecnológica**: La prospectiva tecnológica también conocida como vigilancia tecnológica, es un proceso sistemático que analiza el estado actual y las perspectivas de progreso científico y tecnológico para identificar áreas estratégicas de investigación y tecnologías emergentes para concentrar los esfuerzos de inversión y así obtener los mayores beneficios económicos o sociales, la prospectiva tecnológica está orientada a un conjunto de técnicas que permiten definir la relevancia de una tecnología en un momento futuro.
15. **Seguridad de la información**: Condición que resulta del establecimiento y mantenimiento de medios de protección, que garanticen un estado de inviolabilidad de influencias o de actos hostiles específicos que puedan propiciar el acceso a la información no autorizada, o que afecten la operatividad de las funciones de un sistema de computación, bajo los principios

de confidencialidad, integridad, privacidad y disponibilidad de la información.

16. **Software libre**: Programa de computación en cuya licencia el autor o desarrollador garantiza al usuario el acceso al código fuente y lo autoriza a usar el programa con cualquier propósito, copiarlo, modificarlo y redistribuirlo con o sin modificaciones, preservando en todo caso el derecho moral al reconocimiento de autoría.
17. **Tecnología de información**: Tecnologías destinadas a la aplicación, análisis, estudio y procesamiento en forma automática de información. Esto incluye procesos de: obtención, creación, cómputo, almacenamiento, modificación, manejo, movimiento, transmisión, recepción, distribución, intercambio, visualización, control y administración, en formato electrónico, magnético, óptico, o cualquier otro medio similar o equivalente que se desarrollen en el futuro, que involucren el uso de dispositivos físicos y lógicos.
18. **Tecnologías de información libres**: Son aquellas tecnologías con estándares abiertos que garantizan el acceso a todo el código fuente y la transferencia del conocimiento asociado para su comprensión; libertad de modificación; libertad de uso en cualquier área, aplicación o propósito y libertad de publicación del código fuente y sus modificaciones.
19. **Usabilidad**: Se refiere a los atributos que deben tener los sistemas de información para que sean comprendidos, aprendidos y usados con facilidad por sus usuarios o usuarias.

Capítulo II

Principios y bases del uso de las tecnologías de información

Obligatoriedad del uso de las tecnologías de información

Artículo 6 El Poder Público, en el ejercicio de sus competencias, debe utilizar las tecnologías de información en su gestión interna, en las relaciones que mantengan entre los órganos y entes del Estado que lo conforman, en sus relaciones con las personas y con el Poder Popular, de conformidad con esta Ley y demás normativa aplicable.

El Poder Popular debe utilizar las tecnologías de información en los términos y condiciones establecidos en la ley.

Principio de igualdad

Artículo 7 La obligación establecida en el artículo anterior en ningún caso se entenderá como un modo de restricción o discriminación para las personas, por lo que, el acceso a la prestación de los servicios públicos, como a cualquier actuación del Poder Público, debe ser garantizada por cualquier medio existente, sin perjuicio de las medidas que la presente Ley y la normativa que a tal efecto se establezca, con el fin de hacer efectivo el derecho de las personas a utilizar las tecnologías de información en sus relaciones con el Estado.

Derecho de las personas

Artículo 8 En las relaciones con el Poder Público y el Poder Popular, las personas tienen derecho a:

1. Dirigir peticiones de cualquier tipo haciendo uso de las tecnologías de información, quedando el Poder Público y el Poder Popular obligados a responder y resolver las mismas de igual forma que si se hubiesen realizado por los medios tradicionales, en los términos establecidos en la Constitución de la República y la Ley.
2. Realizar pagos, presentar y liquidar impuestos, cumplir con las obligaciones pecuniarias y cualquier otra clase de obligación de esta naturaleza, haciendo uso de las tecnologías de información.
3. Recibir notificaciones por medios electrónicos en los términos y condiciones establecidos en la ley que rige la materia de mensajes de datos y las normas especiales que la regulan.
4. Acceder a la información pública a través de medios electrónicos, con igual grado de confiabilidad y seguridad que la proporcionada por los medios tradicionales.
5. Acceder electrónicamente a los expedientes que se tramiten en el estado en que éstos se encuentren, así como conocer y presentar los documentos electrónicos emanados de los órganos y entes del Poder Público y el Poder Popular, haciendo uso de las tecnologías de información.
6. Utilizar y presentar ante el Poder Público y demás personas naturales y jurídicas, los documentos electrónicos emitidos por éste, en las mismas condiciones que los producidos por cualquier otro medio, de conformidad con la presente Ley y la normativa aplicable.
7. Obtener copias de los documentos electrónicos que formen parte de procedimientos en los cuales se tenga la condición de interesado o interesada.

8. Disponer de mecanismos que permitan el ejercicio de la contraloría social haciendo uso de las tecnologías de información.
9. Utilizar las tecnologías de información libres como medio de participación y organización del Poder Popular.

Principio de legalidad

Artículo 9 Las actuaciones que realicen el Poder Público y el Poder Popular, deben sujetarse a la asignación, distribución y ejercicio de sus competencias de conformidad con lo establecido en la Constitución de la República, la presente Ley y las normas que rigen la materia.

Principio de conservación documental

Artículo 10 Las comunicaciones, documentos y actuaciones electrónicas que realicen el Poder Público y el Poder Popular se conservarán de conformidad con las condiciones que determine la Ley y la normativa especial aplicable.

Repositorio digital del Poder Público y el Poder Popular

Artículo 11 El Poder Público debe contar con repositorios digitales en los cuales se almacene la información que manejen, así como los documentos que conformen el expediente electrónico, a fin de que sean accesibles, conservados o archivados, de conformidad con la presente Ley y la normativa que regule la materia.

El Poder Popular está sometido a la obligación aquí establecida en los términos y condiciones de la normativa a tal efecto se dicte.

Repositorio digital de programas informáticos

Artículo 12 El Poder Público y el Poder Popular deben registrar ante la autoridad competente los programas informáticos que utilicen o posean; su licenciamiento, código fuente y demás información y documentación que determine la norma instruccional correspondiente.

Principio de transparencia

Artículo 13 El uso de las tecnologías de información en el Poder Público y el Poder Popular garantiza el acceso de la información pública a las personas, facilitando al máximo la publicidad de sus actuaciones

como requisito esencial del Estado democrático y Social de Derecho y de Justicia, salvo aquella información clasificada como confidencial o secreta, de conformidad con la ley que regule el acceso a la información pública y otras normativas aplicables.

Principio de accesibilidad

Artículo 14 El Poder Público, en forma corresponsable con el Poder Popular, participa en el desarrollo, implementación y uso de las tecnologías de información libres, a fin de garantizar a las personas, en igualdad de condiciones, el acceso y la apropiación social del conocimiento asociado a esas tecnologías.

Condiciones de accesibilidad y usabilidad

Artículo 15 En el diseño y desarrollo de los sistemas, programas, equipos y servicios basados en tecnologías de información, se debe prever las consideraciones de accesibilidad y usabilidad necesarias para que éstos puedan ser utilizados de forma universal por aquellas personas que, por razones de discapacidad, edad, o cualquier otra condición de vulnerabilidad, requieran de diferentes tipos de soportes o canales de información.

Fomento del conocimiento de las tecnologías de información

Artículo 16 Es deber del Poder Público, en forma corresponsable con el Poder Popular, garantizar a todas las personas, a través del sistema educativo los medios para la formación, socialización, difusión, innovación, investigación y comunicación en materia de tecnologías de información libres, según los lineamientos de los órganos rectores en las materias.

Formación

Artículo 17 El Poder Público debe proporcionar la formación en materia de tecnologías de información libres de sus respectivos colectivos laborales, para que interactúen con los sistemas y aplicaciones, desempeñando eficientemente sus labores y funciones en la gestión pública. Asimismo debe facilitar la formación de las personas, a fin de garantizar la apropiación social del conocimiento.

Portal de Internet

Artículo 18 Los órganos y entes del Poder Público y el Poder Popular, en el ejercicio de sus competencias, deben contar con un portal de internet bajo su control y administración. La integridad, veracidad y actualización de la información publicada y los servicios públicos que se presten a través de los portales es responsabilidad del titular del portal. La información contenida en los portales de internet tiene el mismo carácter oficial que la información impresa que emitan.

Servicios de información

Artículo 19 Los servicios prestados por el Poder Público y el Poder Popular a través de los portales de internet deben ser accesibles, sencillos, expeditos, confiables, pertinentes y auditables, y deben contener información completa, actual, oportuna y veraz, de conformidad con la ley y la normativa especial aplicable.

Derecho a la participación en la promoción de los servicios y uso de las tecnologías de información

Artículo 20 El Poder Público y el Poder Popular están obligados a garantizar en sus portales de internet el ejercicio del derecho de las personas a participar, colaborar y promover el uso de las tecnologías de información libres, creación de nuevos servicios electrónicos o mejoramiento de los ya existentes.

Mecanismos de ejercicio de contraloría social

Artículo 21 Los servicios prestados por el Poder Público y el Poder Popular deben contener mecanismos que permitan la promoción, desarrollo y consolidación de la contraloría social como medio de participación de las personas y sus organizaciones sociales, para garantizar que la inversión pública se realice de manera transparente y eficiente, en beneficio de los intereses de la sociedad y que las actividades del sector privado no afecten los intereses colectivos o sociales.

Principio de proporcionalidad

Artículo 22 En las actuaciones que realicen el Poder Público y el Poder Popular a través de las tecnologías de información, sólo se exigirán a las personas las medidas de seguridad necesarias según la

naturaleza de los trámites y actuaciones a realizar. Igualmente, se requerirán los datos que sean estrictamente necesarios para tramitar los asuntos que haya solicitado, a los fines de garantizar el cumplimiento de los principios y derechos establecidos en la Constitución de la República y la ley.

Principio de seguridad

Artículo 23 En las actuaciones electrónicas que realicen el Poder Público y el Poder Popular se debe garantizar la integridad, confidencialidad, autenticidad y disponibilidad de la información, documentos y comunicaciones electrónicas, en cumplimiento a las normas y medidas que dicte el órgano con competencia en materia de seguridad de la información.

Servicios de certificación y firma electrónica

Artículo 24 El Poder Público debe garantizar la integridad, confidencialidad, autenticidad y disponibilidad de la información, a través del uso de certificados y firmas electrónicas emitidas dentro de la cadena de confianza de certificación electrónica del Estado venezolano, de conformidad con el ordenamiento jurídico venezolano y la legislación que rige la materia.

De la protección de datos personales

Artículo 25 El uso de las tecnologías de información por el Poder Público y el Poder Popular comprende la protección del honor, vida privada, intimidad, propia imagen, confidencialidad y reputación de las personas; en consecuencia, está sujeto a las limitaciones que establezca la ley sobre la materia.

Validez de los archivos y documentos electrónicos

Artículo 26 Los archivos y documentos electrónicos que emitan el Poder Público y el Poder Popular, que contengan certificaciones y firmas electrónicas tienen la misma validez jurídica y eficacia probatoria que los archivos y documentos que consten en físico.

Copias impresas de los documentos electrónicos

Artículo 27 Cuando la Ley exija que un documento debe ser presentado en formato impreso y se encuentre en formato electrónico, tal requisito

queda satisfecho cuando éste se presente en formato impreso y contenga un código unívoco que lo identifique y permita su recuperación en el repositorio digital institucional correspondiente, de conformidad con la normativa que rige la materia.

Principio de coordinación

Artículo 28 Los proyectos y acciones que desarrollen el Poder Público y el Poder Popular, a fin de consolidar el uso de las tecnologías de información libres en la gestión pública, deben efectuarse de manera coordinada en los términos establecidos en la presente Ley, y están orientados al logro de los fines y objetivos del Estado, sobre la base de las políticas, estrategias, lineamientos y normas en la materia que a tal efecto se dicten.

Principio de colaboración

Artículo 29 El Poder Público y el Poder Popular colaborarán para alcanzar la consolidación del uso de las tecnologías de información libres en el Estado.

Interoperabilidad de las tecnologías de información

Artículo 30 Los procesos soportados en las tecnologías de información en el Poder Público y el Poder Popular deben ser interoperables, a fin de apoyar la función y gestión pública que éstos prestan, garantizando la cooperación y colaboración requerida para proporcionar servicios y procesos públicos integrados, complementarios y transparentes, sobre la base del principio de unidad orgánica.

Sistema de consulta

Artículo 31 El Poder Público debe procurar que el diseño y construcción de sus sistemas, programas, aplicaciones y servicios de información cuenten con facilidades de uso para la consulta electrónica, así como la veracidad y existencia de los documentos electrónicos, circunstancias o requisitos que posean y sean necesarios para realizar una determinada solicitud, trámite o servicio, sin que lo previamente descrito se le transfiera a las personas.

El Poder Popular debe igualmente garantizar que sus sistemas informáticos, cuenten con las mismas facilidades previstas para el

Poder Público establecidas en el párrafo anterior y la que establezca la normativa correspondiente.

Obligación de compartir información

Artículo 32 El Poder Público tiene la obligación de compartir entre sí la información pública que conste en sus archivos y repositorios digitales, de conformidad con lo establecido en la ley que regule la materia sobre el intercambio electrónico de datos, información y documentos, salvo las excepciones establecidas en la Constitución de la República y la normativa aplicable.

El Poder Popular deberá compartir información pública sobre la gestión de los servicios públicos que se le hayan transferido, en los términos establecidos en el presente artículo y demás normativa aplicable.

