

DERECHO Y TECNOLOGÍA

UNIVERSIDAD CATOLICA
DEL TACHIRA

2016

Vicerrectorado Académico
Decanato de Investigación y Postgrado

Número 2/2016 Edición Digital
Depósito Legal en línea: ppi201602TA4734
ISSN en Línea: (en trámite)

Edición Ordinaria 17/2016
Enero - Diciembre 2016
Depósito Legal: p.p 200202TA1209
ISSN: 1317-9306



Universidad Católica del Táchira
San Cristóbal - 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

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 SUNE (Universidad Complutense de Madrid); José Luis BARZALLO (Universidad Andina Simón Bolívar de Ecuador); Gustavo Adolfo AMONI REVERÓN (Universidad Central de Venezuela).

Diseño Gráfico

Nina Gabriela Vásquez

Montaje

Edy Marleni Lozano

Identificación Legal

Depósito Legal: p.p. 200202TA1209
ISSN: 1317-9306
Deposito Legal en Línea: ppi 201602TA4734
ISSN: Está en trámite
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 2/2016 Edición Digital - Edición Ordinaria 17/2016

La edición impresa de la Revista Derecho y Tecnología llega hasta la N° 15 año 2014, por falta de papel. La edición correspondiente al 2016 es en digital y por disposiciones de la Biblioteca Nacional y su departamento de Depósito Legal la numeración en la versión digital es la N° 2, para efectos de la continuidad de la edición ordinaria es la N° 17.

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
mrco@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.



ÍNDICE

Artículos

Sacha Rohán FERNÁNDEZ CABRERA: Responsabilidad de los correos electrónicos en el trabajo	9
Gustavo Adolfo AMONI REVERÓN: La audiencia telemática de extradición. Análisis del auto número 74/2016 de la Sala de Casación Penal del Tribunal Supremo de Justicia venezolano	49
Alejandra de los A. LEÓN PARADA: Valor probatorio de los mensajes de datos y firmas electrónicas en la Sala Civil del Tribunal Supremo de Justicia venezolano	81
Desirée J. RÍOS M.: Visión social de la prueba. Especial referencia a los medios electrónicos	97
Belinda PAZ CALZADILLA: El uso de las nuevas tecnologías en el procedimiento contencioso administrativo en Venezuela ..	125
Mariana del V. BUITRAGO RODRÍGUEZ: Domicilio fiscal electrónico obligatorio para la notificación de comunicaciones o actos administrativos emanadas de la Administración Tributaria venezolana	153

Conferencias

XX Congreso Iberoamericano de Derecho e Informática. Federación Iberoamericana de Asociaciones de Derecho e Informática. Salamanca, octubre, 2016

Jefferson Stewart ESPINOSA VERA: Derechos humanos en la protección ética de los menores en las redes sociales. Caso Colombia y Perú	173
Patricia REYES OLMEDO: Regulación de la protección de datos personales en Chile a la luz de los estándares internacionales. Deficiencias y Desafíos	187

Federico BUENO DE MATA: Diligencias de investigación tecnológicas para la obtención y aportación de mensajes de WhatsApp, Snapchat o Telegram	201
José Heriberto GARCIA PEÑA: Nanotecnología y Derecho: una aproximación al tema desde México	215

Legislación

Venezuela

Resolución N° 2016-001 de fecha 12 de diciembre de 2016, sobre Participación Telemática de los sujetos procesales en las Audiencias de la Sala de Casación Penal	231
--	-----

Jurisprudencia

Gustavo Adolfo AMONI REVERÓN: Recopilación de sentencias del Tribunal Supremo de Justicia relacionadas con el uso y la valoración jurídica de las Tecnologías de la Información durante el 2016	249
Índice acumulado	255

DOCTRINA

Privacidad de los correos electrónicos en el trabajo

Sacha Rohán Fernández Cabrera*

SUMARIO: I. Introducción. II. Generalidades. III. Marco regulatorio en Venezuela. IV. Alguna jurisprudencia y legislación en el mundo. V. Empleados públicos y privados. VI. El control de los trabajadores sobre sus correos electrónicos, posibilidades y límites de los patronos. VII. Valor probatorio de estos correos electrónicos en juicio. VIII. Conclusiones.

Resumen

En la mayoría de los trabajos tanto públicos como privados se le suministra al trabajador y empleado un correo electrónico laboral para ser utilizado, siendo que actualmente existen pocos países que tengan algún tipo de regulación específica sobre el uso, límites y responsabilidades en el empleo del mismo por parte de estos, así como tampoco a quién pertenece este y cuáles son los derechos y límites tanto del patrono o empleador en relación a la posibilidad de control, revisión, supervisión del mismo, también queda la duda sobre a quién pertenece el contenido de la información allí transmitida.

Palabras clave: Correo electrónico. Derecho a la privacidad. Derecho a la inviolabilidad de la correspondencia. Derecho a la libertad de empresa.

Abstract

In the majority of public and private employments a business e-mail address is supplied to the worker. Nevertheless, few countries are currently imposing regulations

Recibido: 20/1/2017 • Aceptado: 5/2/2017

* Universidad Central de Venezuela, *Facultad de Ciencias Jurídicas y Políticas, Escuela de Derecho*, abogado (14/366). *Doctor en Ciencias, Mención Derecho. Especializaciones en Derecho Procesal y Derecho Internacional Económico y de la Integración*; Ex Auxiliar de Investigación Docente, Ex Profesor contratado de Derecho Administrativo e Introducción al Derecho, profesor de Derecho de Obligaciones (pregrado); Ex Profesor en la Especialización de Derechos Humanos (postgrado). Universidad Alejandro de Humboldt, *Facultad de Ciencias Económica y Sociales*, Ex Profesor de Sistemas de Cobros y Pagos Internacionales. Instituto Venezolano de Derecho Procesal, Miembro y Bibliotecario Suplente. Autor de diversos estudios en revistas especializadas. Conferencista en diferentes eventos. Tribunal Supremo de Justicia, Abogado Auxiliar II. sfernandez_edu@yahoo.com.

on the use, limitations and responsibilities of the assigned e-mail address. It is not clear who owns it and what the rights and limits are for both the employee and employer in the context of control, revision and supervision. In addition, there is still doubt about who owns the content of the information transmitted by that mean.

Keywords: Email. Right to privacy. Right to privacy of correspondence. Right to Free Enterprise.

I. Introducción

La mayoría de las constituciones del mundo establecen el derecho a la privacidad, junto con la inviolabilidad de la correspondencia y demás formas de comunicación. Del mismo modo no se debe olvidar que algunos autores establecen diferencias entre privacidad y la intimidad. Para Cabrera, el artículo 60 constitucional separa ambos conceptos. Asimismo, el artículo 197 del Código Orgánico Procesal Penal acoge el criterio de que la intimidad es diferente a la vida privada¹.

Así, dentro de las actividades humanas, no hay duda de que el correo electrónico sirve como herramienta personal y de trabajo que es utilizada diariamente por millones de personas que lo utilizan para un sinnúmero de actividades diarias, que va desde la comunicación personal hasta el intercambio de mensajes y documentos laborales.

Sin embargo, no es lo mismo cuando se usa para fines personales que cuando se utiliza ligada a la actividad laboral, ya que en la segunda suele existir interés por parte de los empleadores de que en su uso se cumpla con los propósitos de la empresa; por ello es que establecen a veces la prohibición del uso de Internet o el bloqueo de algunos sitios de Internet, algunas redes sociales y los correos electrónicos, como una práctica común, que busca asegurar la productividad.

De esta manera, al tratar de controlar la información que circula dentro de las empresas y organizaciones se pueden sobrepasar los límites entre este interés y la privacidad del trabajador.

Aunque el trabajador y empleado pudiese estar utilizando los recursos y plataformas de la empresa u organismo en el horario de trabajo y fuera de él, ello no significa que toda la información que comunique o reciba electrónicamente pueda ser revisada por sus empleadores.

Por ello, su uso puede presentar una serie de interrogantes tanto para trabajadores como para patronos en cuanto a si las empresas y organismos públicos pueden limitar su acceso; o si tiene acceso el empleador o patrono a la correspondencia de un empleado o trabajador; o qué pasa si se accede al correo

¹ Jesús E. CABRERA: *La prueba ilegítima por inconstitucional*. Ediciones Homero. Caracas. 2013. p. 530.

electrónico a través de los recursos proporcionados por la empresa u organismo; así como si los hechos son iguales con los empleados del sector público y privado; también hasta qué punto el trabajador tiene control sobre su correo electrónico.

Finalmente nos podríamos preguntar, si el empleo de la internet (del correo personal) toca o integra la esfera de los derechos humanos del trabajador, máxime cuando la Organización Internacional del Trabajo, OIT ha reconocido la validez del trabajo mediante el empleo de esta herramienta, bien sea desde la empresa, del hogar o desde otras localidades.

II. Generalidades

Es lógico que los empleadores o patronos quieran asegurarse que sus empleados y trabajadores hagan bien su trabajo, pero en el lado contrario, los empleados no quieren que alguien los esté vigilando en cada momento de su vida mientras están en el sitio de trabajo, lo cual refleja el conflicto que existe en cuanto al monitoreo en el trabajo.

De este modo, es innegable que las nuevas tecnologías permiten que se pueda monitorear muchos aspectos del trabajo de los empleados y trabajadores, incluyendo comunicaciones telefónicas, uso de computadoras, Internet y buzones de voz, entre otros, siendo que este tipo de actividad prácticamente carece de toda regulación en nuestro país y muchas partes del mundo, aunque existe la Ley Especial contra los Delitos Informáticos, publicada en la Gaceta Oficial N° 37.313 del 30 de octubre de 2001. Por eso, se debe observar si la política de la compañía dice algo al respecto sobre el poder o no vigilar o monitorear la información del trabajador y empleado, por lo que algunos autores dicen que sí se puede y otros que no, haya o no regulación.

Tanto es así, que en Estados Unidos de Norteamérica (EE.UU.), existe una compañía que ofrece servicios de tecnología que proporciona información sobre el comportamiento de un empleado de las “huellas” digitales que deja todos los días en el trabajo, pudiendo analizar datos electrónicos para así generar un patrón de conducta de un trabajador (patrones de palabras, cambios en el lenguaje y estilo y los patrones de comunicación entre individuos) que después el empleador puede utilizar para evaluar el desempeño y conducta del mismo. Por otra parte, se encuentra también la Ley Patriota o *Patriot Act*, que permite por razones de seguridad interceptar todo tipo de mensaje y comunicación, incluso sin orden judicial.

En EEUU, la mayoría de los empleadores monitorean a sus empleados, debido en parte a que están preocupados por las posibles demandas de las que puedan ser objeto y otros aspectos legales, en razón de que la evidencia o prueba electrónica está tomando un papel cada vez más protagónico en demandas e investigaciones de agencias gubernamentales. Debido a ello, los empleadores monitorean las páginas de Internet que visitan sus empleados con el fin de evitar actividades inapropiadas y utilizan programas para bloquear conexiones

a sitios web que son considerados inadecuados, para de esa manera evitar que se visiten sitios para adultos con contenido sexual, que no visiten sitios donde puedan jugar, socializar, hacer compras, participar en subastas o leer blogs o sitios web de deportes, monitorean el contenido, las pulsaciones de teclado y el tiempo que pasa alguien en el teclado; además de bloquear ciertos sitios también monitorean blogs y lo que se está escribiendo sobre la compañía; así como los sitios de redes sociales, por lo que esta actividad incluye también que se monitoree el correo electrónico, incluso con tecnología que lo hace de forma automática, siendo que se han despedido a empleados debido al uso inapropiado del correo electrónico.

Aunado a lo anterior, las compañías utilizan el video como método de vigilancia para hacerle frente al robo, la violencia, el sabotaje y el desempeño de los empleados en el trabajo, siendo que la mayoría de los empleadores notifican a sus empleados sobre el monitoreo por video en general y relacionado al desempeño de los empleados.

Igualmente, un gran número de empresas españolas, ante la falta de claridad jurídica respecto al uso del correo electrónico en el puesto de trabajo, llevan un control exhaustivo de la actividad de sus empleados, utilizando en la red *software* que son especializados en la monitorización del uso de internet o del *e-mail* por parte del trabajador.² De esta manera se emplean las “*cookies*” como el primer control de la privacidad de las empresas, que contienen datos e información de fidelidad de cada persona, siendo enviada al disco duro del ordenador, existiendo otras herramientas como VNC y Back Orifice, que permiten controlar otro equipo conectado a internet, al tratarse de programas que pueden observar el trabajo en la computadora de otra persona que se encuentre conectada a la red, además del correo electrónico, incluyendo los textos que se han escrito y los programas utilizados durante el horario laboral, utilizándose mucho el programa “*Espía Carnivore*”, que rastrea los correos electrónicos, así como también se utilizan herramientas conocidas como “*filtros de paquete*” el cual es un sistema desarrollado por el FBI que se usa solamente cuando hay aprobación judicial, requiriendo los mismos trámites y garantías que deben aplicarse para la protección de la intimidad debido a las intervenciones en las líneas telefónicas³.

Frente a lo anterior se debe tomar en cuenta que el derecho a la intimidad y a la privacidad en nuestro país está protegido constitucionalmente en los artículos 60 y 143 de la Constitución, además de ciertas normas legales específicas sobre la materia, entre ellas: 1) la Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos; 2) la Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado; 3) la

² ¡Atención! El Jefe lee tus mensajes de ICQ. <http://pontonet.netfirms.com/es/esin2004.htm>. [Consulta: 2016, septiembre 22].

³ Rosana FIERREZ: Control de la privacidad en Internet: desde las ‘cookies’ hasta Carnivore, (17-12-2000) <http://www.delitosinformaticos.com/noticias/97505704727635.shtml>. [Consulta: 2016, septiembre 22].

Ley de Mensaje de Datos y Firmas Electrónicas, 4) la Ley del Inforgobierno, junto con la demás legislación vinculada y relacionada con este derecho que se pueda aplicar al caso concreto.

De allí, que resulte importante analizar también el alcance de la garantía constitucional a la inviolabilidad de las comunicaciones, establecida en el artículo 48 de la Constitución y en la Ley sobre Protección a la Privacidad de las Comunicaciones, que tienen por objeto impedir cualquier forma de registro, interceptación o apoderamiento de comunicaciones personales o privadas, sin nuestro consentimiento u orden judicial previa de un tribunal competente.

Con el ordenamiento jurídico sobre el tema, en nuestro país y otras partes del mundo, se pretende cubrir toda forma de correspondencia, de comunicación espiritual y material entre dos o más individuos proyectado el uno hacia el otro u otros, por cualquier medio que esté dentro de las posibilidades técnicas del país y de la sociedad de que se trate. Por lo que la privacidad en una comunicación tiene este carácter cuando el emisor o remitente escoge singularizadamente a la o las personas que la han de recibir, siendo que bajo una interpretación extensiva, esta garantía constitucional se debe aplicar aún cuando el destinatario no sea determinado individualmente, pero sea determinable por otros medios.

Así, la singularización del destinatario de correo, permiten desestimar los argumentos que sostienen que el correo electrónico debería asimilarse más bien a una postal que a una carta contenida en sobre cerrado, toda vez que si bien los medios técnicos permiten efectivamente la intromisión al correo electrónico de las personas no cifrado y enviado, ello no aminora la responsabilidad de quien de esta forma viola la privacidad de las comunicaciones, lo contrario nos llevaría al absurdo de pensar que las comunicaciones telefónicas (que también son técnicamente posible de interferir o interceptar) no son privadas, cuestión que nadie se atrevería a sostener ni mucho menos defender.