Plataforma tecnológica del Estado

Artículo 33 El Poder Público debe contar con una plataforma tecnológica integrada, bajo su control y administración, que permita el efectivo uso de las tecnologías de información en sus relaciones internas, con otros órganos y entes, y en sus relaciones con las personas, apoyando la gestión del sector público y la participación del Poder Popular en los asuntos públicos.

Del conocimiento libre

Artículo 34 El desarrollo, adquisición, implementación y uso de las tecnologías de información por el Poder Público, tiene como base el conocimiento libre. En las actuaciones que se realicen con el uso de las tecnologías de información, sólo empleará programas informáticos en software libre y estándares abiertos para garantizar al Poder Público el control sobre las tecnologías de información empleadas y el acceso de las personas a los servicios prestados.

Los programas informáticos que se empleen para la gestión de los servicios públicos prestados por el Poder Popular, a través de las tecnologías de información, deben ser en software libre y con estándares abiertos.

De las licencias

Artículo 35 Las Licencias para programas informáticos utilizados en el Poder Público, deben permitir el acceso al código fuente y a la

transferencia del conocimiento asociado para su compresión, su libertad de modificación, libertad de uso en cualquier área, aplicación o propósito y libertad de publicación y distribución del código fuente y sus modificaciones. Únicamente se adoptarán aquellas licencias que garanticen que los trabajos derivados se licencien en los mismos términos que la licencia original.

El Poder Popular debe garantizar que las licencias de los programas informáticos empleados en la gestión de los servicios públicos transferidos, cumplan con las condiciones y términos establecidos en el presente artículo.

Soberanía e independencia tecnológica

Artículo 36 El Estado garantiza la apropiación social del conocimiento asociado a las tecnologías de información libres que se desarrollen, adquieran, implementen y usen con el fin de emplearlas de forma independiente.

Igualmente, aquellas tecnologías privativas en proceso de migración a tecnologías libres, deben garantizar el uso y ejecución de modo independiente. Para ello, se establecerán fuentes de financiamiento que impulsen programas y proyectos de investigación y desarrollo, fomenten la industria nacional de información libres y promueva la formación del talento humano en materia de tecnología de información libres, en los términos y condiciones establecidos en la presente Ley.

Título II
De la organización en el Poder Público para el uso de las Tecnologías de Información

Capítulo I
Del Consejo Nacional para el Uso de las Tecnologías de Información

Creación del Consejo Nacional para el Uso de las Tecnologías de Información

Artículo 37 Se crea el Consejo Nacional para el Uso de las Tecnologías de Información en el Poder Público, como máximo órgano de consulta para la planificación y asesoramiento del Poder Público en los asuntos relacionados con las tecnologías de información, contribuyendo en la consolidación de la seguridad, defensa y

soberanía nacional. Es presidido por el Vicepresidente Ejecutivo o Vicepresidenta Ejecutiva de la República y tendrá como fin promover y consolidar el uso, desarrollo, implementación y aprovechamiento de las tecnologías de la información en el Poder Público, mediante la coordinación de las acciones a tal efecto se establezcan.

Conformación

Artículo 38 El Consejo Nacional para el Uso de las Tecnologías de Información en el Poder Público, está integrado por:

1. El Vicepresidente Ejecutivo o Vicepresidenta Ejecutiva de la República, en su condición de Órgano directo y colaborador del Presidente o Presidenta de la República, y en su condición de Presidente o Presidenta del Consejo Federal de Gobierno, quien lo preside.
2. El Ministerio del Poder Popular con competencia en materia de planificación.
3. El Ministerio del Poder Popular con competencia en materia ciencia tecnología e innovación.
4. El Ministerio del Poder Popular con competencia en materia de comunas.
5. La Procuraduría General de la República.
6. La Asamblea Nacional.
7. El Tribunal Supremo de Justicia.
8. El Consejo Nacional Electoral.
9. El Consejo Moral Republicano y;
10. El Banco Central de Venezuela.

Competencias

Artículo 39 El Consejo Nacional para el Uso de las Tecnologías de Información en el Poder Público tiene las siguientes competencias:

1. Promover el adecuado uso y aprovechamiento de las tecnologías de información en el Poder Público y en el Poder Popular.
2. Establecer lineamientos, políticas y estrategias para el acceso, uso, promoción, adquisición y desarrollo de las tecnologías de información libres.

3. Impulsar la mejora de la gestión pública y calidad de los servicios públicos que se presten a las personas a través de tecnologías de información.

4. Promover la transparencia en el Poder Público, a fin de garantizar el derecho fundamental de las personas al acceso a la información pública.

5. Garantizar que los programas y proyectos que se implementen en el Poder Público, contemplen los requerimientos para su implantación y sustentabilidad, con base en la provisión de las capacidades financieras, institucionales y de talento humano que resulten necesarias.

6. Proponer ante las autoridades competentes el marco normativo necesario para garantizar el aprovechamiento y uso de las tecnologías de información en el Poder Público y en el Poder Popular, de conformidad con la presente Ley.

7. Dictar las normas necesarias para su funcionamiento, a través del respectivo reglamento que al efecto se dicte.

8. Las demás que determine la ley.

Capítulo II
De la Comisión Nacional de las Tecnologías de Información

Creación

Artículo 40 Se crea la Comisión Nacional de las Tecnologías de Información, como un instituto público dotado de personalidad jurídica y patrimonio propio, distinto e independiente de la República, con competencias financieras, administrativas, presupuestarias, técnicas, normativas y de gestión de recursos, las cuales serán ejercidas de acuerdo con los lineamientos y políticas establecidos por el órgano de adscripción en coordinación con la Comisión Central de Planificación, con los privilegios y prerrogativas de la República; estará adscrito al Ministerio del Poder Popular con competencia en materia de ciencia, tecnología e innovación. Dicho Instituto tendrá su sede en la ciudad de Caracas, y podrá crear direcciones regionales para la consecución de sus actividades en el Territorio Nacional.

Competencias de la Comisión Nacional de las Tecnologías de Información

Artículo 41 Son competencias de la Comisión Nacional de las Tecnologías de Información las siguientes:

1. Elaborar el Plan Nacional de Tecnologías de Información para el Estado, alineado con las directrices establecidas en el Plan de Desarrollo Económico y Social de la Nación, y demás planes nacionales en coordinación con el Ministerio del Poder Popular con competencia en materia de planificación, de conformidad con la ley aplicable.
2. Establecer las políticas, estrategias y lineamientos en materia de regulación, acceso, desarrollo, adquisición, implementación y uso de las tecnologías de información en el Poder Público.
3. Establecer, de manera coordinada con la Superintendencia de Servicios de Certificación Electrónica, las políticas, estrategias, lineamientos y regulaciones en materia de seguridad informática en el Poder Público.
4. Establecer mecanismos de coordinación e intercambio con el Poder Público y con el Poder Popular, así como con instituciones privadas, nacionales e internacionales, especializadas en tecnologías de información y materias afines.
5. Promover, conjuntamente con el Poder Público y con el Poder Popular, el acceso y uso de las tecnologías de información, a fin de contribuir en la gestión, incrementar la eficiencia, transparencia, y mejorar sus relaciones con las personas.
6. Establecer las políticas de promoción, fomento y fortalecimiento del sector productivo de las tecnologías de información.
7. Promover la formulación y ejecución de iniciativas que permitan impulsar la investigación, el desarrollo, adquisición, implementación y uso de las tecnologías de información en el Poder Público y en el Poder Popular.
8. Administrar el repositorio de programas informáticos libres y de programas informáticos utilizados por el Poder Público y por el Poder Popular, así como la información asociada a éstos.
9. Participar en nombre de la República ante organismos internacionales en materia de tecnología de información, en coordinación con el Ministerio del Poder Popular con competencia en materia de relaciones exteriores.
10. Promover, en corresponsabilidad con el Poder Popular, la innovación de las tecnologías de información, impulsando

programas y proyectos de investigación y desarrollo que fomenten la industria nacional de las tecnologías de información y la formación del talento humano.

11. Velar para que los planes y proyectos que se implementen estén alineados con las políticas nacionales de fomento a la industria nacional de tecnologías de información.

12. Autorizar al Poder Público, con carácter excepcional, el uso de tecnologías de información privativas, en los casos y condiciones establecidos en la Presente Ley y normativa aplicable.

13. Otorgar, suspender y revocar la certificación de los programas informáticos, equipos y servicios en materia de tecnologías de información, a ser desarrollados, adquiridos, implementados y usados por parte del Poder Público y del Poder Popular.

14. Otorgar, suspender y revocar las acreditaciones a las unidades de servicios de verificación sobre programas informáticos, equipos y servicios en materia de tecnologías de información, de conformidad con la normativa aplicable.

15. Asegurar que los funcionarios públicos, funcionarias públicas, empleados y empleadas al servicio del Poder Público, adquieran las competencias y habilidades necesarias para cumplir sus roles de forma efectiva, a través de programas de educación, entrenamiento y formación en tecnologías de información y seguridad informática.

16. Colaborar en la formulación de las políticas, estrategias y lineamientos en materia de regulación, acceso, desarrollo, adquisición, implementación y uso de las tecnologías de información en el Poder Público.

17. Establecer las políticas, estrategias, lineamientos y regulaciones en materia de seguridad informática en el Poder Público.

18. Ejecutar los lineamientos, políticas y estrategias para el acceso, uso, promoción, adquisición y desarrollo de las tecnologías de información libres, emanados del Consejo Nacional para el Uso de las Tecnologías de Información en el Poder Público.

19. Garantizar la mejora de la gestión pública y la calidad de los servicios públicos que se presten a las personas, a través de las tecnologías de la información.

20. Velar por el cumplimiento de las normas que en materia de tecnologías libres de información y de seguridad de la información se dicten.

21. Promover la transparencia en el Poder Público, a fin de garantizar a las personas el derecho fundamental al acceso a la información pública.

22. Establecer mecanismos de coordinación y colaboración entre el Poder Público y el Poder Popular, a fin de propiciar el intercambio electrónico de datos, información y documentos; el análisis de problemáticas comunes y la realización de proyectos conjuntos en materia de tecnologías de información.

23. Garantizar el cumplimiento de las políticas; lineamientos, normas y procedimientos requeridos para el intercambio electrónico de datos, información y documentos con el objeto de establecer un estándar de interoperabilidad.

24. Resolver los conflictos que surjan en relación al acceso e intercambio electrónico de datos, de información y documentos o al uso inadecuado de éstos, conforme a los términos y condiciones establecidos en el Decreto con Rango, Valor y Fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los órganos y Entes del Estado.

25. Promover una efectiva gestión de la seguridad de la información para proteger los activos de información y minimizar el impacto en los servicios causados por vulnerabilidades o incidentes de seguridad.

26. Garantizar que los programas y proyectos que se implementen en el Poder Público contemplen los requerimientos para su implantación y sustentabilidad, con base en la provisión de las capacidades financieras, institucionales y de talento humano que resulten necesarias.

27. Promover la optimización de la utilización de los recursos de tecnologías de información del Estado, mediante la promoción de una adecuada gestión de activos, mediante la colaboración interinstitucional, la racionalización de compras y la implementación de soluciones pertinentes de conformidad con la Ley.

28. Dictar las normas y procedimientos instruccionales aplicables en el desarrollo, adquisición, implementación y uso de tecnologías de información, así como los servicios asociados a esas tecnologías.

29. Inspeccionar y fiscalizar el cumplimiento de las disposiciones de la presente Ley, así como la normativa en materia de su competencia.

30. Abrir de oficio o a instancia de parte, sustanciar y decidir los procedimientos administrativos sancionatorios previstos en la presente Ley y normativa aplicable, en el ámbito de su competencia.

31. Dictar medidas preventivas y correctivas en el curso de los procedimientos administrativos de su competencia, cuando así lo requiera.

32. Ejercer acciones administrativas o judiciales de cualquier índole para la salvaguarda y protección de sus derechos e intereses.

33. Velar por el cumplimiento de las disposiciones de esta Ley y demás actos que dicte, cuya vigilancia le competa.

34. Las demás que determine la ley.

Patrimonio

Artículo 42 El patrimonio de la Comisión Nacional de las Tecnologías de Información estará constituido por:

1. Los recursos anuales que le sean asignados en la Ley de Presupuesto para el ejercicio fiscal correspondiente;
2. Otros ingresos y bienes que le puedan ser asignados o transferidos por órganos y entes del Poder Público;
3. Los bienes provenientes de las donaciones, legados y aportes de carácter lícito;
4. Sus ingresos propios, obtenidos por el desarrollo de sus actividades y por los servicios que preste;
5. Lo recaudado por tributos, de acuerdo a lo establecido en la presente Ley;
6. Las multas por las infracciones de acuerdo a la presente Ley;
7. Los demás bienes que adquiera por cualquier título.

Dirección de la Comisión Nacional de las Tecnologías de Información

Artículo 43 La Dirección de la Comisión Nacional de las Tecnologías de Información estará a cargo de un Consejo Directivo. El Consejo Directivo estará integrado por un director o directora general, quien presidirá el Instituto, y cuatro directores o directoras, quienes serán de libre nombramiento y remoción del Presidente o Presidenta de la República Bolivariana de Venezuela, cada uno de los cuales tendrá un suplente, designado o designada de la misma forma, quien llenará las faltas temporales. Las ausencias temporales del Director o Directora General serán suplidas por el Director o Directora Principal que éste o ésta designe.