Consideramos que la interpretación extensiva que debe darse a los derechos humanos, constitucionales y fundamentales, permite considerar que el correo electrónico está protegido constitucionalmente y por los tratados de derechos humanos, de manera tal que su registro, interceptación o apoderamiento de su contenido, son ilícitos constitucionales y constituye una flagrante violación de los derechos humanos, salvo las excepciones y condiciones establecidas en la ley en tal sentido, pudiendo los afectados incluso recurrir a los organismos del sistema internacional o interamericano de protección de dichos derechos, solicitar las indemnizaciones correspondientes y ejercer acciones penales pertinentes.

Lo anterior es importante si consideramos que la intimidad y la privacidad son unas de las principales garantías que protegen al individuo frente a intromisiones ilegítimas del Estado e incluso de otros particulares. El uso cada vez más extensivo y popular, entre toda la población de las nuevas tecnologías trae consigo también el respeto de la intimidad en cualquier ambiente social, incluyendo el lugar de trabajo, donde solemos pasar la mayor parte activa del día.

De allí que no pueda existir un ejercicio indiscriminado de las facultades de control del empresario, en los ambientes de trabajo donde el uso de herramientas informáticas es fundamental para la prestación de los servicios, ya que ello puede ocasionar importantes lesiones a las garantías constitucionales antes mencionadas y mucho menos a de ser avalado por los tribunales y la legislación. En tal sentido, sería un abuso el control de la correspondencia electrónica de los trabajadores por parte de su empleador.

Puede pensarse que un empleador regule y controle legítimamente el uso que hagan del correo electrónico sus dependientes, pero en ningún caso tener acceso a la correspondencia electrónica privada enviada y recibida por el trabajador, lo cual estaría fundamentado no sólo por las normas constitucionales que amparan las comunicaciones privadas sino que también por los tipos penales que establecen los delitos de interceptación, interferencia e interrupción de servicios de telecomunicaciones contenidas en las leyes antes mencionadas y otras que se indicarán más adelante, por cuanto, el correo electrónico es una herramienta que se sustenta en un servicio complementario de telecomunicaciones junto con otras herramientas de trabajo que también son suministradas por el empleador para el desarrollo de las labores encomendadas, como el teléfono, por lo que su uso no se puede ver limitado y menos aún intervenido so pretexto del ejercicio de las facultades que emanan del poder de dirección del empleador.

El empleador debe contar con los medios necesarios para tener herramientas suficientes para prevenir y limitar los excesos y abusos que en la utilización de estos medios de trabajo y comunicación se puedan cometer por parte del trabajador, pero para ello no son necesarias ni modificaciones legales ni abusos soterrados de garantías constitucionales, tan sólo bastaría con implementar reglamentos internos adecuados dentro de las empresas y servicios públicos, o establecerse en las convenciones colectivas, en las que se contengan claramente las reglas de uso de los mismos que sean claras y transparentes para todas las partes involucradas, antes de que se produzca cualquier lesión a cualquiera de ellas, mucho mejor si tal regulación se realiza a través una legislación específica que toque el tema. En definitiva esto tendría que ver con la concertación empleador-trabajador para regular la materia, donde tal vez la actuación sindical y las llamadas comisiones tripartitas podrían también participar para regular la materia.

III. Marco regulatorio en Venezuela

En Venezuela, las instituciones públicas y privadas, como en el resto del mundo también utilizan las Tecnologías de Información y Comunicación, un ejemplo del reconocimiento de esto es la sentencia de la Sala Constitucional del Tribunal Supremo de Justicia N° 523 del 09 de abril de 2001, con respecto a la acción de amparo vía correo electrónico, señalando como un hecho notorio la existencia de Internet como medio novedoso de transmisión electrónica de

comunicación, lo cual además de esta regulado en el Decreto Ley N° 1204 sobre Mensajes de Datos y Firmas Electrónicas, publicado en G.O. N°- 37.148 del 28 de febrero de 2001, dando valor probatorio a dichas transmisiones.

Posteriormente la Sala Constitucional, en sentencia N° 982 del 06 de junio de 2001, se refirió al sitio *web* oficial del Tribunal Supremo de Justicia, como medio auxiliar de divulgación de su actividad judicial, así como también que constituyen mensajes de datos las cuentas, señalándola como *“información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio”*, luego en el fallo N° 1336 del 03 de agosto de 2001, la Sala Constitucional y la decisión N° 2031 del 19 de agosto de 2002, reitera estos criterios.

Ya en cuanto a lo que se refiere a la normativa existente, nos encontramos con el Decreto Ley N° 825 del 10 de mayo de 2000, publicado en la Gaceta Oficial N° 36.955 del 22 de mayo de 2000, por medio del cual se decretó el acceso y el uso de Internet como política prioritaria para el desarrollo cultural, económico, social y político de la República Bolivariana de Venezuela, por lo que los órganos de la Administración Pública Nacional deben emplearla para facilitar la tramitación de asuntos, usando Internet para el intercambio de información.

Luego está el Decreto Ley N° 1204 sobre Mensajes de Datos y Firmas Electrónicas del 28 de febrero de 2001, que establece en su artículo 5: *“Los Mensajes de Datos estarán sometidos a las disposiciones constitucionales y legales que garantizan los derechos a la privacidad de las comunicaciones y de acceso a la información personal”*. Esta ley siguió la política de Gobierno, tal como se estableció en la Ley que autoriza al Presidente de la República para dictar Decretos con Fuerza de Ley en las materias que se delegan (Ley Habilitante) del 2000, publicada en la Gaceta Oficial N° 37.077 del 14 de noviembre de 2000, que delegó la posibilidad de *“Dictar medidas que regulen la actividad informática, a fin de otorgar seguridad jurídica para la expansión y desarrollo de las comunicaciones electrónicas, especialmente dirigidas al uso de la red mundial de comunicaciones”*.

Esta ley mediante Decreto 3.335, contenido del Reglamento parcial de la Ley sobre Mensajes de Datos y Firmas Electrónicas, publicada en la Gaceta Oficial 38.086 del 12 de diciembre de 2004, establece lo relativo a la acreditación de los proveedores de servicios de certificación nacionales y extranjeros, su supervisión, el registro de los auditores, así como de lo relativo a los certificados electrónicos de las firmas electrónicas, junto con los estándares, planes y procedimientos de seguridad que deben ser suministrados por estos proveedores.

También se encuentra la Ley Sobre Delitos Informáticos del 30 de octubre de 2001, publicada en la Gaceta Oficial N° 37.313 del 30 de octubre de 2001, contempla en sus artículos 6, 13, 14, 20, 21 y 22, los delitos contra la privacidad de las personas y de las comunicaciones, referentes a la violación de la privacidad de data o información personal y la propiedad de la misma; violación de la

privacidad de las comunicaciones y revelación indebida de data o información personal, las cuales se deben vincular con las disposiciones contenidas en los artículos 186 al 191 del Código Penal Venezolano, en lo que se refiere al Título II, Capítulo V “*De los Delitos contra la Inviolabilidad del Secreto*”, en los cuales se contemplan penas de multas, arresto y prisión, para quienes estén subsumidos en los supuesto allí previstos, las cuales serían plenamente aplicables a los correos electrónicos.

Se encuentra igualmente la Ley de Infogobierno, publicada en la Gaceta Oficial N° 40.217 del 17 de octubre de 2013, que 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, teniendo como uno de sus aspectos importantes la seguridad de la información como resultado 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, teniendo especial relevancia los artículos 25 y 77 relativos al respecto al uso de las tecnologías de información por el Poder Público y el Poder Popular que debe comprender la protección del honor, vida privada, intimidad, propia imagen, confidencialidad y reputación de las personas; aunque sujeto a las limitaciones de la ley; así como que se tiene la obligación de proteger la información que obtiene por intermedio de los servicios que se prestan a través de las tecnologías de información y la que repose en sus archivos o registros electrónicos.

También está la Ley de Simplificación de Trámites Administrativos, publicada en la Gaceta Oficial Extraordinario N° 5.393 del 22 de octubre de 1999, cuya finalidad es racionalizar y optimizar las tramitaciones que realizan las personas ante la Administración Pública a los fines de mejorar su eficacia, eficiencia, pertinencia, utilidad, para así lograr una mayor celeridad y funcionalidad en las mismas, reducir los gastos operativos, obtener ahorros presupuestarios, cubrir insuficiencias de carácter fiscal y mejorar las relaciones de la Administración Pública con las personas.

Por su parte la Ley Orgánica Procesal del Trabajo, publicado en la Gaceta Oficial N° 37.504 del 13 de agosto de 2002, en su artículo 126 permite que el tribunal, a solicitud de parte o de oficio, practique la notificación del demandado por los medios electrónicos de los cuales disponga, siempre y cuando éstos le pertenezcan, siendo que para la certificación de la notificación, se procederá de conformidad con lo establecido en la Ley sobre Mensajes de Datos y Firmas

Electrónicas, atendiendo siempre a los principios de inmediatez, brevedad y celeridad, dejando constancia en el expediente, que efectivamente se materializó la notificación del demandado. Acá y en otras leyes similares, se debe entender que la citación y notificación se realizar por un funcionario público en actividades laborales con un correo institucional o laboral, para ejercer su trabajo.

Igualmente se debe ver lo establecido en el artículo 16, literal “d”, del Reglamento de la Ley Orgánica del Trabajo, publicado en la Gaceta Oficial Extraordinario N° 5.292 del 25 de enero de 1999, que establece las obligaciones fundamentales del patrono con el trabajador con el que tiene una relación individual de trabajo, debiendo respetar su dignidad, privacidad, intimidad y libertad de conciencia, todo lo cual se extiende al derecho a la privacidad de las comunicaciones que el trabajador emita o reciba en el curso de la prestación de sus servicios al patrono, en razón del principio de progresividad e interpretación extensiva de los derechos humanos. En cuanto a los deberes del trabajador, el artículo 17, literal a *eiusdem*, se encuentran el prestar el servicio en las condiciones y términos pactados o que se desprendieren de la naturaleza de la actividad productiva y observar las órdenes e instrucciones que, sobre el modo de ejecución del trabajo, dictare el patrono, lo cual está en concordancia con lo previsto en el artículo 18 del Reglamento mencionado, que establece el derecho del trabajador a no acatar instrucciones que comprometan manifiestamente su vida, salud o la preservación de la empresa o sean incompatibles con su dignidad, sin perjuicio del deber de obediencia, con lo que si recibe instrucciones respecto al uso del correo electrónico y una advertencia de que puede estar monitoreado, el trabajador debe tomar las previsiones correspondientes. No obstante, lo anterior, el trabajador tiene la posibilidad de ejercer la acción de amparo prevista en el artículo 14 *eiusdem*, en caso de ser discriminado por su negativa justificada a cumplir las órdenes patronales, pudiendo retirarse justificadamente si el patrono persistiere en dichas órdenes a pesar de la disconformidad expresada por el trabajador.

Del mismo modo la Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos, publicada en la Gaceta Oficial N° 39.610 del 7 de febrero de 2011, en su artículo 31 numeral 3, señala que el acto mediante el cual se dé inicio al procedimiento se procederá a notificar al presunto infractor, por correspondencia postal, efectuada mediante correo público o privado, por sistemas de comunicación telegráficos, facsímiles, electrónicos y similares siempre que se deje constancia en el expediente de su recepción; siendo que cuando se practique mediante sistemas facsímiles o electrónicos, la Comisión Nacional de Telecomunicaciones, convendrá con el presunto infractor la definición de un lugar o dirección facsímil o electrónica.

En tónica similar a la ley anterior esta la Ley Orgánica de Telecomunicaciones, también publicada en la Gaceta Oficial N° 39.610 del 7 de febrero de 2011, que indica en su artículo 26 numeral 5, que la solicitud de habilitaciones administrativas ante la Comisión Nacional de Telecomunicaciones,

se puede hacer ante este ente e indicar una dirección de correo electrónico en la que se podrán hacer las notificaciones correspondientes.

Por su parte la Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado; publicada en la Gaceta Oficial N° 39.945 del 15 de junio de 2012, establece que esta ley tiene por objeto establecer las bases y principios que regirá el acceso e intercambio electrónico de datos, información y documentos entre los órganos y entes del Estado y todo el sector público y sector privado bajo el control público, con el fin de garantizar la implementación de un estándar de interoperabilidad como una herramienta que garantiza el desarrollo de servicios públicos integrados, complementarios 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, ante lo cual están obligados a permitir entre sí, el acceso, intercambio y reutilización, por medios electrónicos, de los datos de autoría, información y documentos de acceso público que posean, en los términos y condiciones de esta ley.

Relevante también es lo establecido en la Ley sobre Protección a la Privacidad de las Comunicaciones, publicada en la Gaceta Oficial N° 34.863 del 16 de diciembre de 1991, que busca proteger la privacidad, confidencialidad, inviolabilidad y secreto de las comunicaciones que se produzcan entre dos o más personas, cualquiera sea el medio que se utilice, siendo que el que arbitraria, clandestina o fraudulentamente grave o se imponga de una comunicación entre personas, la interrumpa o impida, será castigado con prisión, de allí que se requiera que las autoridades de policía, como auxiliares de la administración de justicia, solicitarán razonadamente al Juez de Primera Instancia en lo Penal, que tenga competencia territorial en el lugar donde se realizaría la intervención, la correspondiente autorización, con expreso señalamiento del tiempo de duración, que no excederá de sesenta (60) días, pudiendo acordarse prórrogas sucesivas., siendo que excepcionalmente en casos de extrema necesidad y urgencia, los órganos de policía podrán actuar sin autorización judicial previa, notificando de inmediato al Juez de Primera Instancia en lo Penal, sobre esta actuación, en acta motivada que se acompañará a las notificaciones y a los efectos de la autorización que corresponda, en un lapso no mayor de ocho horas.

De hecho en Venezuela el empleo de los medios electrónicos por parte de la Administración está regulado, entre otros cuerpos normativos, en la Ley Orgánica de Administración Pública, publicada en Gaceta Oficial Extraordinaria N° 6.147 del 17 de noviembre de 2014, en sus artículos 11 y 152, hace referencia a la implementación los mecanismos electrónicos, informáticos y la tecnología por parte de los órganos y entes de la Administración Pública, para su organización, funcionamiento y relación con las personas, estableciendo y manteniendo una página en Internet, para el cumplimiento de sus fines, siendo que los documentos

reproducidos por dichos medios gozarán de la misma validez y eficacia del documento original, siempre que se cumplan los requisitos exigidos por ley y se garantice la autenticidad, integridad e inalterabilidad de la información.

En este sentido y acorde con lo anterior, el artículo 125 del Código Orgánico Tributario, publicado en la Gaceta Oficial N° 37.305 del 17 de octubre de 2001, también refiere y autoriza la implementación de los medios electrónicos por parte de la Administración Pública.

Asimismo, el numeral 8, del artículo 38 de la Ley Orgánica de la Jurisdicción Contencioso Administrativa, publicada en la Gaceta Oficial N° 39.451 del 22 de junio de 2010, autoriza el uso de notificaciones y citaciones electrónicas señalando que: *“el Tribunal podrá practicar las citaciones y notificaciones por medios electrónicos”*.

Finalmente, en cuanto a los cuerpos normativos, se encuentra el numeral 3 del artículo 91 de la Ley Orgánica del Tribunal Supremo de Justicia, publicado en la Gaceta Oficial N° 39.522 del 1 de octubre de 2010, consagra que de no ser posible la notificación personal, ésta podrá practicarse, entre otros medios, por *“...boleta que sea enviada a través de sistemas de comunicación telegráficos, facsimilares, electrónicos y similares, en cuyo caso el Secretario o Secretaria dejará constancia en el expediente de haberla practicado. A tal efecto las partes indicarán su dirección de correo electrónico o número de fax cuando se incorporen al proceso. Al momento de librarse la boleta se ordenará su publicación en el portal electrónico del Tribunal Supremo de Justicia...”*, debiéndose esto vincular con el artículo 92 *eiusdem*.

En tal sentido, el uso del correo electrónico por parte de la Administración Pública y de los órganos judiciales también se puede apreciar en la jurisprudencia de la Sala Político Administrativa, como se pueden apreciar en las sentencias N° 1.011 del 8 de julio de 2009, la N° 1.437 del 8 de octubre de 2009, la N° 100 del 3 de febrero de 2010, la N° 1.358 del 15 de octubre de 2014 y la N° 403 del 15 de abril de 2015; así como las decisiones del Juzgado de Sustanciación de la Sala Político Administrativa N° 383 del 1° de diciembre de 2015, N° 108 del 31 de marzo de 2016 y N° 133 del 21 de abril de 2016, entre otras.

IV. Alguna jurisprudencia y legislación en el mundo

Ya indicamos que algunos patronos y empleadores efectúan monitoreo de las computadoras u ordenadores que se utilizan en el trabajo, para de esa manera tener una forma de conocer la forma de trabajar de los empleados, utilizando para ello varios tipos de monitoreo de computadoras como el uso de programas que les permiten ver lo que está en su pantalla o los datos que están archivados en el aparato o en el disco duro, el uso de Internet y el correo electrónico.

Así las personas cuyos trabajos requieren el procesamiento intenso de palabras o datos podrían estar sujetas a monitoreo de pulsaciones de teclado, a

través de sistemas que informan al patrono sobre el número de pulsaciones de teclado por hora que realiza el empleado; saber si las pulsaciones de teclado están por debajo o encima del número estándar requerido; ver si las pulsaciones de teclado está ligado a problemas de salud como discapacidades ocasionadas por el estrés y problemas físicos como el síndrome del túnel carpiano; o permitir conocer la cantidad de tiempo que un empleado permanece alejado de la computadora o sin que la computadora esté en uso.

En este sentido es importante que tanto empleador como empleados, desde un primer momento conozcan las condiciones, regulación y normativas tanto públicas como privadas de la empresa que existen sobre el tema. Por ello, el empresario debe informar que el correo electrónico de la empresa se va a supervisar, monitorizar y revisar, así como prohibir el uso personal de ese correo electrónico del trabajo, de allí que la sentencia del Tribunal Europeo de Derechos Humanos también advierte de la necesidad de definir de manera más clara qué clase de información puede recolectar un empresario⁴.

No obstante, estimamos que se debe tomar en cuenta que las llamadas redes sociales son múltiples, ya no es solamente Internet, el Facebook, Instagram, etc., que se han convertido en herramientas que el trabajador también puede emplear para desempeñar su actividad. En este sentido, también pudiera ocurrir que el trabajador deba revisar la web en ciertos horarios para enterarse de la marcha de sus asuntos familiares, esto se podría concertar empleador-trabajador.

Existen algunos fallos en España que ya se habían pronunciado en la misma dirección del Tribunal Europeo de Derechos Humanos, indicándose que una empresa puede auditar, previo aviso, los instrumentos informáticos que utiliza un trabajador. En un primer momento, el Tribunal Supremo español en su sentencia de 26 de septiembre de 2007, frente a la duda de si la empresa podía acceder al correo electrónico del trabajador estableció que

en síntesis prevé la posibilidad de que el empresario pueda acceder al control del ordenador, del correo electrónico y los accesos a Internet de los trabajadores, siempre que la empresa de buena fe haya establecido previamente las reglas de uso de esos medios con aplicación de prohibiciones absolutas o parciales e informado de que va existir un control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos.

Luego en este mismo caso, el mismo Tribunal Supremo de este país en sentencia de octubre de 2007, STS 6128/2007 – ECLI:ES:TS:2007:6128⁵, señala que la empresa podía establecer una vigilancia de las comunicaciones de sus

4 Esta es la sentencia 12 de enero de 2016, por el Tribunal de Derechos Humanos de Estrasburgo (Francia), la cual comentaremos más adelante.

5 <http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=326542&links=&optimize=20071018&publicinterface=true>. [Consulta: 2016, Septiembre 22].

empleados, pero para ello, debía informar a los trabajadores de que iba a “existir un control” de los medios para comprobar que se hacía un uso correcto de los mismos. Posteriormente, el Tribunal Supremo da un paso más en su sentencia de 6 de octubre de 2011 en la que estableció que *“si la empresa prohíbe totalmente el uso de estas tecnologías con fines particulares, ya sea dentro o fuera del horario laboral, no se puede entender que el Derecho Fundamental a la Intimidad o al Secreto de las comunicaciones opera en el uso de estos equipos”*.

Después en otros fallos vinculados con el tema, el Tribunal Constitucional español en la sentencia STC 241/2012 respalda la tesis de que ante el acceso a un programa de chat instalado por los propios trabajadores en un equipo multiusuario y sin clave de acceso, no cabe alegar expectativa en privacidad, sobre todo si previamente la empresa ha prohibido la instalación de este tipo de programas y en el fallo 170/2013 del 7 de octubre, ratifica el criterio de que el despido disciplinario de un trabajador que trabajaba en una empresa del sector químico, que estaba pasando información a la competencia mediante el correo electrónico profesional y, en base a ello, se le despidió disciplinariamente, fue conforme a derecho, al entender que como el convenio colectivo de las empresas del sector químico establece que los medios informáticos son medios profesionales, debe entenderse prohibido el uso personal de los mismos.

Este fallo del 7 de octubre de 2013, en sentencia 170/2013⁶, el Tribunal Constitucional, amplió esta medida y estableció el alcance de la privacidad de los correos electrónicos en el entorno laboral, señalando que no hacía falta aviso previo si el convenio colectivo así lo disponía, ya que de esa manera se sobreentendía que el trabajador tenía conocimiento al respecto, en ese caso, el convenio colectivo de la industria química tipificaba como falta leve *“la utilización de los medios informáticos propiedad de la empresa (correo electrónico, intranet, internet, etc.) para fines distintos de los relacionados con el contenido de la prestación laboral, con la salvedad de lo dispuesto en el artículo 79.2”*, aunado al hecho de que el correo institucional o laboral lleva implícita la posibilidad de control y acceso a los emails, y el trabajador no puede albergar una *“expectativa fundada y razonable de privacidad”* en lo relativo a los asuntos profesionales, el acceso a los correos es proporcional a la situación de sospecha que vivía la empresa y que el registro del correo corporativo del trabajador es una medida *“justificada”*, *“idónea”* para verificar si revelaba datos de reserva vigilada a terceros y *“necesaria”* para justificar el despido disciplinario, además de *“ponderada y equilibrada”* pues ninguno de los mensajes objeto de la controversia reflejaba aspectos de la vida personal y familiar del trabajador. Ese artículo advierte del carácter profesional del correo

6 <http://hj.tribunalconstitucional.es/docs/BOE/BOE-A-2013-11681.pdf>. [Consulta: 2016, septiembre 22].

electrónico, que debe utilizarse entre trabajadores o con la dirección, y que para usarse con otros motivos necesitaba de un acuerdo previo con la dirección.

Este fallo se refiere a una “petición de amparo” interpuesta por un trabajador de una empresa de la industria química que había revelado a una empresa competidora información interna y confidencial sobre la primera, siendo que la empresa el tener sospechas sobre este realizó ante notario el examen del ordenador del trabajador y encontró mensajes de correo electrónico enviados a terceros relativos a la cosecha de los productos de su empresa durante dos años, procediendo a despedirlo por transgresión de la buena fe, siendo que el trabajador alegó que se había vulnerado el secreto de las comunicaciones, por cuanto por parte de la empresa no existía una política o instrucciones respecto del uso del correo electrónico, tal como se había establecido la sentencia del Tribunal Supremo de 26 de septiembre de 2007 antes mencionada⁷.

En el presente caso, aunque no se había definido una política de uso del correo electrónico, el convenio colectivo aplicable al trabajador claramente establecía una prohibición del uso del ordenador para fines personales, por lo que lo importante no es en realidad si existe o no una regulación interna específica en la empresa sobre el uso de los medios informáticos en la misma, sino si, por las vías que sea, el trabajador tiene una “*expectativa razonable de confidencialidad*” en la utilización de dichos medios, ya que en la medida en que el trabajador deba conocer el convenio colectivo aplicable a su situación, debería saber que el ordenador y el correo electrónico de la empresa sólo podían utilizarse para fines estrictamente relacionados con la actividad laboral, no para usos privados, sin que por tanto gocen dichas comunicaciones de la protección constitucional. Además, consideró el tribunal que el examen del correo electrónico que llevó a cabo la empresa se circunscribió a comunicaciones no personales, sino sobre hechos relativos a la actividad de la empresa en la que prestaba sus servicios, por lo que en modo alguno se vulneró su intimidad.

Por lo tanto, en España, si el convenio colectivo lo especifica, se podrá revisar los correos de los empleados sin aviso previo y, en caso contrario, deberá existir una advertencia.

Antes el 14 de noviembre de 2000, fecha en que se decidió por la Sala Social del Tribunal Superior de Justicia de Cataluña, el llamado caso *Deutsche*

⁷ En España el control empresarial de los medios informáticos de la empresa está fundamentado por la potestad de vigilancia del trabajador bajo el Estatuto de los Trabajadores, aunque dicha facultad de control no es absoluta, sino que debe pasar un triple filtro de idoneidad, necesidad y proporcionalidad. En este sentido, la sentencia del Tribunal Supremo de 2007, venía de indicar que, en la medida en que en la práctica existe en las empresas un uso tolerado de los medios informáticos, en especial el correo electrónico, para fines no estrictamente profesionales, los trabajadores tienen una expectativa de privacidad respecto a los mensajes recibidos y enviados por esta vía, siendo por ello, deber del empresario establecer los límites en cuanto al uso de dichas herramientas, debiendo definir si se permite o no un uso personal del correo electrónico de la empresa, a fin de que éstos puedan actuar conforme a la política de la empresa.

Bank en lo que fuera el primer juicio por intromisión en el correo electrónico de dicho país, se trató de un trabajador que fue despedido por hacer un uso incorrecto de su email al enviar y recibir una gran cantidad de chistes y otros mensajes personales por dicho medio, enterándose la empresa al acceder a su email, siendo que en juicio incluso aportaron algunos de estos impresos y se declaró el despido procedente por falta de lealtad laboral. No obstante, con posterioridad se han dictado otras sentencias en sentido contrario y obligaban a la empresa a readmitir al trabajador por haber vulnerado su intimidad y el secreto de sus comunicaciones. Por ello, es que el Tribunal Supremo en la sentencia mencionada del 2013, se pronunció en una sentencia de “unificación de doctrina” reconociendo el derecho a la intimidad del trabajador pero supeditándolo, en cierto modo, a las instrucciones y controles impuestos por la empresa, donde la empresa debe informar expresamente al trabajador de sus obligaciones en el uso del correo electrónico profesional y del eventual acceso a su contenido, por lo que siempre que se dé dicha información, la empresa podrá acceder sin más al email.

Sin embargo, esto es lo referente a la vía laboral, en cuanto a si el trabajador es o no correctamente despedido o la indemnización que debe percibir, pero lo relativo a lo penal que se puede derivar de estos asuntos, en el mismo *caso Deutsche Bank* el trabajador “correctamente” despedido según la vía social, denunció a sus antiguos jefes por vía penal por violación de la inviolabilidad de la correspondencia y el derecho fundamental a la intimidad, siendo que el Juzgado de Instrucción 2 de Barcelona, el 15 de mayo de 2001, absolvió a los directivos de Deutsche Bank Juan Cruz Alcalde, José Antonio Soler y Albert Faulin Berned de un delito continuado de descubrimiento y revelación de secretos al interceptar correos electrónicos personales del entonces empleado de la entidad bancaria Gregorio Giménez, siendo que se trataba de la primera denuncia en España por intromisión en el correo electrónico de un trabajador, este proceso inició luego de que el denunciante fuese despedido de la entidad bancaria, siendo los acusados Juan Cruz Alcalde y José Antonio Soler (directores de Recursos Humanos y de Relaciones Laborales), los que acordaron el despido del afectado en noviembre de 1999, hecho por el que el Sindicato de Empleados del Grupo Deutsche Bank les acusó de un delito contra la libertad sindical por el que se siguieron diligencias ante el Juzgado de Instrucción 21 de Barcelona, alegando que el despido no había sido sancionado en los 28 años en los que trabajó y los acusados decidieron interceptar su correo electrónico –según señalaba el escrito de acusación del trabajador-, con el fin de “obtener pruebas con las que sustentar un eventual despido disciplinario”.

Posteriormente mediante sentencia 2844/2014 de la Sala de lo Penal de Tribunal Supremo de 16 de junio de 2014, se volvió a cambiar en lo que respecta a las técnicas de monitorización y el acceso al correo electrónico profesional del empleado, creando dos líneas jurisprudenciales diferentes a la hora de valorar la licitud de una prueba.

La Sentencia de la Sala de lo Penal, indica que por existir suficiente material probatorio para condenar en este proceso, ante los argumentos dados por la Sentencia recurrida de la Audiencia Provincial

...el ordenador registrado era una herramienta propiedad de la empresa y facilitada por la empresa a don AAA exclusivamente para desarrollar su trabajo, por lo que entendemos que incluso en aquel supuesto en que pudiera utilizar el ordenador para emitir algún tipo de mensaje de carácter personal, entendemos que al utilizar precisamente un ordenador ajeno, de la empresa, y destinado exclusivamente para el trabajo a la empresa, estaba asumiendo -cediendo- la falta de confidencialidad -secreto- de las comunicaciones que pudiera tener el señor AAA utilizando tal terminal informático,

siendo que el Tribunal Supremo decide a través de un *obiter dicta* establecer su doctrina en esta materia.

Por lo tanto, de las sentencias de la Sala de lo Social del Tribunal Supremo y del Tribunal Constitucional indicadas anteriormente, se entiende que estas argumentaciones deben quedar delimitadas en el ámbito exclusivo de la jurisdicción social y no así en la penal, disponiendo que

a nuestro juicio, el texto constitucional es claro y tajante cuando afirma categóricamente que: «se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial». De allí que haya afirmando el Tribunal Supremo que «no contempla, por tanto, ninguna posibilidad ni supuesto, ni acerca de la titularidad de la herramienta comunicativa (ordenador, teléfono, etc. propiedad de tercero ajeno al comunicante), ni del carácter del tiempo en el que se utiliza (jornada laboral) ni, tan siquiera, de la naturaleza del cauce empleado (“correo corporativo”), para excepcionar la necesaria e imprescindible reserva jurisdiccional en la autorización de la injerencia,

y que tampoco una renuncia tácita a ese derecho puede convalidar la ausencia de intervención judicial.