Quórum

Artículo 44 El Consejo Directivo sesionará válidamente con la presencia del director o directora general, o quien haga sus veces, y dos directores o directoras. Las decisiones se tomarán por mayoría absoluta de los miembros del Consejo cuando se encuentren presentes todos sus integrantes, y por unanimidad cuando ocurriere el quórum mínimo.

El régimen ordinario de sesiones del Consejo directivo lo determinará el reglamento interno que se dictará de conformidad a lo previsto en esta Ley.

Prohibición para integrar el Consejo Directivo

Artículo 45 No podrán ser designados o designadas director o directora general miembros del Consejo directivo ni suplentes:

1. Las personas que tengan parentesco hasta el cuarto grado de consanguinidad o segundo de afinidad, o sean cónyuges del Presidente o Presidenta de la República, del Vicepresidente Ejecutivo o Vicepresidenta Ejecutiva de la República o de la máxima autoridad del órgano rector o de algún miembro de la dirección de la Comisión Nacional de las Tecnologías de Información.
2. Quienes en beneficio propio o de un tercero, directa o indirectamente, hayan celebrado contratos de obra o de suministro de bienes o servicios con la Comisión Nacional de las Tecnologías de Información y no los hayan finiquitado en el año inmediatamente anterior a sus designaciones.
3. Quienes tengan conflicto de intereses con el cargo a desempeñar.
4. Las personas que hayan sido declaradas en estado de quiebra, culpable o fraudulenta, y los condenados o condenadas por delitos contra el patrimonio público.

Responsabilidad de los miembros del Consejo Directivo

Artículo 46 Los miembros del Consejo Directivo serán responsables civil, penal, disciplinaria y administrativamente de las decisiones adoptadas en sus reuniones de conformidad con las leyes que rigen la materia.

Competencias del Consejo Directivo

Artículo 47 Al Consejo Directivo le corresponden las siguientes competencias:

1. Someter a la consideración del órgano rector todas las políticas, estrategias y lineamientos en materia de regulación, acceso, desarrollo, adquisición, implementación y uso de las tecnologías de información en el Poder Público al igual que en el Poder Popular, cuando realice gestiones públicas.
2. Aprobar y discutir el plan operativo anual y el balance general, así como los estados financieros de la Comisión Nacional de las Tecnologías de Información, conforme a los proyectos presentados por el Director o Directora General.
3. Dictar el reglamento interno de la Comisión Nacional de las Tecnologías de Información.
4. Aprobar la creación, modificación o supresión de direcciones regionales que se consideren necesarias para el cumplimiento de los fines de la Comisión Nacional de Tecnologías de Información.
5. Aprobar el estatuto de los funcionarios públicos y funcionarias públicas de la Comisión Nacional de Tecnologías de Información.
6. Autorizar al Director o Directora General para suscribir y actualizar convenios y contratos que tengan por objeto el desarrollo, comercialización, producción y agilización de actividades y proyectos vinculados con las tecnologías de información libres, previa autorización del órgano rector.
7. Autorizar la suscripción y enajenación de bienes muebles e inmuebles propiedad de la Comisión, de conformidad con lo dispuesto en la ley que rige la materia.
8. Autorizar al Director o Directora General de la Comisión Nacional de las Tecnologías, conjuntamente con dos miembros del Consejo Directivo, para abrir, movilizar y cerrar las cuentas bancarias del instituto, cumpliendo con las normas que rigen la materia.
9. Las demás que le confieren las leyes y sus reglamentos respectivos.

Capítulo III
De las atribuciones de la Comisión Nacional
de las Tecnologías de Información

Atribuciones del Director o Directora General

Artículo 48 Corresponde al Director o Directora General de la Comisión Nacional de las Tecnologías de Información:

1. Ejercer la representación del Instituto y emitir los lineamientos para organizar, administrar, coordinar y controlar los recursos humanos, materiales y financieros del Instituto.
2. Autorizar la realización de inspecciones o fiscalizaciones.
3. Ordenar la apertura y sustanciación de procedimientos administrativos sancionatorios.
4. Nombrar, remover o destituir al personal del Instituto y ejercer la potestad disciplinaria, de conformidad con los procedimientos del correspondiente estatuto.
5. Celebrar en nombre del Instituto, previa aprobación del Consejo Directivo, convenios y contratos con organismos nacionales e internacionales, de conformidad con la ley.
6. Dictar los lineamientos generales para la elaboración del proyecto de presupuesto, el plan operativo anual y el balance general del Instituto, y someterlo a la aprobación del Consejo Directivo, de conformidad con la ley.
7. Otorgar poderes para la representación judicial y extrajudicial del Instituto.
8. Delegar atribuciones para la firma de determinados documentos, en los casos que determine el reglamento interno del Instituto.
9. Ejercer las competencias del Instituto que no estén expresamente atribuidas a otra autoridad.
10. Elaborar y presentar el proyecto del reglamento interno del Instituto a la consideración del Consejo Directivo.
11. Convocar y presidir las sesiones del Consejo Directivo, así como suscribir los actos y documentos que emanen de sus decisiones.
12. Presentar la memoria y cuenta del Instituto a consideración del Consejo Directivo y del Ministerio del Poder Popular con competencia en materia de ciencia, tecnología e innovación.
13. Las demás que le confieran la ley y los reglamentos.

Régimen de los funcionarios y funcionarias

Artículo 49 Los funcionarios públicos y funcionarias públicas de la Comisión Nacional de las Tecnologías de Información se regirán por la Ley del Estatuto de la Función Pública, salvo disposiciones especiales que el Ejecutivo Nacional decida sobre el reclutamiento, selección, ingreso, el desarrollo, la evaluación, los ascensos, los traslados, las suspensiones en el ejercicio de los cargos, la valoración de los cargos, las escalas de remuneraciones y el egreso. Las materias enumeradas en este artículo son de orden público; no pueden renunciarse ni relajarse por convenios individuales o colectivos, ni por actos de las autoridades de la Comisión Nacional de las Tecnologías de Información.

Capítulo IV
De las unidades de apoyo

Unidades de apoyo

Artículo 50 Son unidades de apoyo a los efectos de la presente Ley:

1. El ente normalizador del uso de las tecnologías de información.
2. El órgano normalizador en seguridad informática.
3. Cualquier otra instancia que esté vinculada con el objeto y fines de esta Ley.

Ente normalizador

Artículo 51 El ente normalizador en materia de tecnologías de información y el órgano normalizador en seguridad de la información, ejercerán las funciones de unidades de apoyo especializadas de la Comisión Nacional de las Tecnologías de Información, en las materias de su competencia y de conformidad con las normas de funcionamiento dicte la Comisión.

Sección Primera
Normalizador de las Tecnologías de Información

Autoridad competente

Artículo 52 El Centro Nacional de Tecnologías de Información, ente adscrito al órgano con competencia en tecnologías de información, es el

encargado de apoyar a la Comisión Nacional de las Tecnologías de Información a normalizar el desarrollo, adquisición, implementación y uso de estas tecnologías en el Poder Público y en el Poder Popular, conforme a las políticas, lineamientos y estrategias que se establezcan al efecto.

Competencia

Artículo 53 El Centro Nacional de Tecnologías de Información tiene, en el ámbito de aplicación de la presente Ley, las siguientes atribuciones:

1. Proponer a la Comisión Nacional de las Tecnologías de información las líneas de investigación para el desarrollo de programas y equipos informáticos que apoyen la solución de problemas en el Poder Público y en el Poder Popular.
2. Contribuir con la formación y difusión para la apropiación social del conocimiento en tecnologías de información libres en el país.
3. Solicitar al Poder Público y al Poder Popular la información necesaria para el cumplimiento de sus funciones, en el ámbito de su competencia.
4. Colaborar con la Comisión Nacional de las Tecnologías de Información en la promoción del acceso e intercambio de datos, información y documentos entre los órganos y entes del Poder Público, así como entre éstos y el Poder Popular.
5. Ejercer las funciones de unidad de apoyo especializado para la Comisión Nacional de las Tecnologías de Información.
6. Presentar el informe anual sobre su gestión al órgano rector y a la Comisión Nacional de las Tecnologías de Información.
7. Coordinar con el órgano competente los procedimientos, acciones y actividades necesarias para el desarrollo de la gestión del Sistema Venezolano para la Calidad en materia de tecnologías de información en el Poder Público.
8. Velar por el cumplimiento de las disposiciones de esta Ley y demás actos que se dicten, cuya vigilancia le competa.
9. Las demás atribuciones que determine la Ley.

Sección Segunda
Normalizador de seguridad informática

De la Superintendencia de Servicios de Certificación Electrónica

Artículo 54 La Superintendencia de Servicios de Certificación Electrónica, adscrita al Ministerio del Poder Popular con competencia en materia en ciencia, tecnologías e innovación, es el órgano competente en materia de seguridad informática, y es responsable del desarrollo, implementación, ejecución y seguimiento al Sistema Nacional de Seguridad Informática, a fin de resguardar la autenticidad, integridad, inviolabilidad y confiabilidad de los datos, información y documentos electrónicos obtenidos y generados por el Poder Público y por el Poder Popular, así como la generación de contenidos en la red.

Competencias

Artículo 55 La Superintendencia de Servicios de Certificación Electrónica tendrá, en el ámbito de aplicación de esta Ley, las siguientes competencias:

1. Desarrollar, implementar y coordinar el Sistema Nacional de Seguridad Informática.
2. Dictar las normas instruccionales y procedimientos aplicables en materia de seguridad informática.
3. Establecer los mecanismos de prevención, detención y gestión de los incidentes generados en los sistemas de información y en las infraestructuras críticas del Estado, a través del manejo de vulnerabilidades e incidentes de seguridad informática.
4. Articular e insertar en el Poder Público y en el Poder Popular las iniciativas que surjan en materia de seguridad informática, dirigidas a la privacidad, protección de datos y de infraestructuras críticas, así como intervenir y dar respuesta ante los riesgos y amenazas que atenten contra la información que manejen.
5. Proponer al órgano rector líneas de investigación asociadas a la seguridad informática que apoye la solución de problemas en el Poder Público y en el Poder Popular.
6. Contribuir en la formación de las personas y del componente laboral, que promueva el establecimiento de una cultura de resguardo y control sobre los activos de información presentes en los sistemas de información.

7. Realizar peritajes en soportes digitales, previo cumplimiento del procedimiento legal pertinente, apoyando a las autoridades competentes en investigaciones, experticias e inspecciones relacionadas con evidencias digitales.

8. Evaluar los medios de almacenamiento digital, de acuerdo a los criterios de búsquedas establecidos en la solicitud de entes u organismos del Estado que así lo requieran.

9. Extraer, revisar y analizar las trazas y bitácoras de equipos y herramientas de redes.

10. Auditar el funcionamiento e integridad de aplicaciones y base de datos donde se presuma inconsistencias incorporadas con el objeto de causar daños.

11. Prestar asesoría técnica en materia de informática forense a los órganos de apoyo a la investigación penal.

12. Administrar el registro público de homologación de equipos o aplicaciones con soporte criptográfico.

13. Ejecutar las funciones de unidad de apoyo especializado de la Comisión Nacional de las Tecnologías de Información en el Poder Público, en el área de su competencia.

14. Presentar el informe anual sobre su gestión al órgano rector y a la Comisión Nacional de las Tecnologías de Información.

15. Coordinar con el órgano competente los procedimientos, acciones y actividades necesarias para el desarrollo de la gestión del Sistema Venezolano de la Calidad en materia de seguridad informática en el Poder Público y en el Poder Popular.

16. Las demás que establezca la ley.

Unidades de servicios de verificación

Artículo 56 La Comisión Nacional de las Tecnologías de Información, previo cumplimiento de las condiciones que determine la norma instruccional correspondiente, podrá acreditar a las personas naturales o jurídicas la cualidad de unidad de servicios de verificación y certificación, a fin de realizar funciones de auditoría sobre los programas informáticos, equipos de computación o servicios en materia de tecnologías de información a ser desarrollados, adquiridos, implementados y usados por el Poder Público y por el Poder Popular, para constatar el cumplimiento de las disposiciones de la presente Ley y demás normativa aplicable.

Capítulo V
De los subsistemas que conforman el Sistema Nacional de Protección y Seguridad Informática

Subsistemas que integran el Sistema Nacional de Protección y Seguridad Informática

Artículo 57 El Sistema Nacional de Protección y Seguridad Informática tiene como objeto proteger, resguardar, mitigar, y mejorar la capacidad de respuesta del Poder Público y del Poder Popular frente a riesgos y amenazas derivados del desarrollo de los sistemas de información. El Sistema Nacional de Protección y Seguridad Informática está integrado por:

1. Subsistema de Criptografía Nacional.
2. Subsistema Nacional de Gestión de Incidentes Telemáticos.
3. Subsistema Nacional de Informática Forense.
4. Subsistema Nacional de Protección de Datos.

El Reglamento respectivo establecerá los términos y condiciones de implementación del Sistema Nacional de Protección y Seguridad Informática.

De la aprobación, certificación y homologación de los equipos o aplicaciones criptográficas

Artículo 58 La Superintendencia de Servicios de Certificación Electrónica, con el objeto de garantizar la integridad, calidad e independencia tecnológica, aprueba, certifica y homologa los equipos o aplicaciones con soporte criptográfico que use el Poder Público y el Poder Popular.