De esta manera, la sentencia fija claramente que en el caso de los correos electrónicos sin abrir por el destinatario, rige la protección constitucional que otorga el artículo 18.3 de la Constitución española respecto al secreto de las comunicaciones, y para los que ya han sido abiertos por el destinatario y otros aspectos susceptibles de control como los datos del tráfico, historial de navegación Web o acceso al disco duro, rige la protección del artículo 18.1 *eiusdem* del derecho a la intimidad y del artículo 18.4 *ibidem* a la protección de datos personales, por lo que su control e intervención vendría amparada si se cumplen los requisitos fijados por las Sentencias del Supremo y Constitucional analizadas con anterioridad. Sin embargo, aunque el Tribunal Supremo fijó su doctrina para la válida aportación como prueba a un proceso penal de un correo electrónico, que fue abierto antes de que lo hiciera el destinatario del mismo, se

puede entender que no solamente afecta a los correos electrónicos, sino a cualquier sistema de mensajería instantánea y Chat que permita establecer una comunicación entre dos o más personas.

Por lo tanto en España, los tribunales han tenido la ocasión de pronunciarse frente al uso no autorizado de los recursos de Internet por el trabajador⁸, e igualmente sobre el uso del correo electrónico por los sindicatos⁹, así como el Tribunal Superior de Justicia de Cataluña estimó justificado el despido de dos trabajadores que durante dos meses intercambiaron correo electrónico considerado obsceno y despreciativo hacia sus subordinadas¹⁰, lo cual según ya hemos visto cobró relevancia cuando el *Deutsche Bank* despidió a un trabajador tras treinta años de servicios para la entidad, por utilización inapropiada del correo electrónico, aportando, como prueba en juicio, algunos de los e-mails enviados por el trabajador, siendo que declaró procedente el despido de quien, sin conocimiento ni autorización de la empresa, envió a través del correo electrónico mensajes ajenos a la prestación de servicios en horario laboral, prescindiendo del hecho que la empresa revisó el correo del trabajador para decidir la medida, sin mediar el consentimiento de éste¹¹. Estas sentencias han movido al Senado español a instar al Gobierno para que adopte medidas necesarias para que el correo electrónico e internet sean considerados instrumentos de comunicaciones e información entre los trabajadores, en especial con sus representantes¹².

En Estados Unidos de Norteamérica (EEUU), nos sorprende que no exista una adecuada protección legal para el uso de e-mail o correo electrónico por parte de los trabajadores, aunque se han planteado varios casos judiciales sobre despidos fundados en el uso inapropiado de la red o internet que han sentado precedentes en orden a salvaguardar la privacidad del trabajador, en tanto este disponga de una “*expectation of privacy*” o “*esperanza razonable de privacidad*” y no se encuentren comprometidos intereses públicos. La jurisprudencia ha estimado que una simple comunicación escrita al trabajador del empleador, indicando que su correo electrónico puede estar siendo controlado,

8 De tal suerte se ha estimado justificado el despido de quien, pese a la advertencia empresarial de sancionar las navegaciones irregulares en Internet, destina su jornada laboral a visitar sitios ajenos a los fines de la empresa y hace uso del computador para desarrollar actividades relacionadas con negocios propios. Tribunal Superior de Justicia de Madrid, Sala de lo Social, 16 de octubre de 1998.

9 La Audiencia Nacional falló a favor de la organización sindical en su querrela contra el Grupo BBVA, en la que reconocía el derecho del sindicato a “transmitir noticias de interés sindical a sus afiliados y a los trabajadores en general a través del correo electrónico con la mesura y normalidad inocua con la que se venía realizando”. Audiencia Nacional, Sala de lo Social, 6 de Febrero de 2001.

10 STSJ Cataluña, 5 de julio de 2000 (Ar. 3452).

11 STSJ Cataluña, 14 de noviembre de 2000 (Ar. 3444).

12 J. GARCÍA VIÑA: “Relaciones laborales e Internet”. *Revista de Trabajo y Seguridad Social (Estudios Financieros)*, N° 223. 2001, pp. 37 y ss.

rebaja las expectativas de intimidad y legitima la intromisión de éste en la correspondencia de sus empleados, lo cual ha sido objeto de duras críticas por la violación que conlleva de las libertades individuales, la falta de consideración hacia la dignidad del trabajador y las desventajas competitivas que origina para la actividad empresarial.

En Inglaterra, existe la *Regulation of Investigatory Powers Act 2000* que facultó al gobierno inglés para elaborar una regulación sobre la interceptación de las comunicaciones de los trabajadores, lo que llevó a la publicación de una ley que fue controvertida y que es la *Lawful Business Practice Regulations*, en la cual se consagró la regla general de no poder interceptar las comunicaciones sin consentimiento de estos; sin embargo, la regulación admite numerosos supuestos que legitimarían tal control empresarial, prescindiendo del consentimiento del trabajador, que van desde razones que abogan por la seguridad nacional hasta asegurar el buen funcionamiento del sistema informático de la empresa, incluso para comprobar el cumplimiento de normas de conducta en el seno de ésta. Con posterioridad, *the Information Commissioner*, autoridad de control para el tratamiento de datos personales, emitió un código de conducta, mediante el cual se procura mitigar los efectos de la regulación antedicha¹³.

En Chile, el tema aún no ha sido objeto de una regulación legislativa especial, aunque se introdujeron modificaciones en la Ley 19.759 del Código del Trabajo, innovando en la protección de los derechos fundamentales del trabajador al interior de la empresa, teniendo plena vigencia en el marco de las relaciones laborales.

Allí, la Dirección del Trabajo se refirió por primera vez al tema en el 2012/-Dictamen ORD. N° 260/19 de 24-01-2002. estableciendo las bases generales sobre la utilización y control de los correos electrónicos dentro de la empresa, señalando que, de acuerdo a las facultades que posee el empleador para administrar su empresa, puede regular “las condiciones, frecuencia y oportunidad de uso de los correos electrónicos”, pero nunca podrá tener acceso a la correspondencia electrónica privada recibida por los trabajadores, similar a lo que ocurre con las llamadas telefónicas privadas o a la existencia de espacios que se consideran privados dentro de la empresa, como cajones o casilleros personales de los trabajadores.

Por ello, ante la falta de esta normativa y en protección de los derechos humanos al interior de la empresa, la Dirección del Trabajo chilena, haciendo uso de sus facultades esbozó algunas consideraciones mediante dictamen 0260/0019 del 24 de enero del 2002, en el que asumió el tema relativo a las condiciones de uso de los correos electrónicos de la empresa por los trabajadores, y a las facultades que conciernen al empleador a su respecto. Este dictamen considera

¹³ Mark Jeffery: *¿Carta blanca para espiar a los trabajadores? Perspectivas inglesas sobre poder informático e intimidad* <http://www.uoc.es/web/esp/art/uoc/0109042/jeffery.html>. [Consulta: 2016, septiembre 22].

que aparecen dos valores constitucionales en conflicto como lo son la garantía constitucional de inviolabilidad de toda forma de comunicación privada y la facultad del empleador de organizar, dirigir y administrar su empresa, que emana de la garantía constitucional del derecho de propiedad¹⁴.

La Dirección del Trabajo considera situaciones análogas a las que tienen lugar con el uso del correo electrónico, como las llamadas telefónicas, en el cual el empleador no debe imponerse del contenido de las conversaciones, aún siendo los medios de su propiedad, lo cual se extiende a lookers, casilleros, gavetas de escritorio y otros espacios que considera una “proyección natural de la persona”, por lo que concluye que con “similar predicamento deben abordarse las situaciones a que dé lugar el uso del correo electrónico”. De allí, que la regulación formal del uso de los e-mail por el empleador, de regular, limitar o restringir el empleo de estos por los dependientes en el reglamento interno de la empresa, está sujeto al régimen de impugnación previsto en el Código del Trabajo, aunado a que la regulación de esta materia también puede tener lugar por vía del contrato individual de trabajo o el instrumento colectivo, pero en ambos casos, la regulación no puede significar limitar la garantía constitucional de inviolabilidad de la comunicación privada. De allí que considere que cualquier criterio regulador, manifestando que la recepción de correo electrónico reviste carácter privado y queda por ello protegido constitucionalmente, mas convencionalmente puede privarse de tal carácter, por ejemplo imponiendo al trabajador la práctica de remitir su correspondencia con copia al empleador o su representante. Por ello, en el dictamen dijo que

... de acuerdo a las facultades con que cuenta el empleador para administrar su empresa, puede regular las condiciones, frecuencia y oportunidad de uso de los correos electrónicos de la empresa, pero en ningún caso podrá tener acceso a la correspondencia electrónica privada enviada y recibida por los trabajadores.

Luego en otro dictamen, señaló que las partes pueden establecer normas, restricciones y formalidades para el uso de los correos electrónicos en el reglamento interno o en los respectivos contratos individuales de trabajo¹⁵.

Sobre la base de esto la Corte Suprema chilena³.- Corte Suprema de Justicia, Rol N° 2502-2012, fallo de 12 de mayo de 2012., se pronunció respecto a si es relevante la forma en cómo se ha accedido al contenido de los correos electrónicos, indicando que el valor protegido es la intimidad, que es manifestación de la esfera privada de los trabajadores, y por lo tanto resulta que cualquier tipo

¹⁴ El dictamen 0260/0019 del 24 de enero del 2002, de la Dirección del Trabajo se encuentra disponible en <http://www.dt.gob.cl/legislacion/1611/w3-article-63171.html>. [Consulta: 2016, septiembre 22].

¹⁵ El dictamen 1147/34 del 21 de marzo del 2005, de la Dirección del Trabajo se encuentra disponible en <http://www.dt.gob.cl/1601/w3-article-81104.html>. [Consulta: 2016, Septiembre 22].

de interceptación no autorizada de los correos electrónicos es ilícita y violatoria del mismo¹⁶.

Hay varias sentencias que han indicado que los correos electrónicos de los trabajadores son un tipo de comunicación privada, protegidos por la Constitución, por lo que se debe resguardar los derechos a la vida privada y a la inviolabilidad de las comunicaciones personales. De esta manera, es ilícito la interceptación de los correos electrónicos de los trabajadores por parte de los empleadores, sin autorización de los primeros, aun cuando las cuentas de correo sean otorgadas por la empresa. Así, se estima que los empleadores solo pueden regular las condiciones, frecuencia y oportunidad de su uso, en el reglamento interno, en los contratos individuales de trabajo, y a través de contratos colectivos, siendo que prevalecen así los derechos fundamentales de los trabajadores, por sobre los intereses del empleador.

Recientemente, mediante una sentencia publicada el martes 12 de enero de 2016, por el Tribunal de Derechos Humanos de Estrasburgo (Francia), dijo que estaba justificado que una empresa lea e inspeccione los correos electrónicos —privados o profesionales— de cualquier empleado, haciendo referencia a un caso ocurrido en Rumanía, en el que la empresa accedió al correo electrónico de un trabajador y se encontró con contenido personal, que leyó e incluso transcribió. El tribunal estimó que no existía vulneración de la privacidad porque los mensajes de contenido privado fueron enviados durante el horario laboral, a través de herramientas corporativas y, además, estaba prohibido expresamente por la normativa interna de la compañía, aunado al hecho de que la empresa comunicó a Mihai Bărbulescu¹⁷, que sus mensajes y correos electrónicos (que entraban y salían de esta cuenta de Messenger) estaban siendo vigilados desde hacía una semana e incluso le mostraron transcripciones literales de los correos electrónicos personales, por lo que *“fue informado de las normas de la empresa en todo momento”* y sabía el riesgo que asumía al utilizar las herramientas de la compañía con fines exclusivamente privados, por lo que *“El empleador actuó dentro de sus facultades disciplinarias (...) por tanto, el acceso [al correo electrónico del empleado] había sido legítimo”*, siendo que la empresa, aunque desde el momento de la interceptación de los mensajes —que pensaba en todo momento que eran profesionales— conocía la identidad de los destinatarios, nunca desveló de quiénes se trataba. Por ese motivo se consideró que existía un “equilibrio” entre la lectura de mensajes privados de un empleado por parte

¹⁶ Tribunal Constitucional “Alcalde de la I. Municipalidad de Melipilla con Ministros de la Corte de Apelaciones de Santiago” del 22 de mayo de 2013 Rol. 9563-2012 / Caso “Omar Alejandro Figueroa Silva con Carabineros de Chile” del 30 de agosto de 2012, Rol 5322-2012 / Sentencia N 2502-2012 del 12 de mayo de 2012.

¹⁷ Ingeniero rumano contratado por una empresa rumana, después de que fuera despedido en 2007, porque su superior sospechaba que había dado un uso privado a las herramientas de la compañía y descubrió que utilizaba Yahoo! Messenger para comunicaciones tanto de índole personal como profesional, se encontró con contenido personal, que leyó e incluso transcribió.

de su empleador y el mantenimiento del derecho a la privacidad, debido a que “no es irracional el hecho de que un empleador quiera verificar que los empleados realizan efectivamente tareas profesionales en horas de trabajo”. No obstante esta decisión aún no es definitiva ya que las partes disponían de tres meses para recurrir la decisión del tribunal.

A esta persona se le despidió sobre el fundamento de que la empresa prohíbe en su normativa interna el uso de los recursos corporativos —como podía ser esta cuenta de Yahoo (creada para que atendiera los clientes) o la propia conexión a Internet— para fines personales.

Así este fallo se dictó, con seis votos a favor y uno en contra (el del magistrado portugués Paulo Pinto de Albuquerque), avalando que las empresas puedan leer e inspeccionar el correo electrónico privado o profesional (del trabajo) de sus empleados si sospechan que alguno está haciendo un uso personal de las herramientas de trabajo, luego de desestimar el recurso impuesto¹⁸.

En tal sentido, se estimo que el empresario tenía derecho a comprobar si el trabajador estaba centrado en sus tareas porque pensaba que la cuenta a la que estaba accediendo sólo tenía un uso laboral. La sentencia consideró que no había vulneración al derecho de privacidad porque los mensajes de contenido privado fueron enviados durante el horario laboral, a través de herramientas corporativas y, además, estaba prohibido expresamente por la normativa interna de la compañía, con lo cual se avaló lo ya indicado por un tribunal rumano¹⁹.

De esta manera se buscó un “equilibrio” entre la lectura de mensajes privados de un empleado por parte de su empleador y el mantenimiento del derecho a la privacidad.

Por otro lado, al *Cour de Cassation* de Francia, en el año 2001, señaló que los empresarios no pueden abrir y leer los *e-mails* personales de sus empleados, aunque sean recibidos o enviados a través de una cuenta puesta a disposición por el empleador para fines exclusivamente laborales, porque constituye una

¹⁸ Se debe tomar en cuenta que este empleado trabajó entre 2004 y agosto de 2007 en el departamento de ventas de una empresa privada de ingeniería, donde se le ordenó crear una cuenta de Yahoo Messenger con el propósito de responder a las inquietudes de los clientes.

¹⁹ Además también se debe considerar que el 13 de julio de 2007, la dirección de la empresa comunicó a Bărbulescu que sus mensajes y correos electrónicos (que entraban y salían de esta cuenta de Messenger) estaban siendo vigilados desde hacía una semana e incluso se le mostraron transcripciones literales de los correos electrónicos personales donde, en ocasiones, hablaba de sexo y temas de salud, según el comunicado del tribunal, con su pareja y su hermano, motivo por el cual el 1 de agosto se le comunicó el fin de su contrato laboral en la empresa.