De los registros públicos de homologación y sus fines

Artículo 59 La Superintendencia de Servicios de Certificación Electrónica es el órgano encargado de supervisar y exigir los certificados de homologación o sellos de certificación por modelo o versión de los equipos o aplicación con soporte criptográfico. A tal efecto, lleva un registro público del código de homologación para proveedores de servicios de certificación de los entes u organismos del Poder Público y del Poder Popular que hayan sido homologados y certificados.

Título III
De los Tributos

Capítulo I
De las contribuciones parafiscales

De las contribuciones por actividades comerciales

Artículo 60 Todas las personas jurídicas cuyo objeto sea la importación, distribución y comercialización de software privativo al Poder Público, pagarán a la Comisión Nacional de Tecnologías de Información el dos y medio por ciento (2,5%), de la utilidad neta del ejercicio. Lo cancelado por este concepto, se realizará dentro de los noventas días siguientes del cierre del ejercicio fiscal.

El monto en bolívares de la cancelación de esta contribución, será deducido del pago del Impuesto Sobre la Renta.

Contribución por servicios

Artículo 61 Toda persona que preste servicios de software privativos al Poder Público, pagará una contribución del uno y medio por ciento (1,5%) de la utilidad neta del ejercicio, a la Comisión Nacional de Tecnologías de Información, dentro de los noventa días siguientes al cierre del ejercicio fiscal.

El monto en bolívares de la cancelación de la presente contribución, será deducido del pago del Impuesto sobre la Renta.

Capítulo II
De las tasas y contribuciones especiales

Certificación

Artículo 62 El Poder Público debe solicitar ante la Comisión Nacional de las Tecnologías de Información, la certificación del cumplimiento de las disposiciones de la presente Ley y demás normativa aplicable de los programas informáticos por equipos de computación según su tipo o modelo, el cual causa una tasa de cincuenta Unidades Tributarias (50 U.T.).

De las tasas por certificación y homologación de los equipos o aplicaciones con soporte criptográfico

Artículo 63 La homologación de los equipos o aplicaciones con soporte criptográfico, a que hace mención el artículo 58, tendrá una duración de tres años y su solicitud de tramitación causará una tasa de trescientas Unidades Tributarias (300 U.T.). Las aplicaciones y equipos con soporte criptográfico libre estarán exentos del pago de la tasa prevista en el presente artículo.

Procedimiento

Artículo 64 La tramitación de la solicitud de acreditación o renovación como unidad de servicios de verificación y certificación se sustanciará de conformidad con el procedimiento previsto en la Ley Orgánica de Procedimientos Administrativos, y causará el pago de una tasa que no podrá ser mayor de treinta Unidades Tributarias (30 U.T.) ni menor a quince Unidades Tributarias (15 U.T.).

Contenido de la acreditación

Artículo 65 La acreditación correspondiente contendrá, además de los extremos requeridos por la Ley Orgánica de Procedimientos Administrativos y los previstos establecidos en el Registro Nacional de Contratistas los siguientes:

1. El tipo de acreditación que se trate.
2. La determinación de las características y de los servicios que presta.
3. El tiempo durante la cual se otorga no podrá ser superior a dos años.
4. La remisión expresa a la norma instruccional que contenga las funciones y obligaciones de las unidades de servicios de verificación y certificación.

Excepción del uso de programas informáticos libres

Artículo 66 La Comisión Nacional de las Tecnologías de Información, excepcionalmente podrá autorizar, hasta por tres años, la adquisición y el uso de software que no cumpla con las condiciones de estándares abiertos y software libre, cuando no exista un programa desarrollado que lo sustituya o se encuentre en riesgo la seguridad y defensa de la Nación.

La Comisión Nacional de las Tecnologías de Información, al autorizar el uso del software privativo, establecerá las condiciones y términos para el desarrollo de una versión equivalente en software libre y estándares abiertos.

De las contribuciones especiales por la utilización de software privativo

Artículo 67 El órgano o ente del Poder Público al igual que el Poder Popular que sea autorizado a adquirir, usar y actualizar un software privativo, debe pagar una contribución especial al Fondo Nacional de Ciencia, Tecnología e Innovación la cantidad equivalente entre el cinco por ciento (5%) y el diez por ciento (10%) del valor de adquisición del software privativo. Este aporte debe efectuarse dentro del ejercicio fiscal correspondiente a la adquisición del programa.

Igualmente, el órgano o ente del Poder Público y el Poder Popular deben pagar una contribución especial al Fondo Nacional de Ciencia, Tecnología e Innovación equivalente entre el cinco por ciento (5%) y el diez por ciento (10%) del valor correspondiente a los gastos asociados al soporte y uso del software privativo.

Las contribuciones a que se refiere este artículo deben efectuarse hasta que sea sustituido el software privativo por un software libre y con estándares abiertos.

El reglamento respectivo determinará la base de cálculo de la alícuota de la contribución a pagar.

Destino de las contribuciones parafiscales y tasas

Artículo 68 Los recursos producto de lo recaudado por concepto de contribuciones parafiscales y tasas, serán destinados al desarrollo y fomento del sector de tecnologías libres de información, en un monto no menor del cincuenta por ciento (50%) de lo recaudado, y el resto formará parte de los ingresos propios de la Comisión Nacional de las Tecnologías de Información.

Capítulo III
Disposiciones Comunes

Facultades tributarias

Artículo 69 La Comisión Nacional de las Tecnologías de Información ejercerá las facultades y deberes que le atribuye el Código Orgánico Tributario a la Administración Tributaria, en relación con los tributos

establecidos en la presente Ley. Igualmente, el Ministerio del Poder Popular con competencia en materia de ciencia, tecnología e innovación ejercerá las facultades y deberes a los que se refiere este artículo, por lo que respecta a las tasas correspondientes al Fondo Nacional de Ciencia, Tecnología e Innovación.

Título IV
Desarrollo del Sector de Tecnologías de Información Libres

Promoción de la industria nacional de tecnologías de información libres

Artículo 70 El Estado venezolano, a través del Ministerio del Poder Popular con competencia en materia de ciencia, tecnología e innovación conjuntamente con la Comisión Nacional de Tecnologías de Información impulsan el desarrollo, fortalecimiento y consolidación de la industria nacional de tecnología de información libres, garantizando el ejercicio de la soberanía tecnológica y el desarrollo integral de la nación. A tales fines, promueve:

1. Programas de investigación en los sectores prioritarios para el desarrollo nacional y la independencia tecnológica con tecnologías de información libres.
2. La investigación nacional en tecnologías de información libres.
3. Polos de innovación regionales en la República, que asocien la investigación con la industria nacional de tecnologías de información libres.
4. El financiamiento a la investigación, innovación y desarrollo en tecnologías de información libres, así como a la formación en estas tecnologías.
5. Programas que impulsen la creación de consultoras, creadores y creadoras independientes en tecnologías de información libres.
6. La creación y desarrollo de empresas de propiedad social en tecnologías de información libres, conforme al sistema económico comunal.
7. Prospectiva tecnológica.
8. Programas para captar y formar investigadores e investigadoras y potenciar el talento humano en tecnologías de información libres.

9. La apropiación social del conocimiento mediante planes de formación en tecnologías de información libres.

10. La creación, desarrollo y articulación de una red nacional de soporte técnico en tecnologías de información libres.

11. La racionalización del uso de recursos mediante el despliegue de infraestructura orientada a servicios de tecnologías de información libres.

12. Una base de conocimiento que impulse la apropiación social de las tecnologías de información libres.

13. Impulsar y apoyar, conjuntamente con el Ministerio del Poder Popular con competencia en materia de comunas, la conformación de las comunas de tecnologías libres, integradas por los usuarios, usuarias, activistas, colectivos y comunidades del software y hardware libres de la República Bolivariana de Venezuela, de conformidad con la presente Ley y demás normativa aplicable.

14. Cualquier otro mecanismo que permita establecer incentivos que promuevan la industria nacional de tecnologías de información libres.

Del financiamiento con fondos públicos

Artículo 71 El financiamiento con fondos públicos está dirigido a impulsar un sistema económico socio productivo de las tecnologías de información libres, que desarrolle las actividades de investigación, diseño, creación, desarrollo, producción, implementación, asistencia técnica, documentación y servicios relativos tanto al software y como al hardware libres.

Exoneraciones tributarias

Artículo 72 El Ejecutivo Nacional podrá exonerar, total o parcialmente, el pago del impuesto por enriquecimiento neto a la venta de bienes y prestación de servicios en tecnologías de información libres, de acuerdo a lo establecido en la legislación que rige la materia tributaria.

Recursos para las tecnologías de información libres

Artículo 73 El Fondo Nacional de Ciencia, Tecnología e Innovación destinará, además de los aportes recaudados conforme a los artículos 63 y 64 de la presente Ley, un porcentaje no menor al dos por ciento (2%) de los recursos provenientes de los aportes

para la ciencia, la tecnología y la innovación, para el financiamiento de los programas y planes de promoción para consolidar la industria nacional de tecnologías de información libres, conforme a lo establecido en el artículo 70 de esta Ley.

Título V
Derecho y Garantía de las personas sobre el acceso a la información

Naturaleza de la información

Artículo 74 La información que conste en los archivos y registros en el Poder Público y en el Poder Popular es de carácter público, salvo que se trate de información sobre el honor, vida privada, intimidad, propia imagen, confidencialidad y reputación de las personas, la seguridad y defensa de la Nación, de conformidad con lo establecido en la Constitución de la República, la ley que regule la materia sobre protección de datos personales y demás leyes que rigen la materia.

Suministro de información

Artículo 75 El Poder Público y el Poder Popular, a través de las tecnologías de información, están obligados a notificar a las personas:

1. Que la información será recolectada de forma automatizada;
2. Su propósito, uso y con quién será compartida;
3. Las opciones que tienen para ejercer su derecho de acceso, ratificación, supresión y oposición al uso de la referida información y;
4. Las medidas de seguridad empleadas para proteger dicha información, el registro y archivo, en las bases de datos de los organismos respectivos.

Prohibición de exigir documentos físicos

Artículo 76 El Poder Público y el Poder Popular no pueden exigirle a las personas, la consignación de documentos es formato físico que contengan datos o información que se intercambien electrónicamente, de conformidad con la ley.

Protección de la información

Artículo 77 El Poder Público y el Poder Popular tienen la obligación de proteger la información que obtiene por intermedio los servicios que presta a través de las tecnologías de información y la que repose en sus archivos o registros electrónicos, en los términos establecidos en esta Ley, y demás leyes que regulen la materia.

Tratamiento de datos personales de niños, niñas y adolescentes

Artículo 78 Previa solicitud de la persona legitimada, el Poder Público y el Poder Popular, a través de las tecnologías de información, pueden recopilar datos de niños, niñas y adolescentes en relación a sus derechos y garantías consagrados en la Constitución de la República y la normativa correspondiente.

El receptor de los datos debe darle prioridad, indicar los derechos que lo asisten y la normativa aplicable para llevar a cabo el trámite solicitado en beneficio del niño, niña o adolescente. Una vez que se obtenga dicha información se empleará únicamente a los fines el trámite.

Prohibición de compartir datos personales de niños, niñas y adolescentes

Artículo 79 La información a que se refiere el artículo anterior no puede ser divulgada, cedida, traspasada, ni compartida con ninguna persona natural o jurídica, sin el previo consentimiento de su representante legal, salvo cuando el menor de edad sea emancipado, en la investigación de hechos punibles, por una orden judicial, o cuando así lo determine la ley. El consentimiento expreso que se haya dado sobre la información del niño, niña o adolescente siempre puede ser revocado.

Título VI
Régimen Sancionatorio

Responsabilidad de los funcionarios públicos, funcionarias públicas, servidores públicos y servidoras públicas

Artículo 80 Todas aquellas personas que ejerzan una función pública, incurren en responsabilidad civil, penal y administrativa por las infracciones cometidas a la presente Ley.

De las infracciones y multas

Artículo 81 Independientemente de la responsabilidad a que se refiere el artículo anterior, todas aquellas personas en el ejercicio de una función pública, incurren en responsabilidad y serán sancionadas por la Comisión Nacional de las Tecnologías de Información, según el procedimiento previsto establecido en la Ley Orgánica de Procedimientos Administrativos, con multa comprendida entre cincuenta Unidades Tributarias (50 U.T.) y quinientas Unidades Tributarias (500 U.T.), por las siguientes infracciones:

1. Omitan la elaboración, presentación o implementación del Plan Institucional de Tecnologías de Información, en los términos señalados en la presente Ley y en la normativa aplicable.
2. Cuando ordenen o autoricen el desarrollo, adquisición, implementación y uso de programas, equipos o servicios de tecnologías de información que no cumplan con las condiciones y términos establecidos en la presente Ley y normativa aplicable a la materia, sin previa autorización de la autoridad competente.
3. Cuando incumplan las normas instruccionales, normas técnicas y estándares dictados por la autoridad competente de conformidad con la ley.
4. Cuando no registre ante la autoridad competente los programas informáticos que utilicen o posean; su licenciamiento, código fuente y demás información y documentación de conformidad con la ley.
5. Cuando en sus actuaciones electrónicas, omitan el uso de certificados y firmas electrónicas.
6. Cuando usen equipos o aplicaciones con soporte criptográfico sin la correspondiente aprobación, certificación y homologación de la autoridad competente.

7. Cuando altere un dato, información o documento suministrado por los servicios de información.

8. Cuando emplee para fines distintos a los solicitados, los datos, información o documentos obtenidos a través de un servicio de información.