Por ello, como fue informado de las normas de la empresa en todo momento y sabía el riesgo que asumía al utilizar las herramientas de la compañía con fines exclusivamente privados. “El empleador actuó dentro de sus facultades disciplinarias (...) por tanto, el acceso [al correo electrónico del empleado] había sido legítimo”, por lo que no hay ninguna razón para cuestionar el dictamen del tribunal rumano. En una primera instancia el empleado se querelló contra la empresa, cuyo nombre no se ha hecho público, pero la denuncia se desestimó porque «no es irracional el hecho de que un empleador quiera verificar que los empleados realizan efectivamente tareas profesionales en horas de trabajo».

violación de su intimidad y de su vida privada, lo cual es válido incluso aunque el empresario haya prohibido la utilización no profesional de internet²⁰.

En Argentina, se han encontrado escasas posturas doctrinarias vinculadas estrictamente al tema investigado, esto es la cuestión en el marco de una relación laboral²¹ y en lo que respecta a la jurisprudencia, no fue sino hasta el año 2003 que comenzaron a conocerse fallos como el de un tribunal de primera instancia que declaró procedente el despido de una trabajadora por enviar *e-mails* pornográficos con la herramienta informática de la empresa en horario laboral²², siendo que dicho fallo luego fue revocado por la Cámara interviniente²³. También fue dictada una resolución de Cámara²⁴ que, declaró la improcedencia del despido de un empleado por usar el *e-mail* laboral para fines particulares, ante la ausencia de una política de uso de la herramienta informática previamente establecida y notificada a los empleados²⁵; frente a todo esto se han producido proyectos legislativos al respecto, los cuales no son coincidentes.

V. Empleados públicos y privados

Ya visto lo general respecto al correo, debemos observar si es distinto el caso de los funcionarios públicos y los correos electrónicos enviados y recibidos en el desempeño de sus funciones, en razón del desempeño de la función pública que ejercen y que está legítimamente sujeto al escrutinio de la ciudadanía, al

20 Cour de Cassation, Chambre Sociale, 2/10/01, sentencia 1. 99-42,492, “M. Frédéric Onofc. Societé Nikon France S.A.”. El fallo se refiere al caso de Nikon France contra uno de sus antiguos empleados, que en 1995 fue despedido por pasar la mayor parte del tiempo de su horario de trabajo utilizando el correo electrónico de la empresa para fines personales, <http://cs.gsmbox.com/news/mobileneuws/all/62164.gsmbox>. Puede consultarse el fallo en su idioma original en <http://www.courdecassation.fr/agenda/arrets/99-42942arr.htm>.

21 Galdós: “Correo electrónico, privacidad y datos”. *Revista de Derecho de Daños*, 2001-3-157; Grassis: El despido con causa en el @b-uso del correo electrónico e internet en horario de trabajo <http://www.eldial.com.ar>. [Consulta: 2016, septiembre 22]; Loguarro: Uso y mal uso del e-mail laboral. Un fallo eemplar <http://www.eldial.com.ar>. [Consulta: 2016, septiembre 22].

22 Juzgado Nacional 1º Instancia Laboral N° 24, 27/5/03, sentencia 72/03, “V.R.I. c. Vestidos S.A. s/Despido”, <http://www.eldial.com.ar/nuevodiaU030627-a.asp>. [Consulta: 2016, septiembre 22].

23 CNAT, Sala X, 17/10/03, sentencia 12.245, <http://www.eldial.com.ar>, número especial del 1617/04. [Consulta: 2016, septiembre 22].

24 CNAT, Sala VIII, 27/3/03, sentencia 36.580, “Pereyra, Leandro Ramiro c. Servicios de Almacén Fiscal Zoona F’ranca y Mandatos S.A. s/Despido”, en <http://www.eldial.com.ar/nuevodia/030711-b.asp>. [Consulta: 2016, septiembre 22].

25 A los fallos citados pueden agregarse CNAT, Sala 1, 10/4/03, sent. 80.557, “U.J.A. c. Bayer Argentina S.A. s/Despido”; ídem, Sala 111, 29/8/03, sent. 85.145, “B.M.c. SGS Societé Generale de Surveillance S.A. s/Despido”; ídem, Sala VII, 23/2/04, sent. 37.287, “Zitelli, Gustavo Martín c. Fibertel S.A. s/Despido”; ídem, Sala X, 13/8/03, sent. 11.924, “García, Delia María del Rosario c. YPF Yacimientos Petrolíferos Fiscales S.A. s/Despido”; ídem, Sala X, 26/8/03, sent. 11.988, “Giménez, Victoria c. Crear Sistemas S.A. y otros/Despido”, todos en <http://www.eldial.com.ar>. [Consulta: 2016, septiembre 22].

existir un interés público en la transparencia de los actos de la administración del Estado, lo cual incluye los correos electrónicos de sus funcionarios.

En tal sentido se debe dar un equilibrio de intereses, algunos se inclinan por una mayor publicidad de los actos públicos, al considerar que al entregarse los correos institucionales estos no poseen ningún dato que se considere privado del funcionario con la Administración pública.

Por otra parte, se pudiera alegar que 7.- Contraloría General de la República, Dictamen N° 57.201, 2013.: 1) la utilización de insumos públicos (equipo, Internet, horario de trabajo) no determina que el correo posea carácter público; 2) tampoco es público en todos los casos de correos de uso de direcciones o servicios institucionales, pues se reconoce un interés privado por sobre el público, cuando el contenido no incluye información de relevancia pública; 3) por la definición abierta de “acto administrativo” en la mayoría de las legislaciones, los correos electrónicos son potenciales contenedores de tales actos, siendo relevante su publicación en cuanto es tangencial al tema. De esta manera, sólo serían correos necesariamente públicos aquellos enviados desde la casilla institucional, que contengan un acto administrativo o de relevancia pública que amerite la publicidad del mismo, no obstante algunas regulaciones en el derecho comparado no se hace señalamiento alguno respecto al mecanismo a utilizarse para conocer ese contenido a fin de determinar su carácter público o no²⁶.

En este sentido, se puede pensar que en el caso de los trabajadores de la Administración pública, se debe entender que existe un interés público en el escrutinio de sus actividades, ante lo que pueden surgir dos posiciones encontradas: 1) la posición que respalda la procedencia de una esfera de privacidad del funcionario, que abarcaría todo aquello que no posea un acto de relevancia administrativa, y 2) la posición acerca de la publicidad por defecto de los correos institucionales en su totalidad²⁷.

Así es evidente que existen intereses en pugna que no permiten dar una solución de manera absoluta o binaria, sino que cada país deberá darle un marco regulatorio que permita asegurar de mejor forma tanto el interés público como los derechos humanos, fundamentales y constitucionales de los funcionarios públicos, siendo que a veces la jurisprudencia no es suficiente para dar las soluciones debidas, sino que harán falta cambios legales que regulen los mecanismos para determinar si el contenido de correos electrónicos en la Administración pública son parte o no de los deberes de transparencia de estos.

26 Para ampliar sobre este punto del acto administrativo electrónico se puede ver a Mónica RIVERA CAJAS: “El acto administrativo electrónico en Venezuela”. *Revista Derecho y Tecnología*, N 15, Universidad Católica del Táchira, 2014, pp. 85-104.

27 Sin embargo, este segundo criterio ha sido cuestionado en Chile mediante de recursos por inconstitucionalidad, por lo que pareciera en ese país haber una tendencia orientada a una mayor protección de las comunicaciones, por sobre el principio de transparencia, lo que estaría respaldado por la Ley 20.285.

Lo cierto es que el control del correo electrónico afecta tanto a trabajadores privados como a los servidores públicos, por ello en Cataluña, se está preparando un Código Deontológico para limitar el uso de internet y del *e-mail* por parte de los funcionarios de la Administración catalana, mediante el cual se pretende recoger posibles conductas prohibidas, normas de seguridad y control de códigos de acceso.

En el caso de Venezuela, se debe tomar en cuenta lo establecido en los artículos 8, 10, 45.2 y 50 de la Ley Contra la Corrupción que establecen que toda la información sobre la administración del patrimonio público que corresponda a las personas reguladas en esta ley, tiene el carácter público, siendo que los particulares tienen el derecho de solicitar a los órganos y entes administrativos, cualquier información sobre la administración y custodia del patrimonio público de dichos órganos y entes, pudiendo acceder y obtener copia de los documentos y archivos correspondientes para examinar o verificar la información que se les suministre, de acuerdo con el ordenamiento jurídico vigente, salvo las excepciones que por razones de seguridad y defensa de la Nación expresamente establezca la ley, todo esto sin perjuicio de lo establecido en la Ley Orgánica del Ministerio Público y en el Código Orgánico Procesal Penal, en los que la Fiscalía General de la República puede solicitar a los órganos de investigación penal, realizar actuaciones complementarias que permitan recabar los elementos probatorios conducentes a determinar la procedencia del ejercicio de las acciones a que haya lugar, contra las personas sometidas a investigación por el órgano contralor, de tal manera que los funcionarios o empleados públicos y los particulares están obligados a rendir declaración de los hechos que conozcan y a presentar a la Contraloría General de la República o a sus delegados, al Ministerio Público y al órgano jurisdiccional competente, según el caso, libros, comprobantes y documentos relacionados con el hecho que se averigua, por lo que cuando se tratare de inspección de cartas, telegramas, papeles privados y cualquier otro medio de correspondencia o comunicación (como el correo electrónico), se procederá de conformidad con lo establecido en la Constitución de la República Bolivariana de Venezuela, el Código Civil y el Código Orgánico Procesal Penal.

Por su parte, la Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado; publicada en la Gaceta Oficial N° 39.945 del 15 de junio de 2012, en su artículo 43, establece que los órganos y 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 y ciudadanas.

También se ha de tomar en cuenta y es aplicable, en nuestro criterio, a los correos de trabajo de los funcionarios públicos la Ley Sobre Delitos Informáticos, que como dijimos contempla en sus artículos 6, 13, 14, 20, 21 y 22, los delitos

contra la privacidad de las personas y de las comunicaciones, referentes a la violación de la privacidad de data o información personal y la propiedad de la misma; violación de la privacidad de las comunicaciones y revelación indebida de data o información personal, las cuales se deben vincular con las disposiciones contenidas en los artículos 186 al 191 del Código Penal Venezolano, en lo que se refiere al Título II, Capítulo V “*De los Delitos contra la Inviolabilidad del Secreto*”, en los cuales se contemplan penas de multas, arresto y prisión, para quienes estén subsumidos en los supuesto allí previstos, las cuales serían plenamente aplicables a los correos electrónicos.

Se encuentra también la Ley de Infogobierno, en la que debemos recordar que busca la apropiación social del conocimiento; así como se rige por los principios de confidencialidad, integridad, privacidad y disponibilidad de la información, teniendo especial relevancia los artículos 25 y 77 relativos al respecto al uso de las tecnologías de información por el Poder Público y el Poder Popular que debe comprender la protección del honor, vida privada, intimidad, propia imagen, confidencialidad y reputación de las personas; aunque sujeto a las limitaciones de la ley; así como que se tiene la obligación de proteger la información que obtiene por intermedio de los servicios que se prestan a través de las tecnologías de información y la que repose en sus archivos o registros electrónicos. Esto obviamente, no se refiere solo al ciudadano común o particular sino también respecto a los empleados y funcionarios públicos.

En relación con los empleados públicos que no son funcionarios y el personal obrero, les sería aplicable el artículo 16, literal “d”, del Reglamento de la Ley Orgánica del Trabajo, antes mencionado y que establece las obligaciones fundamentales del patrono (en este caso Administración Pública) con el trabajador con el que tiene una relación individual de trabajo, debiendo respetar su dignidad, privacidad, intimidad y libertad de conciencia, todo lo cual se extiende al derecho a la privacidad de las comunicaciones que el trabajador emita o reciba en el curso de la prestación de sus servicios al patrono, en razón del principio de progresividad e interpretación extensiva de los derechos humanos. Pero también le son aplicables los deberes del trabajador del artículo 17, literal a *eiusdem*, mencionado en los párrafos anteriores respecto a las condiciones y términos pactados de la prestación del servicio, en concordancia con lo previsto en el artículo 18 *ibidem*, relativo al derecho del trabajador a no acatar instrucciones que comprometan manifiestamente su vida, salud o la preservación de la empresa o sean incompatibles con su dignidad.

Respecto a estos funcionarios, empleados y obreros también les es aplicable el Decreto Ley Sobre Mensajes de Datos y Firmas Electrónicas, en su artículo respecto a los derechos a la privacidad de las comunicaciones y de acceso a la información personal, así como lo establecido en su Reglamento parcial, en relación a los planes y procedimientos de seguridad que deben ser suministrados por estos proveedores.

Además, no se debe olvidar la distinta normativa que indica que la Administración Pública puede usar el correo electrónico como la Ley de Simplificación de Trámites Administrativos; la Ley Orgánica Procesal del Trabajo; la Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos; la Ley Orgánica de Telecomunicaciones; la Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado; la Ley Orgánica de Administración Pública; el Código Orgánico Tributario; la Ley Orgánica de la Jurisdicción Contencioso Administrativa, la Ley Orgánica Procesal del Trabajo y la Ley Orgánica del Tribunal Supremo de Justicia.

Por ello, cualquier transgresión al respecto haría aplicable la Ley sobre Delitos Informáticos en lo relativo a los delitos contra la privacidad de las personas y de las comunicaciones, de la data o información personal y la propiedad de la misma; en relación con los artículos 186 al 191 del Código Penal Venezolano, sobre los delitos contra la inviolabilidad del secreto. Así como también se les aplicaría la Ley sobre Protección a la Privacidad de las Comunicaciones, en relación a la privacidad, confidencialidad, inviolabilidad y secreto de las comunicaciones.

VI. El control de los trabajadores sobre sus correos electrónicos, posibilidades y límites de los patronos

El uso del correo electrónico empleado para realizar las comunicaciones personales conlleva cierta expectativa de privacidad e intimidad, que suelen estar protegidas por la Constitución y las leyes de cada país. De esta forma, en el ámbito laboral, si bien el empleador suele tener una facultad legal para fijar las condiciones externas del uso del correo electrónico, no puede del mismo modo inmiscuirse en las comunicaciones mismas realizadas por esa vía, por afectar a los derechos fundamentales de los trabajadores, ya hemos visto como la jurisprudencia de algunos países no están contestes en este sentido, sino que por el contrario algunos consideran que no existe limitación alguna.

Esta falta de unidad de criterios en los distintos países mencionados, hace aún más difícil establecer un criterio único sobre todo en el caso de los funcionarios de la Administración pública, donde existe un interés público comprometido en el deber de transparencia por parte del Estado, por lo que es allí donde se requiere un esfuerzo mayor por parte del legislativo, a fin de armonizar los intereses legítimos de la ciudadanía con los derechos de quienes trabajan para el Estado.

Ahora bien, se puede pensar en dos puntos: 1) el primero, si es admisible imponer limitaciones por el empleador al empleo del correo electrónico por parte de los trabajadores y, en caso de ser afirmativa la respuesta, bajo qué condiciones legales, formales y materiales; 2) el segundo, si el empleador o

patrono dispone de las facultades para imponerse del uso que el trabajador está dando al correo electrónico.

En cuanto a si es posible al empleador imponer limitaciones al uso del correo electrónico, al ser este una herramienta de propiedad de la empresa, que es puesta a disposición del dependiente para una prestación más eficaz de los servicios objeto del contrato, pareciera que es posible admitir la imposición de restricciones, así como que tales condiciones y limitaciones se contengan en algún reglamento interno de la empresa, siendo que lo mismo sería extensivo a la reglamentación de la materia en un contrato colectivo.