9. Cuando niegue, obstaculice o retrase la prestación de un servicio de información.

10. Cuando niegue o suministre en forma completa o inexacta información sobre el uso de las tecnologías de información, seguridad informática o interoperabilidad.

11. Exigir la consignación, en formato físico, de documentos que contengan datos de autoría, información o documentos que se intercambien electrónicamente.

12. Cuando incumplan los niveles de calidad establecidos para la prestación de los servicios de información.

13. Celebrar, por sí o por intermedio de terceros, acuerdos que tengan por objeto, el intercambio electrónico de datos, información o documentos con otros órganos o entes del Estado, sin la autorización previa de la autoridad competente.

Delegación para el inicio y sustanciación del procedimiento administrativo

Artículo 82 La Comisión Nacional de las Tecnologías de Información puede delegar en las unidades de apoyo, el inicio y sustanciación de los procedimientos administrativos sancionatorios por las infracciones cometidas a la presente Ley.

Inhabilitación

Artículo 83 Sin perjuicio de las demás sanciones que correspondan, la Contraloría General de la República, de manera exclusiva y excluyente, inhabilitará al servidor público o servidora pública, de conformidad al procedimiento correspondiente en los siguientes casos:

1. Cuando se niegue, obstruya o retrase, de manera injustificada, la prestación de un servicio de información que haya sido ordenado por la autoridad competente conforme a la ley.

2. Cuando adquiera un software privativo sin haber sido autorizado expresamente por la autoridad competente.

Revocatoria de la acreditación y certificación

Artículo 84 La Comisión Nacional de las Tecnologías de Información revocará las acreditaciones de las unidades de servicios de verificación y certificación, así como las certificaciones que se otorguen conforme a la presente Ley, siguiendo el procedimiento previsto en la Ley Orgánica de Procedimientos Administrativos, por las causas siguientes:

1. El incumplimiento de las condiciones establecidas en la norma instruccional correspondiente para el otorgamiento de la acreditación o certificación.
2. El suministro de datos falsos para obtener la acreditación.
3. Cuando en la fiscalización, inspección o auditoría de un programa informático, equipo de computación o servicio de información, se hayan incumplido los procedimientos en los términos establecidos en las normas instruccionales correspondientes.
4. Cuando haya certificado un programa informático, equipo de computación o servicio de información sin cumplir las disposiciones de la presente ley y demás normativa aplicable.

Disposiciones Transitorias

Primera: El Poder Público y el Poder Popular, dentro de los noventa días siguientes a la entrada en vigencia de esta Ley, deben registrar ante la Comisión Nacional de las Tecnologías de Información los programas informáticos que estén usando o posean, licencias y demás documentación asociada, de conformidad con la normativa instruccional correspondiente.

Segunda: En caso que algún órgano o ente del Poder Público o el Poder Popular, para el momento de entrada en vigencia de la presente Ley, cuente con tecnologías de información que no cumplan con lo aquí establecido, deberán presentar ante la Comisión Nacional de las Tecnologías de Información, dentro de los doce meses siguientes, un plan institucional de adaptación o migración de las tecnologías de formación para su aprobación.

Tercera: El Poder Público y el Poder Popular deberán elaborar los planes institucionales correspondientes para implementar el uso de las tecnologías de información libres en su gestión interna, en sus relaciones con otros órganos y entes, con el Poder Popular y con las personas. Estos planes deberán ser presentados ante la Comisión Nacional de las Tecnologías de Información, en las condiciones y términos que establezca la norma instruccional correspondiente

y podrá ordenarse la aplicación de los correctivos necesarios cuando contravengan la ley y la normativa que corresponda.

Cuarta: A partir de la publicación en Gaceta Oficial de la presente Ley, el Centro Nacional de Tecnologías de Información y la Superintendencia de Servicios de Certificación Electrónica, procederán a su reestructuración, adecuación, organización y funcionamiento de conformidad con las competencias atribuidas en esta Ley, y se establece un lapso máximo de diez meses para tales efectos.

Disposiciones Derogatorias

Primera: Se deroga el Decreto N° 3.390 de fecha 23 de diciembre de 2004, mediante el cual se dispone que la Administración Pública, Nacional empleará prioritariamente Software Libre desarrollado con Estándares Abiertos en sus sistemas, proyectos y servicios informáticos, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 38.095 de fecha 28 de diciembre de 2004.

Segunda: Se deroga el Capítulo I del Título III y el Título V del Decreto con Rango, Valor y Fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 39.945 de fecha 15 de junio de 2012.

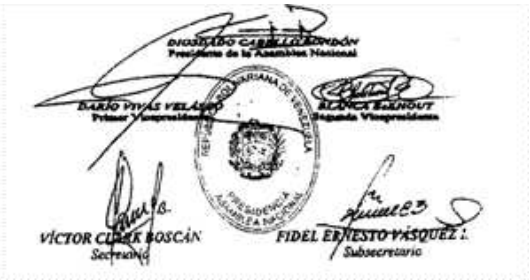
Disposiciones Finales

Primera: Todo programa informático que se desarrolle, adquiera o implemente en el Poder Público, después de la entrada en vigencia de esta Ley, deberá ser en software libre y con estándares abiertos, salvo las excepciones expresamente establecidas en la ley y previa autorización del ente competente.

Segunda: El Poder Público deberá proceder a la digitalización de sus archivos físicos. Los mensajes de datos que resulten de esta digitalización serán firmados electrónicamente por la persona autorizada, con el fin de certificar dichas copias electrónicamente.

Tercera: La presente Ley entrará en vigencia una vez transcurrido diez meses contados a partir de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

Dada, firmada y sellada en el Palacio Federal Legislativo, sede de la Asamblea Nacional, en Caracas, a los diecisiete días del mes de septiembre de dos mil trece. Años 203° de la Independencia y 154º de la Federación.



Promulgación de la Ley de Infogobierno, de conformidad con lo previsto en el artículo 213 de la Constitución de la República Bolivariana de Venezuela.

Palacio de Miraflores, en Caracas, a los diez días del mes de octubre de dos mil trece. Años 203° de la Independencia, 154° de la Federación y 14° de la Revolución Bolivariana.

Cúmplase,
(L.S.)

Refrendado
El Vicepresidente Ejecutivo de la República
(L.S.)
Jorge Alberto Arreaza Monstserrat

Refrendado
El Ministro del Poder Popular del Despacho de la Presidencia y Seguimiento de la Gestión de Gobierno
(L.S.)
Wilmer Omar Barrientos Fernández

Refrendado
El Ministro del Poder Popular para Relaciones Interiores, Justicia y Paz
(L.S.)
Miguel Eduardo Rodríguez Torres

Refrendado
El Ministro del Poder Popular para Relaciones Exteriores
(L.S.)
Elías Jaua Milano

Refrendado
El Ministro del Poder Popular de Planificación
(L.S.)
Jorge Giordani

Refrendado
El Ministro del Poder Popular de Finanzas
(L.S.)
Nelson José Merentes Díaz

Refrendado
La Ministra del Poder Popular para la Defensa
(L.S.)
Carmen Teresa Meléndez Rivas

Refrendado
El Ministro del Poder Popular para el Comercio
(L.S.)
Alejandro Antonio Fleming Cabrera

Refrendado
El Ministro del Poder Popular para Industrias
(L.S.)
Ricardo José Menéndez Prieto

Refrendado
El Ministro del Poder Popular para el Turismo
(L.S.)
Andrés Guillermo Izarra García

Refrendado
El Ministro del Poder Popular para la Agricultura y Tierras
(L.S.)
Yván Eduardo Gil Pinto

Refrendado
El Ministro del Poder Popular para la Educación Universitaria
(L.S.)
Pedro Enrique Calzadilla

Refrendado
La Ministra del Poder Popular para la Educación
(L.S.)
Maryann del Carmen Hanson Flores

Refrendado
La Ministra del Poder Popular para la Salud
(L.S.)
Isabel Alicia Iturria Caamaño

Refrendado
La Ministra del Poder Popular para el Trabajo y Seguridad Social
(L.S.)
María Cristina Iglesias

Refrendado
El Ministro del Poder Popular para Transporte Terrestre
(L.S.)
Haiman El Troudi Douwara

Refrendado
El Ministro del Poder Popular para Transporte Acuático y Aéreo
(L.S.)
Hebert Josué García Plaza

Refrendado
El Ministro del Poder Popular para Vivienda y Hábitat
(L.S.)
Ricardo Antonio Molina Peñaloza

Refrendado
El Ministro del Poder Popular de Petróleo y Minería
(L.S.)
Rafael Darío Ramírez Carreño

Refrendado
El Ministro del Poder Popular para el Ambiente
(L.S.)
Miguel Leonardo Rodríguez

Refrendado
El Ministro del Poder Popular para Ciencia, Tecnología e Innovación
(L.S.)
Manuel Ángel Fernández Meléndez

Refrendado
La Ministra del Poder Popular para la Comunicación y la Información
(L.S.)
Delcy Eloína Rodríguez Gómez

Refrendado
El Ministro del Poder Popular para las Comunas y Protección Social
(L.S.)
Reinaldo Antonio Iturriza López

Refrendado
El Ministro del Poder Popular para la Alimentación
(L.S.)
Félix Ramón Osorio Guzmán

Refrendado
El Ministro del Poder Popular para la Cultura
(L.S.)
Fidel Ernesto Barbarito Hernández

Refrendado
La Ministra del Poder Popular para el Deporte
(L.S.)
Alejandra Benítez Romero

Refrendado
La Ministra del Poder Popular para los Pueblos Indígenas
(L.S.)
Aloha Joselyn Núñez Gutiérrez

Refrendado
La Ministra del Poder Popular para la Mujer y la Igualdad de Género
(L.S.)
Andreína Tarazón Bolívar

Refrendado
El Ministro del Poder Popular para la Energía Eléctrica
(L.S.)
Jesse Alonso Chacón Escamillo

Refrendado
El Ministro del Poder Popular para la Juventud
(L.S.)
Héctor Vicente Rodríguez Castro

Refrendado
La Ministra del Poder Popular para el Servicio Penitenciario
(L.S.)
María Iris Varela Rangel

Refrendado
El Ministro de Estado para la Banca Pública
(L.S.)
Rodolfo Clemente Marco Torres

Refrendado
El Ministro de Estado para la Transformación Revolucionaria de la Gran Caracas
(L.S.)
Francisco de Asís Sesto Novas

Refrendado
El Ministro de Estado para la Región Estratégica de Desarrollo Integral Central
(L.S.)
Luis Alfredo Motta Domínguez

Refrendado
La Ministra de Estado para la Región Estratégica de Desarrollo Integral Occidental
(L.S.)
Isis Tatiana Ochoa Cañizález

Refrendado
La Ministra de Estado para la Región Estratégica de Desarrollo Integral Los Llanos
(L.S.)
Nancy Evarista Pérez Sierra

Refrendado
La Ministra de Estado para la Región Estratégica de Desarrollo Integral Oriental
(L.S.)
María Pilar Hernández Domínguez

Refrendado
El Ministro de Estado para la Región Estratégica de Desarrollo Integral Guayana
(L.S.)
Carlos Alberto Osorio Zambrano

Refrendado
La Ministra de Estado para la Región Estratégica de Desarrollo Integral de la Zona Marítima y Espacios Insulares
(L.S.)
Marlene Yadira Córdoba de Pieruzzi

Refrendado
El Ministro de Estado para la Región Estratégica de Desarrollo Integral Los Andes
(L.S.)
Celso Enrique Canelones Guevara

JURISPRUDENCIA

Jurisprudencia del Tribunal Supremo sobre el uso de las Tecnologías de Información y Comunicación en la administración de justicia

Mariliana Rico Carrillo*

En el último año ha sido notable la jurisprudencia del Tribunal Supremo de Justicia (TSJ) venezolano donde se considera el uso de las Tecnologías de Información y Comunicación en la administración de justicia. Entre septiembre de 2013 y septiembre de 2014 se han producido diversas sentencias donde se analiza la idoneidad de los medios electrónicos como mecanismos para la interposición de recursos, como instrumentos aptos para realizar notificaciones, o como medios probatorios, entre otros aspectos.

Las sentencias más numerosas son aquellas que se pronuncian sobre el valor probatorio del correo electrónico. Del análisis de las diversas decisiones en esta materia hemos podido observar que aún existen sentencias contradictorias y algunos problemas de interpretación sobre el articulado de la Ley de Mensajes de Datos y Firmas Electrónicas de 2001 (LMDFE). En algunos casos se desecha el valor probatorio de los correos electrónicos aportados en forma impresa al expediente, cuando la norma legal les otorga el valor de una copia simple y establece el procedimiento a seguir en caso de impugnación. En otros aún se observa confusión, más que todo por parte de los jueces de primera y segunda instancia, sobre la función de la Superintendencia de Servicios de Certificación Electrónica, quienes erróneamente han negado el valor probatorio de los mensajes de datos alegando que no se encuentran certificados por ente creado para tal efecto. También se observan algunas imprecisiones de interpretación en las decisiones de las distintas salas respecto de los requisitos necesarios para otorgar autenticidad y valor probatorio a los mensajes de datos.

A continuación presentamos una selección de las principales sentencias correspondientes a este período, comenzando por las más recientes, las cuales han sido agrupadas según la temática tratada.

* Doctora en Derecho mención Cum Laude por la Universidad Carlos III de Madrid. Profesora Titular (Catedrática) de Derecho Mercantil y Nuevas Tecnologías Universidad Católica del Táchira. Árbitro certificado por la Corte Suprema de Justicia del estado de Florida de los Estados Unidos de América.

I. Valor probatorio del correo electrónico

1. Sentencia de la Sala de Casación Social de 1 de julio de 2014[1]. Recurso de casación interpuesto contra la decisión del Juzgado Segundo Superior del Trabajo de la Circunscripción Judicial del Área Metropolitana de Caracas, de 18 de abril de 2011.

   En el proceso por cobro de prestaciones sociales y otros conceptos laborales se consideró el valor probatorio del correo electrónico. En primera instancia, la parte demandada consignó copias de diversos correos electrónicos alegando que fueron enviados por la demandante a un tercero ajeno a la causa. Los correos fueron impugnados en la oportunidad legal correspondiente y se desestimaron en conformidad con lo establecido en los artículos 1.372 y 1.373 del Código Civil, aplicables por remisión del artículo 11 de la Ley Orgánica Procesal del Trabajo.

2. Sentencia de la Sala de Casación Social de 3 de febrero 2014[2]. Recurso de casación interpuesto contra la sentencia del Juzgado Superior Segundo del Trabajo de la Circunscripción Judicial del estado Zulia; de 15 de abril de 2011.

   En el juicio por cobro de prestaciones sociales y otros conceptos laborales, la empresa demandada promueve un correo electrónico en forma impresa. La sala niega valor probatorio alguno a tal documento alegando que no se demostró la autenticidad, confidencialidad e integridad del mensaje a través de medios de prueba auxiliares como la inspección judicial o la experticia.

   En relación con esta decisión, cabe recordar que la LMDFE otorga a los correos electrónicos impresos el valor de una copia simple, por lo que no pueden ser desechados por el simple hecho de producirse de esta forma.

3. Sentencia de la Sala Político Administrativa de 28 de enero de 2014[3]. Recurso de apelación interpuesto contra la sentencia de la Corte Primera de lo Contencioso Administrativo, del 23 de abril de 2013.

1 El texto integro de la sentencia está disponible en: http://www.tsj.gov.ve/decisiones/scs/julio/166383-0819-1714-2014-11-710.HTML (Consulta: 25 de septiembre de 2014)

2 El texto integro de la sentencia está disponible en: http://www.tsj.gov.ve/decisiones/scs/febrero/160811-0056-3214-2014-11-701.HTML (Consulta: 25 de septiembre de 2014)

3 El texto integro de la sentencia está disponible en: http://www.tsj.gov.ve/decisiones/spa/enero/160700-00103-29114-2014-2013-1212.HTML (Consulta: 25 de septiembre de 2014)

La sentencia recurrida declaró sin lugar un recurso de nulidad previo, interpuesto por una sociedad mercantil contra un acto administrativo dictado por la COMISIÓN DE ADMINISTRACIÓN DE DIVISAS (CADIVI) mediante el cual se confirmó la declaratoria de perención de una solicitud de adquisición de divisas.

Tanto en la sentencia apelada como en el recurso se valoran plenamente unos correos electrónicos promovidos por la parte actora, los cuales fueron sometidos a un análisis pericial con el objeto de dar certeza del contenido y la fecha de envío y recepción de las comunicaciones electrónicas.

La validez de los correos electrónicos, agregados en copia simple al expediente, fue determinada a través de una experticia practicada sobre el servidor de la recurrente que demostró la autenticidad e integridad de los mensajes transmitidos, así como la fecha de envío y recepción.

4. Sentencia de Sala de Casación Civil de 11 de octubre de 2013[4]. Recurso de casación interpuesto contra la decisión del Juzgado Superior Marítimo con Competencia Nacional y sede en la ciudad de Caracas, de 25 de febrero de 2013.

En el juicio por indemnización por daños y perjuicios no se otorgó valor probatorio a un plano de estiba enviado por correo electrónico. En este caso, la disconformidad del recurrente respecto de la sentencia de alzada está relacionada con la manera en que el sentenciador valoró el correo electrónico correspondiente a un plano de estiba consignado con el libelo de demanda en formato impreso.

El formalizante denunció infracción los artículos 2°, 4° y 7° de la LMDFE, el primero por falsa aplicación, el segundo por error de interpretación y el tercero falta de aplicación, alegando que el juez de alzada no valoró correos electrónicos remitidos "*…basado en la supuesta exigencia de certificación de firma electrónica para su análisis, supuesto éste que no es ajustado a derecho, configurándose así un vicio en la valoración del referido instrumento probatorio…*"

En el análisis de los hechos, la sala se pronuncia sobre el error en que incurrió el juez en la sentencia recurrida al indicar que "*…la falta de acreditación no perjudica el mensaje de datos, en formato impreso, el juez estaba obligado a examinar y apreciar dicha prueba, conforme lo previsto en el artículo 429 del Código de Procedimiento Civil…*" A pesar de estas consideraciones, la sala declaró improcedente la infracción denunciada y declaró sin lugar el recurso de casación.

4 El texto integro de la sentencia está disponible en: http://www.tsj.gov.ve/decisiones/scc/octubre/157423-RC.000609-111013-2013-13-247.html (Consulta: 25 de septiembre de 2014)

5. Sentencia de la Sala de Casación Social de 26 de septiembre de 2013[5]. Recurso de casación interpuesto contra la sentencia del Juzgado Superior Primero del Trabajo de la Circunscripción Judicial del estado Aragua, de 26 de mayo del 2011.

   En el juicio por cobro de prestaciones sociales y otros conceptos laborales, el demandante promovió diversos correos electrónicos en forma impresa que fueron impugnados y desconocidos por las demandadas, en su carácter de copia simple. También se promovió en formato impreso información de la página web de una de las empresas demandadas.

   Al establecer el valor de estos instrumentos, la sala observa que

   > *….si bien la impresión de los correos electrónicos y página web tienen la misma eficacia probatoria que la Ley otorga a los documentos escritos, la misma dependerá de que el mensaje de datos esté asociado a algún mecanismo de seguridad que permita identificar su origen y autoría, cuestión que no se verificó en el presente asunto, razón por la cual carecen de eficacia probatoria.*

   Aunque la sala no lo menciona en forma expresa, en este caso la eficacia probatoria de los correos queda desvirtuada por la impugnación de los correos electrónicos impresos por parte de la demandada, de acuerdo con lo establecido en el artículo 429 del Código de Procedimiento Civil.

6. Sentencia de la Sala de Casación Civil de 24 de septiembre de 2013[6]. Recurso de casación interpuesto contra la sentencia dictada por el Juzgado Superior en lo Civil, Mercantil y del Tránsito de la Circunscripción Judicial del estado Nueva Esparta, de 30 de noviembre de 2012.

   El recurso de casación fue declarado sin lugar al considerar improcedente la denuncia de la infracción del formalizante, quien alegó que el juez superior había incurrido en el vicio de silencio de prueba y en la infracción del artículo 509 del Código de Procedimiento Civil, al no expresar el mérito probatorio del correo electrónico utilizado por la demandante como medio para interrumpir la prescripción de la acción.

   La Sala de Casación Civil pudo constatar que el juez superior si otorgó valor probatorio tanto al correo electrónico como a la experticia promovida para su ratificación en juicio, considerando que:

5 El texto integro de la sentencia está disponible en: http://www.tsj.gov.ve/decisiones/scs/septiembre/156985-0788-26913-2013-11-897.HTML (Consulta: 25 de septiembre de 2014)

6 El texto integro de la sentencia está disponible en: http://www.tsj.gov.ve/decisiones/scc/septiembre/156903-RC.000550-24913-2013-13218.html (Consulta: 25 de septiembre de 2014)

> *… con el mismo se evidenciaba la interrupción de la prescripción alegada por los accionantes en el juicio, toda vez que consideró que dicha prueba demuestra claramente que la parte actora reclamó el cumplimiento de la obligación de manera cierta y efectiva con el correo electrónico enviado en fecha 10-02-2010, y ello, a su modo de ver, constituye un acto interruptivo de la prescripción de acuerdo con lo estipulado en el artículo 1.969 del Código Civil.*

II. Interposición de recursos por correo electrónico

1. Sentencia de la Sala Constitucional de 19 de noviembre de 2013[7]. Interposición del recurso de amparo a través del correo electrónico.

Por interpretación progresiva del artículo 16 de la Ley Orgánica de Amparo sobre Derechos y Garantías, la Sala Constitucional admite dentro del medio telegráfico la posibilidad de interponer el recurso de amparo a través del correo electrónico, limitándola a casos de urgencia y a su ratificación, personal o mediante apoderado, dentro de los tres (3) días siguientes a su recepción. Esta sentencia reconoce el uso de Internet como medio novedoso y efectivo de transmisión electrónica de comunicación y hace mención a su regulación en la LMDFE.

A pesar que la ley exige en estos casos la ratificación del recurso en los tres días siguientes a la recepción de la comunicación electrónica, la Sala Constitucional eximió al afectado del cumplimiento de este requisito por estar privado de su libertad. Aunque la referida sala valoró positivamente el medio electrónico como mecanismo idóneo para la interposición del recurso, se declaró incompetente para conocer de la acción de amparo, atribuyendo la competencia a la Corte de Apelaciones del Circuito Judicial Penal de la Circunscripción Judicial del Estado Vargas, para que se pronunciase sobre la admisibilidad del amparo interpuesto.

2. Sentencia de la Sala de Casación Social de 13 de noviembre de 2013[8]. Recurso de control de legalidad interpuesto contra la sentencia del Juzgado Superior Civil, Mercantil, del Tránsito y de Menores de la Circunscripción Judicial del estado Trujillo, de 26 de abril del año 2013.

El recurso de control de legalidad contra la sentencia de segunda instancia en un juicio de restitución internacional de custodia de menores, fue interpuesto a través del correo electrónico por la Autoridad Central

7 El texto integro de la sentencia está disponible en:http://www.tsj.gov.ve/decisiones/scon/noviembre/158844-1635-191113-2013-13-0913.HTML (Consulta: 25 de septiembre de 2014)

8 El texto integro de la sentencia está disponible en: http://www.tsj.gov.ve/decisiones/scs/noviembre/158631-1092-131113-2013-13-676.HTML (Consulta: 25 de septiembre de 2014)

Venezolana, en nombre de la parte actora. La Sala de Casación Social valora positivamente la utilización del medio electrónico y considera que se han cumplido los requisitos de forma impuestos en la normativa legal para la interposición del recurso, que fue complementado con el escrito de fundamentación respectivo.

III. La página web del Tribunal Supremo de Justicia como medio de notificación

1. Sentencia de la Sala de Casación Civil de 03 de febrero de 2014[9]. Solicitud de exequátur de sentencia extranjera sobre la disolución del vínculo matrimonial.

   En este procedimiento, se pone de manifiesto la utilidad de la página web del TSJ como un medio complementario para practicar la notificación de la citación por carteles. Ante la imposibilidad de citar a una de las partes interesadas en la causa, el juzgado de sustanciación ordenó citar a la demandada mediante cartel que fijó en la cartelera de la Secretaría de la Sala de Casación Civil y en el portal electrónico del TSJ, de conformidad con lo pautado en los artículos 85, 93 y 98 de la Ley Orgánica que rige las funciones de este Alto Tribunal.

2. Sentencia de la Sala Constitucional de 16 de diciembre de 2013[10]. Solicitud de revisión de la sentencia N° 518, dictada el 4 de julio de 2013 por la Sala de Casación Social que declaró desistido el recurso de casación interpuesto contra la decisión del Juzgado Cuarto Superior del Trabajo de la Circunscripción Judicial del Estado Zulia, de 21 de noviembre de 2011.

   La Sala Constitucional declaró sin lugar la solicitud de revisión presentada, alegando que no hubo indefensión de las partes, toda vez que la Sala de Casación Social programó con suficiente tiempo la audiencia pública y contradictoria

   > *….y esa información estaba reflejada en el portal electrónico de este máximo Tribunal, por lo que la parte contaba con la manera de enterarse y asistir a la misma. Por tanto, lo que se evidencia en el caso*

9 El texto integro de la sentencia está disponible en: http://www.tsj.gov.ve/decisiones/scc/febrero/160791-exe.000044-3214-2014-09-615.html
(Consulta: 25 de septiembre de 2014)

10 El texto integro de la sentencia está disponible en: http://www.tsj.gov.ve/decisiones/scon/diciembre/159750-1777-161213-2013-13-0945.HTML (Consulta: 25 de septiembre de 2014)

de autos es que la falta de seguimiento a la causa constituyó un acto de negligencia de la parte accionante.

Las dos sentencias comentadas en este epígrafe siguen la doctrina del TSJ sobre la «naturaleza informativa» de la página web de esta institución, al entender que se trata de medio auxiliar de divulgación de la actividad judicial. Este criterio fue establecido en la sentencia No. 982 de la Sala Constitucional de 06 de junio de 2001 y ha sido reiterado en diversas decisiones emanadas de las distintas salas que componen el TSJ venezolano.

IV. Prueba testimonial a través de medios audiovisuales

1. Sentencia de la Sala de Casación Penal de 11 de diciembre de 2013[11]. Recurso de casación interpuesto contra la decisión de la Sala Única de la Corte de Apelaciones de la Sección de Adolescente, con competencia en materia de violencia contra la mujer del Circuito Judicial Penal del estado Zulia, de 22 de abril de 2013.