No obstante, en las empresas en las cuales no existe un reglamento interno, o sea obligatorio la entrega de la misma es cuando se pueden presentar mayores conflictos en relación a los derechos de los trabajadores, sobre todo porque desconocería su poder de negociación en la contratación de sus servicios; y, porque si se estableciese una cláusula que indicase que dar tal información sobre el uso de correo electrónico no es necesario, carecería de un control de legalidad y *sería nulo, sobre todo porque consideramos que sería ajeno al espíritu general de la legislación laboral y al carácter constitucional de los derechos potencialmente afectados produciéndose una merma en la privacidad del trabajador*, incluso algunos piensan que cualquier normativa al respecto debería estar autorizada por el órgano administrativo correspondiente, al considerar que una simple comunicación del empleador sobre las condiciones de uso del correo electrónico, no es suficiente.

Las condiciones y limitaciones de uso del correo electrónico que se contemplen en un reglamento interno, deben satisfacer las exigencias previstas en el ordenamiento jurídico, incluyendo la laboral, la que tiene que ver con medios informáticos y la protección de las comunicaciones, mucho más cuando la reglamentación sobre el uso del correo electrónico se contiene en un contrato colectivo o individual de trabajo y dependiendo de cada país deberá ser aprobado por la autoridad laboral administrativa correspondiente como las inspectorías del trabajo²⁸; ya que en caso contrario, las prácticas contractuales conducirían a eludir el cumplimiento de la normativa laboral y del ordenamiento jurídico.

Una reglamentación hecha por el patrono mediante la cual la privacidad de una emisión de correo electrónico se pierda mediante el artilugio de imponer al trabajador la renuncia a tal privacidad o el desvelamiento de su contenido al empleador o a su representante, sería violatoria del derecho a una comunicación privada y el derecho a la intimidad y privacidad, imponiendo condiciones que obstaculizan su libre ejercicio, menoscabando de tal manera el derecho que podría llegar a desaparecer, al imponer la obligatoriedad de la publicidad de la esfera de privacidad del dependiente que se expresa a través de tal medio.

²⁸ En Venezuela se presenta ante la inspectoría del trabajo de conformidad con lo establecido en los artículos 439, 444, 448, 450, 451 y 474 de la Ley Orgánica del Trabajo, los Trabajadores y las Trabajadoras.

La intromisión del empleador en la correspondencia electrónica privada del trabajador está sujeta a acciones civiles y penales del caso, junto con constituir una infracción a las obligaciones que impone el contrato de trabajo, cuya gravedad, podría llegar a constituir causal de despido indirecto en caso del representante del patrono que efectúe tal acción. Por ello, es relevante discernir si la correspondencia electrónica recibida y enviada por el trabajador reviste carácter privado o público; y si existen excepciones que permitan las búsquedas del empleador destinadas a recobrar en forma inconsulta un archivo o documento necesario para el funcionamiento de la empresa u organismo.

Por otro lado, no constituiría una intromisión en el contenido de la correspondencia electrónica, el acceso del empleador para calibrar el volumen de tráfico de e-mail desde el computador del trabajador, sin llegar a verificar su contenido, pero teniendo en claro bajo qué condiciones; cómo se conjugaría el monitoreo del correo electrónico con la legislación sobre protección de datos personales en los países en los que existe (lamentablemente en Venezuela aún no hay nada), en particular con la exigencia de consentimiento del titular de datos personales que debe mediar para legitimar el tratamiento de estos, salvo las excepciones que la propia ley indique. El empleador, bajo la práctica de las llamadas auditorías digitales a la web puede controlar esto.

De acá la importancia de brindar una solución a los problemas jurídicos asociados al empleo del correo electrónico por los trabajadores, tanto por los derechos en colisión, como por la frecuencia de tales conflictos ante la creciente aplicación de la informática en la empresa.

El empleador no tiene plena libertad de revisar el correo corporativo y mucho menos el personal, pero el derecho a la intimidad y la inviolabilidad de las comunicaciones (informáticas o no) no son derechos ilimitados sino que poseen limitantes como lo podría ser lo que establezcan las leyes, un convenio de empresa o el Estatuto de los Trabajadores.

El correo corporativo en cuanto a su privacidad o visibilidad, puede pensarse como ya dijimos en una tarjeta postal y en una carta, siendo que en la primera, no se pretende que el contenido sea privado; en la segunda, sí. De este modo, si la empresa tiene un sistema de comunicación abierto al público donde todas las personas saben que todo el mundo tiene acceso a todos los contenidos, no hay secreto en las comunicaciones y una empresa puede entrar sin lesionar derechos; por el contrario si es un correo a nombre del trabajador de la empresa, con una contraseña única y privada y este considera que es secreto porque no se le indica lo contrario, su contenido podría entrar en el ámbito del derecho a la intimidad. Esto significa que en una empresa se pueden establecer sistemas informáticos en los que no haya secretos, que no tengan clave de entrada, con un entorno usado y visible por todos los trabajadores.

Podríamos preguntarnos si se tiene menos derecho a la privacidad en el trabajo, ante lo cual podemos pensar que un empleado al ingresar al trabajo siempre cede parte de su privacidad por necesidades justificadas de la empresa,

como ocurre en el caso de no poder negarse a que se use su nombre o apellido o que su foto sean usados para llevar a cabo un control de horario (carné de ingresos y egresos, tarjeta de fichaje, página web de la empresa), o impedir que su jefe entre en su oficina alegando que es un espacio personal o privado. Por lo tanto, lo importante es la proporcionalidad en el uso de esos datos, ya que sería desproporcionado que la empresa publicara esa imagen en internet en una página distinta a la de la empresa u organismo, o la usara con unos fines inadecuados, o entre a la oficina sin avisar de manera tempestiva, de allí que si se da un instrumento al trabajador en el ámbito laboral, debe utilizarlo únicamente para esos propósitos.

Hay que tener en claro que el correo electrónico del trabajo y no el correo electrónico personal, es de la empresa u organismo en el que se labora, no obstante existe un hábito o costumbre social que lleva a los trabajadores y empleados a pensar que se puede utilizar privadamente la computadora de la oficina para enviar correos electrónicos particulares, por ello, es relevante que se avise al trabajador y empleado sobre las condiciones de utilización y que se va a monitorizar el uso del correo electrónico o de que solo se puede emplear con unos propósitos determinados, es decir, una aplicación profesional, para evitar que se produzca una expectativa de privacidad en el uso de la computadora en el trabajo, de esta manera no estaría protegido por el derecho a la intimidad y el trabajador tendrá que asumirlo como normas de la empresa.

De allí que una empresa no pueda vigilar a sus trabajadores sin avisar que utilizará sistemas de vigilancia o control, y además estos han de ser siempre de modo proporcional, ya que una empresa no puede instalar cámaras en áreas de descanso o en el baño, porque ese uso no estaría justificado, por ello no se puede emplear una cámara de seguridad como sistema de control laboral de la presencia o ausencia del trabajador si no se le avisa previamente.

Si un empleador tiene sospecha fundada de que algún delito o irregularidad se está cometiendo por parte de sus trabajadores o empleados, debe primero utilizar los instrumentos jurídicos con los que cuenta para denunciar que un trabajador está haciendo mal uso de sus instrumentos de trabajo, y de conformidad con los requisitos y condiciones establecidos, y si el instrumento de control vulnera el secreto de las comunicaciones, hay que recurrir a la autorización judicial, como sería el caso de que un empleador o patrono considere que el trabajador está llevando a cabo una actuación ilícita mediante el correo electrónico ante lo cual tiene que denunciarlo, y un juez deberá autorizar en ese caso la intervención en el soporte correspondiente, sea una computadora u ordenador, un teléfono, etc., sobre todo al considerar que todo trabajador o empleado que divulgue o ceda información confidencial de su trabajo está cometiendo un delito, pero la voluntad del empresario o patrono no es suficiente para violentar el secreto de las comunicaciones o el derecho a la intimidad si no se siguen los canales legales correspondientes.

Se debe tener presente que hay legislaciones como la de EEUU que en la mayoría de los casos se estima que el correo laboral o institucional no le pertenece al trabajador, sino que los empleadores son dueños del sistema de correos electrónicos que utiliza la compañía, y por lo tanto pueden evaluar el contenido de los mensajes, ya sea que se manden internamente junto con aquellos que se transmiten desde su computadora a otra compañía o de otra compañía a su computador por lo que estarían sujetos a ser monitoreados por su empleador, incluyendo cuentas de correo electrónico en línea como Yahoo y Hotmail, así como mensajes instantáneos y los sistemas de buzones de voz, por lo que en general, los empleados no deben suponer que sus comunicaciones son privadas y no son monitoreadas²⁹. De esta manera se practica la censura y la autocensura en las empresas norteamericanas.

Es importante saber que en los sistemas de correos electrónicos y de voz se conservan los mensajes en su memoria incluso después de haber sido borrados, aunque aparenten ser eliminados, los mensajes continúan existiendo en una cinta magnética junto con otros datos importantes en el sistema de la computadora, incluso muchos sistemas de correo electrónico tienen la opción para catalogar los mensajes como “privados”, pero no es una garantía que los mensajes sean confidenciales, ya que puede existir una excepción cuando un empleador tiene una política de correos electrónicos por escrito en donde dice

29 Han habido varios casos legales sobre el monitoreo en el trabajo que ha resultado favorables para el empleador, como los casos *Smyth v. Pillsbury*, www.loundy.com/CASES/Smyth_v_Pillsbury.html. [Consulta: 2016, septiembre 22], y *Falmouth Firefighters Union v. Town of Falmouth*.

Por lo menos una corte ha establecido ciertas limitaciones a las políticas de empleadores que dicen que los correos electrónicos personales no son privados. La Suprema Corte de Justicia de Nueva Jersey concluyó el 30 de marzo de 2010 que los abogados de un empleador violaron los derechos de privacidad de un empleado, así como las reglas de comportamiento profesional, cuando leyeron los mensajes que mandó el empleado a su abogado usando el computador portátil de la compañía y a través de su cuenta personal de Yahoo protegida por una contraseña: *Stengart v. LovingCare Agency, Inc.*, 2010 WL 1189458 (N.J. March 30, 2010). La corte dijo que el privilegio de abogado/cliente aplica a correos electrónicos aunque el empleador tenga una política general que diga que el empleado no debe esperar tener privacidad en la comunicación que se transmite a través del equipo de la empresa. En este caso, la corte se enfocó en la naturaleza del privilegio de privacidad entre el abogado y su cliente. La corte no abordó el tema de si el empleado tenía una expectativa razonable a la privacidad con respecto a la comunicación por correo electrónico con alguien que no fuera su abogado. En el caso *Holmes v. Petrovich Development Company, LLC*, una corte de California determinó que los correos de un empleado a su abogado mandados desde una computadora de trabajo no estaban protegidos por el privilegio abogado/cliente. Sin embargo, en contraste con el caso *Stengart*, este empleado utilizó una cuenta de correo electrónico de la compañía para mandar los correos, en lugar de una cuenta personal. La corte concluyó que el empleado 1) estaba consciente de la política de la compañía que decía que las computadoras sólo deberían usarse para asuntos de negocios; 2) fue advertido que la compañía podía monitorear las computadoras para asegurarse de que se estuvieran siguiendo las reglas establecidas; y 3) se le notificó que los empleados que utilizan las computadoras de la empresa no tienen derecho a la privacidad.

que los mensajes catalogados como «privados» no son confidenciales. Incluso en estos casos podría haber excepciones (vease el caso *Smyth vs. Pillsbury*)³⁰. En este sentido, pareciera que los llamados servidores centrales, conectados a los centros de poder, tornan cada vez menos privados estas herramientas.

Es por ello que algunos empleadores codifican los correos electrónicos de sus empleados para proteger su privacidad, lo cual ocurre en la computadora del emisor del mensaje y después es decodificado en la computadora del destinatario, para garantizar que el mensaje solamente es leído por el emisor y el destinatario, pero aunque este sistema evita que los mensajes sean leídos por colegas o “espías” industriales, el empleador también podría tener acceso a los mensajes decodificados³¹.

También en la mayoría de los casos, el empleador podría monitorear legalmente el uso de teléfonos inteligentes proveídos por la empresa, donde las aplicaciones de monitoreo pueden grabar de manera secreta los mensajes de texto, correos electrónicos, uso del Internet, ubicación, contactos, llamadas, fotos y videos³².

Incluso en EEUU el empleador puede abrir la correspondencia personal si fue mandada al lugar de trabajo del empleado, aunque las leyes federales prohíben la obstrucción de la correspondencia, el correo es considerado como

³⁰ http://www.loundy.com/CASES/Smyth_v_Pillsbury.html. [Consulta: 2016, septiembre 22].

³¹ En un fallo en junio de 2010 en el caso de *City of Ontario v. Quon*, la Suprema Corte de Justicia confirmó unánimemente que el registro de mensajes personales en un *pager* de un oficial de la ley no violaba sus derechos constitucionales ya que el aparato era propiedad del gobierno. El registro, hecho sin orden judicial, no era una violación de los derechos del oficial otorgados por la Cuarta Enmienda (que se trata sobre la protección a pesquisas y aprehensiones arbitrarias) porque se hizo por cuestiones relacionadas al trabajo. La ciudad estaba intentando determinar si necesitaba modificar su contrato de comunicaciones inalámbricas, la cual imponía tarifas después de que los empleados excedían los límites de caracteres en los mensajes de texto. La ciudad obtuvo una transcripción de los mensajes de Quon durante la investigación para determinar si los oficiales estaban utilizando sus *paggers* o “busca personas” para mandar mensajes personales. La transcripción mostró que Quon estaba intercambiando mensajes con contenido sexual explícito. La decisión de la corte generalmente permite que los empleadores gubernamentales vean los mensajes electrónicos de los empleados si los empleadores tienen un motivo razonable relacionado al trabajo.

Este fue un caso de intrusión gubernamental en las comunicaciones personales de un individuo, o sea, una determinación para saber si la Cuarta Enmienda aplicaba a las comunicaciones electrónicas de los empleados públicos. La Cuarta Enmienda no aplicaría a un empleador de la industria privada. Sin embargo, la decisión de la Corte Suprema fijó un criterio o precedente para las decisiones a futuro que tuvieran que ver con empleados de la industria privada.

Hay una lección importante del caso de Quon: la política de privacidad de un empleador en cuanto al monitoreo de información no necesita especificar todos los tipos de comunicación que abarca. Usted, como empleado, debe suponer que cualquier aparato electrónico que sea prohibido por su empleador podría estar sujeto al monitoreo, independientemente si el aparato es o no mencionado en la política que ha dado a conocer la empresa por escrito.

³² <http://www.usatoday.com/tech/columnist/kimkomando/story/2012-02-24/work-monitor-smartphone/53221804/1>. [Consulta: 2016, septiembre 22].

entregado una vez que llega al lugar donde se trabaja tal como lo dice el manual de correo doméstico de USPS (*Domestic Mail Manual o DMM*), que abarca el manejo de correspondencia dirigida a un individuo en una organización³³. Por ello, el empleador no estaría violando las leyes si abre la correspondencia personal de un empleado que ha sido mandada a la dirección de la compañía, una vez entregada la correspondencia, la organización puede decidir cómo distribuirla, así un empleado cuyo cargo es administrar la correspondencia podría estar autorizado que abrir toda la correspondencia para organizarla antes de entregarla, inclusive la correspondencia que esté catalogada como “personal” o “confidencial” para un empleado en especial³⁴. No obstante, pudieran existir ciertas situaciones en donde abrir o leer la correspondencia de un empleado pudieran ser consideradas invasiones a su privacidad y tendrían que ser muy específicas y guiadas por las leyes de responsabilidad civil. Del mismo modo, se tendría que considerar que la enmienda constitucional a la protección a la intimidad y privacidad podría haber quedado en desuso por la Ley Patriota.