En el juicio por la comisión de delitos de abuso sexual a adolescente y amenaza incoado en primera instancia, las declaraciones de las víctimas fueron tomadas a través de los medios audiovisuales (videoconferencia) admitidos en el artículo 27 de la Ley de Protección de Víctimas, Testigos y demás Sujetos Procesales. Esta norma permite el uso de Tecnologías de Información y Comunicación durante el desarrollo del juicio oral y público, de manera alterna y cuando las circunstancias así lo justifiquen, con la finalidad de proteger a los sujetos procesales y a cualquier interviniente llamado al proceso, garantizando siempre el derecho a la defensa y el contradictorio. El juez de primera instancia permitió la declaración de las víctimas a través de la videoconferencia en atención al interés superior de la adolescente involucrada en el caso.

La parte recurrente denuncia la errónea interpretación de esta norma junto con los artículos 16 y 18 del Código Orgánico Procesal Penal (COP), que consagran los principios de inmediación y contradicción en el proceso penal, alegando que

> *…las testimoniales de las víctimas fueron evacuadas de manera ilegal, y están totalmente viciadas (en virtud de haberse tomado entrevista por medio de una video-conferencia, justificado por el tribunal sobre la base del interés superior del niño, niña y adolescente)…*

11 El texto integro de la sentencia está disponible en: http://www.tsj.gov.ve/decisiones/scp/diciembre/159634-459-111213-2013-C13-276.HTML (Consulta: 25 de septiembre de 2014)

Sobre este caso, consideramos necesario precisar que la norma es clara al manifestar que se podrá utilizar el sistema de videoconferencia (y otros medios alternativos) en el desarrollo del juicio oral y público, en circunstancias debidamente justificadas, siempre y cuando se respete el derecho a la defensa y el contradictorio. En cuanto al principio de inmediación, el artículo 16 del COP establece que los jueces deben presenciar, ininterrumpidamente, el debate y la incorporación de las pruebas de las cuales obtienen su convencimiento, circunstancia que puede cumplirse a través del medio electrónico que permite una interacción directa entre el juez y los testigos.

La sala desestima esta denuncia al considerar que el alegato recursivo carece de fundamento, al no establecer claramente la manera como fueron erróneamente interpretadas las disposiciones legales denunciadas.

ÍNDICE ACUMULADO

ARTÍCULOS

CONFERENCIAS

CONTRIBUCIONES ESPECIALES

COMENTARIOS ESPECIALIZADOS

RESEÑA LEGISLATIVA

CRÓNICA JURÍDICA

SECCION MONOGRÁFICA

Las implicaciones jurídicas de las redes sociales en Internet

ARRIETA ZINGUER, Miguel.
- El impacto de las redes sociales en el comercio electrónico con consumidores. **14**, (2013), 135-164

CHACÓN GÓMEZ, Nayibe.
- La responsabilidad de los proveedores de servicio en las redes sociales. **14**, (2013), 207-230

LÓPEZ JIMÉNEZ, David.
- Las redes sociales como espacios publicitarios: el papel de la autorregulación. **14**, (2013), 165-186

RAMÍREZ, Sulmer Paola.
- Los contenidos publicados por el trabajador en *Facebook* y sus consecuencias jurídico laborales. **14**, (2013), 187-205

RICO CARRILLO, Mariliana y LÓPEZ JIMÉNEZ, David.
- Las redes sociales en Internet: consideraciones generales y problemática jurídica. **14**, (2013), 101-112

RICO CARRILLO, Mariliana.
- El ejercicio de los derechos fundamentales y las libertades públicas a través de *Facebook*. **14**, (2013), 113-134

LEGISLACIÓN

II.1. Nacional

Decretos

Decreto N° 825 del 10 de mayo de 2000 mediante el cual se declara el acceso y el uso de Internet como política prioritaria para el desarrollo cultural, económico, social y político de la República Bolivariana de Venezuela. **1**, (2002), 185-188.

Decreto N°1.093 de 24 de noviembre de 2000 mediante el cual se decreta el Reglamento de Interconexión. **2**, (Enero/Junio 2003), 163-180.

Decreto Nº 1.094 de 24 de noviembre de 2000 mediante el cual se decreta el Reglamento sobre Habilitaciones Administrativas y Concesiones de uso y explotación del espectro radio-eléctrico. **2**, (Enero/Junio 2003), 181-207.

Decreto Nº 1.095 de 24 de noviembre de 2000 mediante el cual se decreta el Reglamento de apertura de los servicios de telefonía básica. **2**, (Enero/Junio 2003), 209-245.

Decreto Nº 2.189 de 13 de diciembre de 2002 mediante el cual se decreta el Reglamento sobre los tributos establecidos en la Ley Orgánica de Telecomunicaciones. **2**, (Enero/Junio 2003), 255-280.

Decreto-Ley de Mensajes de Datos y Firmas Electrónicas. **1**, (2002), 255-273.

Decreto N° 2.614, de fecha 24 de septiembre de 2003 mediante el cual se decreta el Reglamento de la Ley Orgánica de Telecomunicaciones sobre el Servi-

Leyes

Reglamentos

Resoluciones

ciamiento o Pago Electrónico", **10**, (2008-2009), 203-226.

Resolución por la cual se dictan "Normas relativas a la Protección de Usuarios y Usuarias de los servicios Financieros". **12**, (2011), 247-265

Providencias

Providencia Administrativa que establece el deber de presentación electrónica de las Declaraciones del Impuesto sobre la Renta. **11**, (2010), 247-249

Providencia Administrativa que establece el deber de presentación electrónica de las Declaraciones del Impuesto al Valor Agregado. **11**, (2010), 251-253

II.2. Internacional

Directivas

Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999. **3**, (Julio/Diciembre 2003), 197-211.

Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000. **3**, (Julio/Diciembre 2003), 213-242.

Directiva 2000/46/CE del Parlamento Europeo y del Consejo, de 18 de septiembre de 2000. **3**, (Julio/Diciembre 2003), 243-252.

Directiva 2007/64/CE del Parlamento Europeo y del Consejo de 13 de abril de 2007 sobre servicios de pago en el mercado interior. **10**, (2008-2009), 227-301.

Directiva 2009/64/CE del Parlamento Europeo y del Consejo del 23 de abril de 2009 sobre Protección jurídica de programas de ordenador. **11**, (2010), 341-349.

Directiva 2010/13/UE del Parlamento Europeo y del Consejo de 10 de marzo de 2010 sobre la prestación de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual). **12**, (2011), 267-311

Leyes Modelo

Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996) con la guía para su incorporación al Derecho Interno. **3**, (Julio/Diciembre 2003), 181-190.

Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (2001). **3**, (Julio/Diciembre 2003), 191-196.

Legislación española

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. **4**, (Enero/Julio 2004), 219-261.

Ley 59/2003, de firma electrónica. **4**, (Enero/Julio 2004), 263-300.

Ley 32/2003, de 3 denoviembre, General de Telecomunicaciones. **5**, (Julio/Diciembre 2004), 161-252.

Ley 22/207, de 11 de julio, sobre Comercialización a Distacia de Servicios Financieros destinados a los Consumidores. **9**, (Enero/Diciembre 2007), 185-2005.

Ley 16/2009 de 13 de noviembre, sobre Servicio de Pago. **11**, (2010), 255-304.

Ley 7/2010 de 31 de marzo, General de la Comunicación Audivisual. **12**, (2011), 313-393

Real Decreto 322/2008 de 29 de febrero sobre el régimen jurídico de las entida-

JURISPRUDENCIA

Tribunal Supremo de Justicia venezolano. **2**, (Enero/Junio 2003), 313-314.
- El valor jurídico de la página Web del Tribunal Supremo de Justicia. **3**, (Julio/Diciembre 2003), 271-273.
- La eficacia probatoria de los correos electrónicos en la jurisprudencia del Tribunal Supremo de Justicia venezolano. **10**, (2008-2009), 325-330.
- Consideraciones sobre la validez de las condiciones generales y particulares de las pólizas de seguros contenidas en soportes documentales electrónicos. **11**, (2010), 353-358.
- De nuevo sobre el valor probatorio de los correos electrónicos en la jurisprudencia del Tribunal Supremo de Justicia venezolano. **12**, (2011), 397-400
- Jurisprudencia del Tribunal Supremo sobre el uso de las Tecnologías de Información y Comunicación en la administración de justicia. **15**, (2014), 341-348.

SALGUEIRO, José Ovidio.
- El valor probatorio del correo electrónico. Comentario a la sentencia 2201-04 de la Corte Superior del Niño y el Adolescente del Área Metropolitana y Nacional de Adopción Internacional. **6-7**, (Enero/Diciembre 2005), 353-355.

URSO CEDEÑO, Giuseppe.
- Sentencia de la Sala Constitucional del Tribunal Supremo de Justicia que resuelve el Recurso de Colisión intentado entre el artículo 40 de la Ley de Protección al Consumidor y al Usuario y los artículos 145 y 214 de la Ley Orgánica de Telecomunicaciones. **4**, (Enero/Julio 2004), 325-329

Sentencias

Sentencia del Tribunal Supremo de Justicia venezolano de 03.08.2001 sobre el reconocimiento del valor jurídico de la información contenida en el sitio web del Tribunal. **1**, (2002), 320-323.

Sentencia de la Sala Constitucional del Tribunal Supremo de Justicia venezolano de 01 de febrero de 2000. **2**, (Enero/Junio 2003), 315-337

Sentencia de la Sala Constitucional del Tribunal Supremo de Justicia venezolano de 19 de agosto de 2002. **3**, (Julio/Diciembre 2003), 275-277.

Sentencia de la Sala Constitucional del Tribunal Supremo de Justicia venezolano de 05 de agosto de 2003. **4**, (Enero/Julio 2004), 331-338

Sentencia de la Sala Constitucional del Tribunal Supremo de Justicia venezolano de 03 de agosto de 2004. **5**, (Julio/Diciembre 2004), 277-305

Sentencia de la Sala Político-Administrativa del Tribunal Supremo de Justicia venezolano de 8 de noviembre de 2005. **6-7**, (Enero/Diciembre 2005), 365-374.

In the United States District Court for the Northern District of California San Jose División, fecha 17 de marzo 2006, **8**, (Enero/Diciembre 2006), 351-369.

Sentencia de la Sala Político Administrativa del Tribunal Supremo de Justicia venezolano de fecha 22 de mayo de 2007 sobre el caso RCTV. **9**, (Enero/Diciembre 2007), 223-259.

Sentencia de la Sala de Casación Civil del Tribunal Supremo de Justicia venezolano de fecha 24 de octubre de 2007 sobre el valor probatorio

RECENSIÓN

trónico, Cavecom, Caracas, 2004, 294 págs. **4**, (Enero/Julio 2004), 341-245.

- BATUECAS CALETRIO, Alfredo: *Pago con tarjeta de crédito: Naturaleza y régimen jurídico*, Revista Aranzadi de Derecho Patrimonial Nº 15 (monográfico), Thomson-Aranzadi, Navarra, 2005, 429 págs. **6-7**, (Enero/ Diciembre 2005), 377-378.

ALBA FERNÁNDEZ, Manuel. Selección y comentarios sobre bibliografía jurídica especializada

- RODRÍGUEZ DE LAS HERAS BADELL, Teresa: *El régimen jurídico de los Mercados Electrónicos Cerrados (e-Marketplaces)*, Madrid, Marcial Pons, 2006. **9**, Enero/Diciembre 2007), 321-324.

LÓPEZ JIMÉNEZ, David: Selección y comentarios sobre bibliografía jurídica especializada

- RICO CARRILLO, Mariliana: *El pago electrónico en Internet: estructura operativa y régimen jurídico*, Madrid, Thomson Reuters Aranzadi, 2012, 304 páginas. **13**, (2012), 281-284

Reglas para el envío de artículos

1. El material presentado debe ser inédito, entendiéndose que el mismo no ha sido publicado ni sometido para publicación en otro medio de divulgación. El Consejo Editorial se reserva el derecho de publicar de manera excepcional artículos que ya han sido publicados.

2. Los artículos deben estar redactados en programas editores que funcionen en ambiente WindowsTM 3.0 o superiores. Los gráficos o imágenes que contenga el artículo deben estar especificados con los formatos o extensiones en que se hicieron (Exce1TM, Corel DrawTM, jpg, gif, bmp, y otros), asimismo, las ilustraciones deben estar numeradas y a continuación del texto (no se aceptarán las que se encuentren al final del artículo). Las revistas podrán decidir no incluirlas, previa comunicación al autor o autores, si éstas no llenan los requisitos técnicos para su reproducción.

3. El texto del artículo debe redactarse tomando en cuenta los siguientes parámetros:
   3.1. La primera página debe contener:
      a) Título del artículo
      b) Nombre del autor o autores
      c) Título académico y afiliación institucional
      d) Dirección del autor y correo electrónico
      e) Síntesis curricular no mayor a diez (10) líneas

   3.2. La segunda página debe contener un resumen no mayor de ciento cuarenta (140) palabras, concentrándose en los objetivos, métodos de estudio, resultados y conclusiones. A1 final del mismo se deben incluir las palabras claves en un número no mayor a cinco (5).
      a) El resumen y las palabras claves deben venir redactadas en español e inglés
      b) Se podrán aceptar artículos redactados en inglés, francés u otros idiomas sólo en casos especiales, debiendo contener las palabras claves en español e inglés.

   3.3. El texto del artículo debe estructurarse en secciones debidamente identificadas, siendo la primera la introducción (o reseña de los conocimientos existentes, limitada estrictamente al tema tratado en el artículo). Las secciones deben identificarse sólo con números arábigos. Cada artículo antes de la primera sección o sección introductoria, debe tener un sumario en el que se enumeren los temas que se van a desarrollar (las secciones en las cuales fue dividido el trabajo).