Igualmente se puede dar el monitoreo de las redes sociales, incluso ser despedido por algo que se publique en alguna de ellas, todo lo cual dependerá de las políticas de cada empleador y las leyes del país en donde se dé el hecho. Esto se ve mucho en EEUU donde muchas compañías tienen políticas que limitan lo que se puede publicar sobre su empleador en las redes sociales³⁵. Algunos de sus estados como California, Colorado, Connecticut, Dakota del Norte y Nueva York tienen leyes que prohíben que los empleadores disciplinen a sus empleados en base a sus actividades en las redes sociales cuando no están trabajando, al menos que dicha actividad pueda dañar a la compañía de una u otra forma, ya que las actualizaciones en las redes sociales relacionadas al trabajo tienen el potencial de causar problemas para la compañía, por las leyes antidiscriminatorias que prohíben que los empleadores disciplinen a los empleados en base a su edad, raza, color, religión, sexo o lugar de origen. Hasta ahora no existe una ley federal que prohíba el monitoreo de los empleados en los sitios de redes sociales, incluso los empleadores pueden contratar a terceros para monitorear las actividades de sus empleados³⁶.

33 El manual dice que “Toda correspondencia enviada a una organización gubernamental o no gubernamental, o un individuo por nombre o título a la dirección de la organización es considerada como entregada a la organización, así como correspondencia enviada a ex oficiales, empleados, contratistas, agentes, etcétera. Si existe un desacuerdo en cuanto a dónde debe entregarse dicha correspondencia, entonces debe ser entregada bajo las órdenes del presidente de la organización o un oficial con un cargo equivalente.” DMM Chapter 508, Section 1.5.1. <http://pe.usps.com/DMM300/Index>. [Consulta: 2016, septiembre 22].

34 <http://www.businessmanagementdaily.com/19709/mail-policy-considerations-maintaining-the-right-to-open-employee-mail>. [Consulta: 2016, septiembre 22].

35 La página de Internet llamada *Compliance Building* tiene una base de datos de políticas de redes sociales de cientos de compañías.

36 En marzo de 2010 una compañía llamada Teneros lanzó un servicio llamado “Social Sentry” que rastrea la actividad en línea de los empleados a través de los sitios de redes sociales.

En relación a la protección a la privacidad en el trabajo, en EEUU se plantea si es jurídicamente vinculante las promesas que hacen los empleadores en cuanto al correo electrónico y otros asuntos de privacidad en el trabajo, siendo que por lo general, las políticas de una compañía sí son jurídicamente vinculantes cuando un empleador da a saber o conocer su política en el trabajo, las cuales se pueden dar a divulgar de varias formas como a través de los libretos para empleados, de memos y contratos para empleados que forman parte del sindicato, existiendo excepciones para investigaciones en donde se sospecha que el empleado hizo algo indebido o ilícito³⁷. Es llamativo que existan muy pocas leyes que regulan el monitoreo de empleados.

VII. Valor probatorio de estos correos electrónicos en juicio

Sin pretender ser exhaustivos sobre este punto, debemos mencionar que estos correos electrónicos generados en los sitios de trabajos ya sea en el sector público o privado, poseen también relevancia en cuanto a su valor probatorio en juicios, así como en cuanto a su eficacia como notificaciones contractuales por correo electrónico, con validez probatoria, al tomar en consideración que cada vez nos comunicamos más por correo electrónico, y cada vez se requiera más de una prueba legal de esas comunicaciones; sobre todo al considerar que:

- 1) Usualmente dichos correos electrónicos no son llevados a juicio en el formato original, es decir, no se incorpora al juicio el documento electrónico original (que está grabado en un disco duro, “CD”, “pendrive” o similar), sino una copia impresa en papel³⁸; y
- 2) Cuando se promueve el documento electrónico original, el mensaje de datos o correo electrónico suele no estar firmado electrónicamente; y por lo tanto no se le reconoce autoría ni se le presume inalterado, por lo que para que al mensaje que pueda dársele en juicio la misma validez probatoria que a un documento con una firma autógrafa, dicho correo debe ser promovido en documento electrónico original y el mismo debe estar además firmado electrónicamente mediante la utilización de un

De acuerdo a un artículo de Read Write Web, los empleadores utilizan estos servicios para “asegurarse de que sus empleados no estén filtrando datos sensitivos en los sitios de redes sociales o portándose de una forma que pudiera dañar la reputación de la compañía”.

³⁷ En el caso *Smyth v. Pillsbury* (C.A. NO. 95-5712, U.S. District Court for the Eastern District of Pennsylvania, Jan.18, 1996, Decided, Jan. 23, 1996) el despido de un empleado fue confirmado por una corte a pesar de que la compañía tiene una política de permitir el uso de los correos electrónicos por cuestiones personales. En este caso, el empleador había mandado mensajes a sus colegas que fueron considerados muy inapropiados para la comunicación en el trabajo.

³⁸ Debemos señalar que la Ley Orgánica Procesal del Trabajo permite que el video-audio de las audiencias se incorporen al expediente.

certificado de firma electrónica emitido por un proveedor acreditado por el Estado venezolano a través de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).

De esta manera, se puede observar que la firma electrónica no debe confundirse con la simple firma escaneada o digitalizada, ya que no son lo mismo, en razón de que la primera según la Ley de Mensaje de Datos y Firmas Electrónicas, es 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, no es un dibujo, forma ni figura, sino un par de claves asociadas; mientras que la segunda es más una foto digital de una firma autógrafa, sin ningún tipo de clave, datos encriptados ni seguridad. Esta ley en sus artículos 2 y 9.2 permite que cualquier persona origine un correo electrónico a través de terceros autorizados y que ese tercero, quién a su vez es signatario o titular de una firma electrónica, asocie dicha firma al mensaje de datos, permitiendo atribuirle autoría.

De allí la importancia de que exista un servicio privado venezolano en Internet o la red, especializado en gestionar notificaciones contractuales por correo electrónico, con validez probatoria, en que las partes en los contratos puedan enviar y recibir notificaciones y comunicaciones vía correo electrónico, quedándose en su poder comprobantes certificados con fecha y hora de envío, que luego pueden ser utilizados válidamente en juicio, lo cual da confiabilidad, es práctico, legal y económico, evitando las dificultades de tener que tratar de notificar a cualquier persona que no desee ser notificado. De este modo cuando es llevado a juicio el comprobante en su versión electrónica e impresa, resulta indiscutible entre las partes la autoría, el contenido, la fecha y la hora de la notificación, tal como lo establece el artículo 4 de la Ley de Mensaje de Datos y Firmas Electrónicas.

Por otra parte la jurisprudencia del Tribunal Supremo de Justicia, se ha pronunciado sobre el uso del correo electrónico, tal como se ha indicado previamente en los puntos anteriores en relación a la Sala Constitucional y la Sala Político Administrativa y su respectivo Juzgado de Sustanciación, pero junto a ellos también se ha pronunciado la Sala de Casación Civil en sus sentencias N° 472 del 19 de julio de 2005, N° 769 del 24 de octubre de 2007, N° 460 del 5 de octubre de 2011 y N° 274 del 30 de mayo de 2013, entre otras.

En tal sentido es importante resaltar lo establecido en el artículo 4 del Decreto Ley de Mensajes de Datos y Firmas Electrónicas, que establece que indica que es los mensajes de datos tienen la misma eficacia probatoria que de los documentos escritos y su promoción, control, contradicción y evacuación como medio de prueba, se debe realizar conforme a lo previsto para las pruebas libres en el Código de Procedimiento Civil; así como que la información reproducida en formato impreso, tendrá la misma eficacia probatoria atribuida en la ley a las

copias o reproducciones fotostáticas, lo cual a su vez se debe vincular con los artículos 2, 7 y 9 de esa misma ley.

Por lo tanto, la normativa artículos del Código de Procedimiento Civil aplicables serían las contenidas en los artículos 7, 395, 429 y 502, lo cual se debe concatenar con el artículo 4 del Código Civil.

Finalmente se debe tomar en consideración a la Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado, en sus artículos 54 y 55, que establecen que 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, por lo que los funcionarios públicos están en la obligación de recibir y tramitar los documentos que se le presenten, validando la autenticidad e integridad del documento a través de la consulta que realice en el repositorio correspondiente y constate que el mismo es copia fiel y exacta del original; indicando finalmente que los datos, información o documentos intercambiados por medios electrónicos entre los órganos y entes del Estado, se tendrán como válidos y surtirán todos sus efectos legales.

VIII. Conclusiones

Las condiciones y limitaciones impuestas al uso por los trabajadores del correo electrónico suministrado por la empresa, así como las facultades de que dispone el empleador para ejercer control sobre ello se han constituido en un problema jurídico recurrente en aquellos países donde la penetración de las nuevas tecnologías ha dado pie a su aplicación empresarial. Estos problemas, tal vez se podría considerar que están relacionados con las relaciones desiguales entre empleador y trabajador, en donde los primeros son los dueños de los medios de producción y los segundos suelen ser los débiles en esa relación.

En tal sentido, se encuentran involucrados el derecho a la intimidad, privacidad e inviolabilidad de la correspondencia, los cuales sólo pueden ser restringidos judicialmente en casos muy concretos, no pudiendo ser limitados por la sola voluntad de la empresa u organismo público, ya que lo contrario implicaría que durante la jornada de trabajo no podríamos movernos de nuestro puesto, casi como esclavos. El hecho de que la computadora o el ordenador como el email sean propiedad de la empresa u órgano público, no es lo más relevante, ya que de manera similar como ocurre con los buzones de correo de nuestro edificio que son de la “comunidad de propietarios”, ello no autoriza al Presidente de la Junta de Condominio o al vecino a acceder y leer nuestra correspondencia, por lo que si el patrono e empleador quiere leer los mensajes de correo electrónico

de sus trabajadores lo que debe hacer jurídicamente es pedir previamente su autorización, de lo contrario, se arriesgan a una eventual acusación por un delito contra la intimidad y demandas civiles por daños y perjuicios.

No obstante, este tema sigue sin resolverse definitivamente, donde dependiendo del país a que se refiera pueden existir múltiples soluciones respecto al tema. Sin embargo, el concepto de secreto de la comunicación deberá cubrir no sólo el contenido de la comunicación, sino también otros aspectos de la misma, como la identidad subjetiva de los interlocutores o el medio que se utiliza. De allí que la falta e intervención judicial podría conllevar el incurrir en un delito.

En consecuencia, independientemente del uso que se le dé a ese correo electrónico, existe la disyuntiva de leer o no leer un correo electrónico con anterioridad a que lo haga su destinatario o posteriormente a que éste lo haga y sus posibles implicaciones legales, con lo cual hay que replantearse muchos protocolos como por ejemplo, qué hacer con la cuenta de correo electrónico de un antiguo empleado a la que pueden seguir entrando correos electrónicos, donde por precaución lo lógico sería que automáticamente y durante un periodo lógico de tiempo saltara un mensaje de error en el que se facilitarían otras vías y personas de contacto con la entidad.

Por ende ante la ausencia de normas claras, concretas y específicas en nuestro país y otras partes del mundo sobre el uso del *e-mail* laboral por parte de los empleados y de las facultades de monitorización de esa herramienta informática por el empleador u órgano público, así como la incertidumbre que ello provoca tanto en la empresa o Administración pública como en los propios trabajadores y empleados, se debe tratar este tema desde la óptica de distintas ramas del derecho vigente, teniendo en consideración la descripción, la interpretación y sistematización de la normativa que tiene injerencia sobre dichas cuestiones. Este vacío legislativo junto con los problemas y perjuicios que para los empresarios puede traer aparejado el uso abusivo de esta herramienta informática que ponen a disposición de sus empleados, hace necesario que los cuerpos legislativos dicten la normativa especializada correspondiente que regule esta materia, con la finalidad de que cada una de las partes que componen la relación laboral sepa a ciencia cierta cuáles son sus derechos, sus limitaciones, sus obligaciones y responsabilidades.

Por eso, hasta tanto esto no se produzca, el dictado de un reglamento interno en la empresa u organismo público, que plasmen las pautas de utilización del recurso informático como así también que especifique hasta dónde llegan los poderes empresariales de control, se convierte en un elemento eficaz no sólo para una convivencia más armónica en la relación de trabajo, sino también para evitar que se produzcan daños causados a terceros con el uso del *e-mail* laboral o, que éste pueda hacerse valer como un instrumento para eximir de responsabilidad al empresario si se está frente a un uso en contra de las disposiciones en él contenidas.

De este modo desde el Derecho laboral: 1) la actual legislación venezolana no regula de manera específica y concreta las comunicaciones realizadas mediante el correo electrónico laboral por los trabajadores de la empresa u órgano público, como así tampoco lo atinente a las facultades de control que el patrono posee respecto del uso de esa herramienta informática puesta a disposición de los empleados para el desarrollo de sus tareas, por lo que, hasta tanto se dicte una normativa específica al respecto, las cuestiones deben resolverse en base a las normas vigentes en la legislación laboral y en las convenciones colectivas del trabajo; 2) el patrono o empleador, conforme a las facultades de organización y dirección de la empresa u organismo y la normativa legal vigente, en función del deber de colaboración y solidaridad que se impone a las partes integrantes de una relación laboral, puede válidamente decidir que el correo electrónico como herramienta que se le provee al empleado, debe ser usada para fines exclusivamente laborales; mientras que el trabajador debe acatar la orden y no puede sentirse agraviado por ella ni por el control que el empleador haga de su cumplimiento, colaborando así con las normas impuestas para un mejor funcionamiento de la empresa u organismo; 3) para evitar cualquier discriminación, esa regulación se debe aplicar a todos los empleados que tengan acceso a la cuenta de correo electrónico y se encuentren en similar situación; 4) el empleado que utilice el correo electrónico laboral para la remisión de mensajes privados y ajenos a motivos laborales en horario laboral, sin conocimiento ni autorización del empleador y con conciencia de la prohibición expresa de utilizar dicho medio de comunicación en su trabajo con fines particulares, infringe el deber de buena fe contractual, donde dependiendo de la gravedad del mensaje, pueda calificar un despido u otra sanción; 5) no se violan los derechos constitucionales del empleado cuando el patrono ha comunicado en forma expresa y fehaciente a sus trabajadores que va a monitorizar los *e-mails* que envían y reciben; 6) el control debe efectuarse respecto a todos los trabajadores en forma automática y si no es posible, los criterios para seleccionar a los trabajadores a controlar no pueden ser discriminatorios ni arbitrarios, sino han de estar basados en criterios de aleatoriedad o fundados en razones objetivas; 7) el patrono debe poner en conocimiento de la autoridad laboral correspondiente la normativa que le permite revisar el correo electrónico de sus empleados y confirmar que esto le ha sido comunicado a sus dependientes laborales y cuáles son los medios y la forma a través de los cuales efectuará dicho control; 8) el control de correo electrónico sólo puede ser externo, vinculado al número de mensajes, a los títulos de los asuntos, al volumen de los archivos adjuntos, al contenido de los mismos, siempre en el marco de respeto de la dignidad del trabajador; 9) el empleado que utiliza la herramienta informática para fines personales, sabiendo que no está autorizado para ello y que la empresa está facultada para revisar su contenido, implícitamente está consintiendo en que ésta acceda a dicha información y no existe violación constitucional alguna; 10) el reglamento interno, deberá ser acatado en todos sus términos por los

empleados, en cumplimiento de su obligación de obediencia, diligencia y fidelidad, sin que sea óbice a que también se regule en la negociación colectiva, precisando la pertinencia, la oportunidad y los límites de la monitorización informática; 11) establecida la normativa se pueden revisar los correos electrónicos sin necesidad del consentimiento del empleado; 12) si no hay nada previsto en la normativa respectiva respecto las condiciones de utilización de la herramienta informática ni sobre los controles que puede ejercer la empresa, o cuando en las normas reguladoras se haya contemplado la posibilidad de utilizarlo cuestiones personales, si el patrono pretende revisar los *e-mails* laborales deberá contar con el expreso consentimiento del trabajador, lo cual debe ser excepcional, adoptando todas las garantías necesarias para que ese consentimiento se encuentre exento de vicio alguno, de lo contrario no puede revisarlo; 13) si se advierte que el trabajador utiliza el correo electrónico para cuestiones que no son concernientes a su trabajo, puede aplicar sanciones, fundadas en el incumplimiento de lo establecido en el reglamento interno de la empresa por parte del empleado; 14) el empleado que contraría la normativa sobre el uso del *e-mail* laboral, incurre en una violación de los principios de colaboración, solidaridad, buena fe contractual, y los deberes de diligencia, obediencia y fidelidad, haciendo procedente el despido con justa causa; 15) la conducta del trabajador que incumple con su obligación, puede quedar comprendida dentro del género injuria, pérdida de confianza, la disminución del rendimiento, daños a los intereses del empleador y, en general, violación de la buena fe contractual; 16) los correos electrónicos personales que sean detectados por el empleador y que fundamenten el despido, pueden ser utilizados como pruebas en el juicio laboral; y 17) el empleado debe responder frente a su empleador, si obra con dolo o culpa grave y le produce un daño, por el uso irregular del *e-mail* laboral.