   3.4. Si parte del material trabajado (textos, gráficos e imágenes utilizados) no son originales del autor o de los autores, es necesario que los mismos estén acompañados del correspondiente permiso del autor (o de los autores) y el editor donde fueron publicados originalmente, en su defecto, se debe indicar la fuente de donde fueron tomados.

   3.5. En las referencias bibliográficas se debe utilizar el sistema de cita formal, haciendo 1a correspondiente referencia en las notas a pie de página, las cuales deben ser enumeradas en números arábigos, siguiendo un orden correlativo.

Las citas, en las notas al pie de página, se harán siguiendo los siguientes ejemplos; según se trate de:

A. Libros

Mariano Aguilar Navarro: *Derecho Internacional Privado*, VI. 4a. edición, 2a. reimpresión. Madrid. Universidad Complutense de Madrid, 1982, p.199 (o pp. 200 y ss).

Marino Barbero Santos: "Consideraciones sobre el Estado peligroso y las Medidas de Seguridad, con especial referencia al Derecho Italiano y Alemán". *Estudios de Criminología y Derecho Penal*. Valladolid. Universidad de Valladolid, 1972, pp. 13-61.

Vicente Mujica Amador: *Aproximación al Hombre y sus Ideologías*. Caracas. Editorial Vidabun, 1990.

Hans Kelsen: *Teoría Pura del Derecho*. XVII edición. Buenos Aires. EUDEBA, 1981.

B. Cita sucesiva del mismo libro

M. Aguilar N.*: Derecho Internacional* V.II.… op. cit., p.78 y ss.

C. Obras colectivas

Haydée Barrios: "Algunos aspectos de cooperación judicial internacional en el sistema venezolano de derecho internacional privado". *Libro-Homenaje a Werner Goldschmidt*. Caracas. Facultad de Ciencias Jurídicas y Políticas, Universidad Central de Venezuela. 1997, pp. 383-419. Si se desea citar un determinado párrafo o página se agrega: especialmente, p. 80 o pp. 95-98.

D. Revistas

Gonzalo Parra-Aranguren: "El Centenario de la Conferencia de La Haya de Derecho Internacional Privado". *Revista de la Facultad de Ciencias Jurídicas y Políticas*, N° 85. Caracas. Universidad Central de Venezuela, 1992, pp. 75-100.

E. Cita sucesiva del mismo artículo

G. Parra-Aranguren: "*El Centenario de la Conferencia*..." op.cit., pp.80-85.

F. Citas de jurisprudencia

Orden de citar: Tribunal, N° y fecha de la sentencia, partes y fuentes de publicación. Ejemplo:
Corte Superior del Distrito Federal, N°…, 6-5-1969 (Jacques Torfs vs. Clemencia de Mier Garcés), Jurisprudencia Ramirez y Garay, Vol. 21, p. 163.

G Citas de testimonios verbales y entrevistas

Se indicará el nombre de la persona que proporciona la información, la forma como se obtuvo y la fecha. Por ejemplo:

F. Rodríguez. Entrevista, 30/03/1999.

Esta información puede suministrarse siempre que lo autorice quien proporciona la información[1].

H. Citas de páginas web

Si la cita se refiere a un sitio web (cita de carácter general) se coloca el *home page*. Si es una página específica dentro de un sitio web (cita de carácter especial) se debe colocar en primer lugar, la dirección del *link* (sub-página) y en segundo lugar la dirección donde aparece alojada la información, (*home page*). Debe indicarse también la fecha de la consulta, entre corchetes, indicando el año, luego el mes y finalmente el día
Ejemplos:

a) Cita de carácter general:
www.zur2.com.fipa. [Consulta: 2008, Noviembre 27].

b) Cita de carácter especial:
   - Tatiana B. de Maekelt: La Ley de Derecho Internacional Privado http://zur2.com/users/fipa/objetivos/leydip1/tamaek.htm 10/02/2001. www.zur2.com.fipa. [Consulta: 2008, Noviembre 27].

   - Haydée Barrios: El Domicilio http://zur2.com/users/fipa/objetivos/leydip1/barrios.htm 8/04/2002. www.zur2.com.fipa. [Consulta: 200, Noviembre 27].

4. Los artículos deben tener una extensión no mayor de cuarenta (40) cuartillas o páginas, escritas a espacio y medio y con un margen izquierdo de cuatro (4) centímetros. Tipo de letra: Times New Roman 12.

5. Los artículos pueden ser remitidos en un archivo adjunto, a la dirección electrónica: albornoz@ucat.edu.ve, o al correo electrónico del director de la revista:

   - Revista Tachirense de Derecho: Prof. José Luis Villegas villegas@ucat.edu.ve
   - Revista *Tributum*: Prof. Jesús Manuel Oliveros joliveros@ucat.edu.ve
   - Revista Paramillo: Prof. Felipe Guerrero felipeguerrero11@gmail.com
   - Revista Derecho y Tecnología: Prof. Mariliana Rico marilianarico@yahoo.com

6. Los autores deberán firmar una autorización (en un formato que remitirá a tal efecto) donde se especifica el derecho que tiene la revista, y por ende, la Universidad Católica del Táchira, de reproducir el artículo en este medio de comunicación, sin ningún tipo de retribución económica o compromiso de la Universidad con el autor o los autores, entendiéndose éste como una contribución a la difusión del conocimiento y/o desarrollo tecnológico, cultural o científico de la comunidad o del país en el área en que se inscribe.

7. Cuando se envíen textos que estén firmados por más de un autor, se presumirá que todos los autores han revisado y aprobado el original enviado.

1 UPEL: *Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales*. Caracas. FEDEUPEL. 2003, p. 91.

8. Se reserva el derecho de hacer las correcciones de estilo que se consideren convenientes, una vez que el trabajo haya sido aceptado por el Consejo de Redacción para su publicación.

9. Los artículos serán analizados por un Comité de Árbitros y por un Consejo de Redacción. El cumplimiento de las normas no garantiza su publicación, si el trabajo no es aprobado por estas instancias.

10. La Universidad Católica del Táchira, el editor y el Consejo de Redacción de la revista, no se responsabilizarán de las opiniones expresadas por los colaboradores en sus respectivos artículos.

11. La UCAT se reserva el derecho de distribuir el contenido de la revistas en su página web o en otras páginas de contenido académico o científico.

Article Submissions Guidelines

1. The material must be unpublished, understanding it had not been published or presented to be evaluated by other divulging means. The Editorial Board reserves the right to publish articles, in exceptional cases, when they have already been published.

2. Articles must be redacted in editor programs that work in Windows™ 3.0 or higher. The graphics or images that present the article must be specified with the formats or extensions where they were made (Excel™, Corel Draw™, jpg, gif, bmp, and others). In the same way, the illustrations must be numbered just after the text (Those illustrations at the end of the article will be not accepted). The journals could decide not to include them, by communication to the author or authors in advance, if them do not fulfill the technical requirements to their publication.

3. The text of the article must be redacted considering the following parameters:
   3.1. The first page must have:
      a) Title of the article
      b) Author or author's name
      c) Academic title and institutional affiliation
      d) Author address and e-mail
      e) Resume no longer than 10 lines

   3.2. The second page must have an abstract no longer than one hundred and forty words (140), focusing on the goals, methodology, results and conclusions. At the end, the key words must be included in a maximum number of five (5).
      a) The abstract and the key words must be written in Spanish and English.
      b) Articles in English, French and other languages could be accepted, just in special cases. In all cases they must have the key words in Spanish and English.

   3.3. The text article must be structured in clearly identified sections, being the first the introduction (description of the existent knowledge, limited to the subject of the article). The sections must be identified with Roman and Arabic numerals. Each article, before section one or introduction, must have a summary where appear numbered the subjects to be discuss on the paper (sections the article was divided).

   3.4. If part of the material (text, graphics, images) is not original of the author or authors, is necessary that this material to be authorized by the original author (or authors) and the editor where were first published, in lack of this, the source where they were taken must be indicated.

   3.5. The formal citing system must be used for the bibliographic references, doing the right reference at the foot of the page numbered in Arabic numeral, following a correlative order.

   The references in the footnotes will be included according to the following examples:

A. Books

Mariano Aguilar Navarro: *Derecho Internacional Privado*, VI. 4a. edición, 2a. reimpresión. Madrid. Universidad Complutense de Madrid, 1982, p.199 (o pp. 200 y ss).

Marino Barbero Santos: "Consideraciones sobre el Estado peligroso y las Medidas de Seguridad, con especial referencia al Derecho Italiano y Alemán". *Estudios de Criminología y Derecho Penal*. Valladolid. Universidad de Valladolid, 1972, pp. 13-61.

Vicente Mujica Amador: *Aproximación al Hombre y sus Ideologías*. Caracas. Editorial Vidabun, 1990.

Hans Kelsen: *Teoría Pura del Derecho*. XVII edición. Buenos Aires. EUDEBA, 1981.

B. Subsequent quotations of the same book

M. Aguilar N.*: Derecho Internacional* V.II.… op. cit., p.78 y ss.

C. Collective Works

Haydée Barrios: "Algunos aspectos de cooperación judicial internacional en el sistema venezolano de derecho internacional privado". *Libro-Homenaje a Werner Goldschmidt*. Caracas. Facultad de Ciencias Jurídicas y Políticas, Universidad Central de Venezuela. 1997, pp. 383-419. Si se desea citar un determinado párrafo o página se agrega: especialmente, p. 80 o pp. 95-98.

D. Journals

Gonzalo Parra-Aranguren: "El Centenario de la Conferencia de La Haya de Derecho Internacional Privado". *Revista de la Facultad de Ciencias Jurídicas y Políticas*, N° 85. Caracas. Universidad Central de Venezuela, 1992, pp. 75-100.

E. Subsequent quotations of the same article

G. Parra-Aranguren: "*El Centenario de la Conferencia*..." op.cit., pp.80-85.

F. Quotation of jurisprudence:

Corte Superior del Distrito Federal, N°…, 6-5-1969 (Jacques Torfs vs. Clemencia de Mier Garcés), Jurisprudencia Ramirez y Garay, Vol. 21, p. 163.

G Quotation of oral testimonies and interviews

It must include the name of the person providing the information, how it was obtained, and the date:

F. Rodríguez. Entrevista, 30/03/1999.

This information can be provided only if it is authorized by the provider of the information[1].

1 UPEL: *Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales*. Caracas. FEDEUPEL. 2003, p. 91.

H. Quotation of web pages

If a quote refers to an entire website (general citation), should include the reference of the home page. If is a **specific page within a website** (special citation), should include in first place, the link (sub-page) and in second place, the reference of the home page. It should also indicate the date the page was visited. This information should be in listing showing year, month, and day.

a) General quotation:
www.zur2.com.fipa. [Visited: 2008, Noviembre 27].

b) Special quotation:
- Tatiana B. de Maekelt: La Ley de Derecho Internacional Privado http://zur2.com/users/fipa/objetivos/leydip1/tamaek.htm 10/02/2001. www.zur2.com.fipa. [Consulta: 2008, Noviembre 27].

- Haydée Barrios: El Domicilio http://zur2.com/users/fipa/objetivos/leydip1/barrios.htm 8/04/2002. www.zur2.com.fipa. [Visited: 200, Noviembre 27].

4. Articles must have a maximum extension of forty (40) pages written in 1.5 space with a left margin of four (4) centimeters. The type letter will be Times New Roman 12.

5. Articles must be sent in an attachment to the e-mail: albornoz@ucat.edu.ve, or to the e-mail of the director of the journal:
   - Revista Tachirense de Derecho: Prof. José Luis Villegas villegas@ucat.edu.ve
   - Revista *Tributum*: Prof. Jesús Manuel Oliveros joliveros@ucat.edu.ve
   - Revista Paramillo: Prof. Felipe Guerrero felipeguerrero11@gmail.com
   - Revista Derecho y Tecnología: Prof. Mariliana Rico marilianarico@yahoo.com

6. Authors should sign an authorization (a format will be sent to this purpose) where it is specified the right of the journal, as well as the Universidad Católica del Táchira, to publish the article on this divulging means, without any economic retribution or commitment of the University with the author or authors, understanding the article is a contribution to the divulging of knowledge and technological development, cultural or scientific of the community or the country in the area where it is registered.

7. When articles are sign by more than an author, it would be presumed that all authors have been check and approved the original text sent.

8. The right of change of stylus that is considered convenient is reserved, once the article has been accepted by the Editorial Board for its publication.

9. An Arbitral Committee and an Editorial Board will analyze the articles. The observance of these rules does not guarantee the publication of the article if this is not approved by these instances.

10. The Universidad Católica del Táchira, the editor, and the Editorial Board of the journal, are not responsible of the expressed opinions by the collaborating and the articles.

11 The Universidad Católica del Táchira reserves the right to distribute the contents of their journals on its website, or on other pages of academic or scientific content.

DERECHO Y TECNOLOGÍA

VICERRECTORADO ACADÉMICO DECANATO DE INVESTIGACIÓN Y POSTGRADO	15/2014

Revista de Derecho y Tecnología, Enero / Diciembre 2014,
de la Universidad Católica del Táchira, la presente edición se terminó
de imprimir en el mes de diciembre de 2014, en los talleres de
Litho Arte, C. A., y su tiraje fue de 250 ejemplares.
San Cristóbal - Venezuela