Desde el Derecho civil: 1) existe responsabilidad que puede derivarse del uso del *e-mail* laboral por parte del trabajador, debiendo responder frente a terceros, perjudicados patrimonial o extrapatrimonialmente por él al utilizar como medio o vía para la concreción del daño el *e-mail* que le ha previsto la empresa, así como al patrono, siendo una responsabilidad subjetiva; 2) si el empleado obró con dolo o culpa en ambos casos debe responder frente al tercero perjudicado, aplicándole las normas sobre responsabilidad civil; 3) la responsabilidad del empresario frente a terceros por actos del trabajador, en su carácter de empleador o de propietario de la casilla de correo, debe responder por el hecho del dependiente; pero si el empleado produce el daño en uso irregular del correo electrónico, no puede atribuirse responsabilidad alguna al empleador por no darse en el caso la necesaria relación que debe existir entre la función y el daño como uno de los presupuestos para que exista responsabilidad civil; 4) en el entendimiento de que el correo electrónico es una cosa, el empresario en su carácter de dueño, titular de la cuenta de correo electrónico y de todos los implementos informáticos necesarios para el envío de los *e-mails* laborales, podría ver comprometida su responsabilidad por los daños causados «con» las

cosas o por el riesgo que implican; 5) en los daños causados «con» la cosa, cuando el empleado hace un uso regular del *e-mail* laboral, el empresario deberá responder; si tal uso tiene carácter de irregular, el empresario podrá eximirse de responsabilidad y demostrar que de su parte no hubo culpa, es decir, acreditar que ha tomado todos los recaudos posibles para evitar que el daño se produzca; 6) si se ha causado un daño a un tercero y esto se debe a los excesos del empleado, si el empleador ha tomado todos los recaudos que tiene a su alcance para evitarlos, no deberá responder; 7) cuando se trate de daños causados por el riesgo de la cosa, se estima que esto no comprende al correo electrónico, ya que no es una cosa peligrosa por naturaleza, aunque sí puede ser peligrosa la actividad, por lo que si se envía un correo electrónico, esa conducta de quien la realiza puede generar daños a terceros y, en este caso, el dueño de la casilla de correo electrónico debería responder frente a los terceros, aunque puede eximirse de tal responsabilidad si acredita que la culpa es de la víctima o de un tercero (el empleado) por quien no debe responder, así como que adoptó medidas de prevención razonables pero no pudo evitarse el daño; 8) si el patrono ha tomado todas las previsiones posibles, como dictar una normativa interna de prohibición de uso del correo electrónico para fines que excedan de las tareas asignadas y ha instalado los programas informáticos correspondientes para evitar la causa de daños a terceros y, no obstante ello, el empleado utiliza el correo electrónico laboral en contra de la voluntad expresa del empleador y causa un daño, el empresario tampoco debe responder en su carácter de propietario o guardián de la cosa, ya que se encontraría configurada la eximente de responsabilidad del art. 1193 del Código Civil; 9) la posibilidad de monitorizar los *e-mails* laborales de los empleados, si se ha previamente avisado que el correo electrónico provisto por la empresa es una herramienta de trabajo a ser utilizada exclusivamente con fines profesionales y que la empresa se reserva la facultad de controlar, evita el ser demandado por el trabajador por violación del derecho a la intimidad ni incurre en una conducta “arbitraria”; 10) tampoco sería la conducta del empleador arbitraria, por cuanto concurre en el caso una causa de justificación (el ejercicio legítimo de un derecho) y, por lo tanto, no debe responder frente al empleado por los daños que pretenda haber sufrido; ya que no existe conducta violatoria ni la ilicitud o arbitrariedad; y 11) el trabajador puede sentirse afectado por la decisión de la empresa de controlar los *e-mails* laborales, pero el patrono no tendrá obligación legal de reparar, siempre y cuando haya dado e informado toda la normativa al respecto, pero, si los *e-mails* laborales se difunden en cuanto su contenido, a cualesquiera sea y le produce un daño al trabajador, éste podrá reclamar el pago de una indemnización por cuanto esa difusión ya no entra en el campo del ejercicio regular del derecho que el empleador tiene.

Desde la perspectiva del Derecho constitucional: 1) Se debe equiparar, a los fines de su protección, la correspondencia epistolar con el correo electrónico, no siendo aplicable al trabajador a quien el patrono le ha provisto un correo electrónico laboral, si previamente se le ha notificado en forma expresa que su

uso debe circunscribirse a cuestiones exclusivamente laborales y que la empresa tiene facultad de controlar que dicha directiva sea cumplida y 2) la información que circule por esta vía es de la empresa, quien es su propietaria en virtud de lo cual el empleado no puede tener expectativa de intimidad alguna.

Finalmente desde el punto del Derecho penal: 1) no puede quedar comprendido el correo electrónico como un género de correspondencia protegida y, por lo tanto, no puede considerarse típica la conducta de abrir, desviar, suprimir, comunicar o apoderarse de un correo electrónico que no le esté dirigido, sin incurrir en analogía prohibida y consecuentemente en violación del principio de legalidad; 2) el empleador que monitoriza el *e-mail* del trabajador, en un contexto determinado, cual es la comunicación de la normativa aplicable que prohíbe el uso del correo electrónico para cuestiones ajenas a lo estrictamente laboral, junto con que se pueden revisar los *e-mails* que se envían y reciben, no incurre en ninguna hecho típico y antijurídico contenido en normativa penal; 3) en ningún caso podría el empleador suprimir, desviar, comunicar o publicar un correo electrónico que no le esté dirigido, sin incurrir en una conducta típica y antijurídica; salvo la supresión o desviación, en el caso de que el *e-mail* abierto legalmente contuviera un contenido ilícito con riesgo para los intereses patronales, por lo que podría alegar el ejercicio de una legítima defensa, la justificación que le permitiría la realización de esas conductas; y 4) también cuando se trata de mensajes que constituyan amenazas contra la persona del empleador o de otras, también las amenazas contra la seguridad del Estado.

Aunado a lo anterior, por último y no menos importante, se encuentra también presente la importancia y relevancia del valor probatorio de estos correos electrónicos generados por los empleados, trabajadores y funcionarios en el sector público y privado, en cuanto a su validez en juicio y producción de efectos frente a terceros y entre la partes involucradas.

La audiencia telemática de extradición. Análisis del auto número 74/2016 de la Sala de Casación Penal del Tribunal Supremo de Justicia venezolano

Gustavo Adolfo Amoni Reverón*

SUMARIO: 1. El auto número 74 del 19 de febrero de 2016 y la sentencia número 344 del 7 de octubre de 2016. 2. Las audiencias de extradición en la Sala de Casación Penal. 2.1 Fundamentación jurídica de la audiencia de extradición. 2.2 El objeto de la audiencia de extradición. 2.2.1. Constitución de la República Bolivariana de Venezuela. 2.2.2 Convenios bilaterales. 2.2.2.1 Ley Aprobatoria del Convenio de Extradición entre el Gobierno de la República Bolivariana de Venezuela y el Gobierno de la República Francesa (2012). 2.2.2.2 Tratado de Extradición celebrado entre los Estados Unidos de América y los Estados Unidos de Venezuela (1922). 2.2.2.3 Tratado de Extradición entre la República de Venezuela y el Reino de España (1990). 2.2.3 Tratados multilaterales. 2.2.3.1. Código de Derecho Internacional Privado o Código de Bustamante (1928). 2.2.3.2 Convención Interamericana de Extradición (1981). 2.2.3.3 Convenio sobre Extradición (1911). 2.2.4 Ordenamiento jurídico interno vigente para la fecha de emisión del fallo. 2.2.4.1. Decreto con Rango, Valor y Fuerza de Ley del Código Orgánico Procesal Penal (2012). 2.2.4.2 Código Penal. 2.2.5 Recapitulación. 2.3. La extradición en la jurisprudencia de la Sala de Casación Penal. 2.4. La audiencia de extradición en la práctica de la Sala de Casación Penal. 2.4.1 Procedimiento de ingreso a la Sala de Casación

Recibido: 20/1/2017 • Aceptado: 8/2/2017

* Abogado *summa cum laude* de la Universidad Carabobo, especialista *Cum Laude* en Derecho Administrativo de la Universidad Católica «Andrés Bello», abogado de la Sala de Casación Penal del Tribunal Supremo de Justicia desde 2005, profesor de pregrado de la Universidad Central de Venezuela y profesor de postgrado de la Universidad Católica «Andrés Bello»; dirección de correo electrónico: gustavoamoni@hotmail.com. En elaboración del trabajo especial de grado para optar al título de especialista en Ciencias Penales y Criminológicas en la Universidad Católica «Andrés Bello», del cual formará parte esta investigación.

Penal. 2.4.2 Topografía de la sala de audiencias de la Sala de Casación Penal. 2.4.3. Desarrollo de la audiencia de extradición pasiva. 2.5 La participación telemática en la audiencia de extradición. 2.5.1. Fundamentos normativos para admitir la audiencia de extradición telemática. 2.5.2. Fundamentos jurisprudenciales para admitir la audiencia de extradición telemática. 2.5.3 Fundamentos fácticos para admitir la audiencia de extradición telemática. 3. Conclusión.

Resumen

La Sala de Casación Penal emitió el auto 74/2016 mediante el cual decidió que puede celebrarse válidamente la audiencia de extradición mediante el uso de la videoconferencia. Para ello, se basó en las previsiones del ordenamiento jurídico nacional así como en jurisprudencia patria y en argumentación obtenida de la experiencia, para concluir que tanto la normativa de derecho vigente para entonces como la tecnología existente y las actuaciones a desarrollar durante la audiencia, admiten la participación telemática de quien fuere convocado a la audiencia de extradición. A pesar de generar tal posibilidad, la audiencia telemática no llegó a producirse; sin embargo, el criterio quedó asentado, constituyendo un aporte contundente para continuar fomentando las bondades de la telematización de los procesos jurisdiccionales en Venezuela, sirviendo de antecedente de la Resolución 2016-001 emitida por la Sala de Casación Penal el 12 de diciembre de 2016.

Palabras clave: Casación penal. Extradición. Videoconferencia. Telepresencia. Audiencia. Telemática.

Abstract

The Criminal Chamber of the Supreme Court of Justice decided by sentence 74/2016 the videoconference can be used to celebrate the extradition hearing. That sentence was founded on the Constitution, the law, jurisprudence, and the experience, concluding that existing laws, technologies, at that time, and the actions to be performed before, during and after the hearing, could be done by telematic means. Nevertheless, the hearing was not celebrated, but the criteria was established and works as an element to promote the use of telematics on trials and also as a precedent of the 2016-001 Rule emitted on December 12 by The Criminal Chamber of the Supreme Court of Justice.

Key words: Criminal appeal. Extradition. Videoconference. Telepresence. Hearing. Telematic.

1. El auto número 74 del 19 de febrero de 2016 y la sentencia número 344 del 7 de octubre de 2016.

El 1º de julio de 2013, la Secretaría de la Sala de Casación Penal recibió la solicitud de extradición del ciudadano francés Jérémie Fourny, requerido por la República Federal de Alemania para juzgarlo por la posible perpetración de los delitos de tentativa de asesinato y lesiones físicas peligrosas, tipificados en los artículos 211, 22, 23 y 224 del Código Penal alemán.

Luego de la audiencia correspondiente, la Sala de Casación Penal declaró procedente la pretensión de extradición¹, por lo que Jérémie Fourny fue trasladado hasta Alemania. Encontrándose allí, la República francesa solicitó a la República Federal de Alemania la extradición del mismo ciudadano, por lo que nuevamente, este último Estado, dirigió una petición a Venezuela, pero esta vez, requiriendo la autorización para acordar la extradición que le fue requerida; es decir, solicitó el consentimiento nacional para reextraditarlo.

Tal pretensión se fundamenta en que la persona se encontraba en la República Federal de Alemania porque la República Bolivariana de Venezuela lo privó de libertad y se lo remitió sobre la base de unos delitos específicos, pero no para que lo reenviara a un tercer país, a fin de cumplir una pena por la perpetración de delitos diferentes; en otras palabras, Alemania podía extraditar a Jérémie Fourny solamente porque Venezuela, a su vez, lo había extraditado antes, de lo contrario, Francia hubiera tenido que pedirselo a Venezuela directamente.

Recibida la solicitud de autorización de extradición (reextradición), la Sala de Casación Penal advirtió que ante la ausencia de algún tratado de extradición con Alemania resolvería la pretensión basándose en un tratado previo suscrito con otro Estado, como se había hecho en otros casos, en esta oportunidad, con Francia, y siendo que este último Estado es quien solicitó a la República Federal de Alemania la extradición del ciudadano francés previamente extraditado desde la República Bolivariana de Venezuela, la Sala estimó *“adecuado a derecho tramitar la pretensión de autos sobre la base de dicho tratado bilateral...”*.

En este orden de ideas, el texto jurídico aludido prevé la reextradición siempre que consten cuatro requisitos: 1) El consentimiento de la parte que ha concedido la extradición; 2) La documentación prevista en el artículo IX² (si la parte

¹ Sentencia número 440 del 3 de diciembre de 2013.

² “a. Original o copia conforme de auto de detención, de orden de aprehensión o de sentencia definitivamente firme o cualquier otra resolución emanada de la autoridad judicial competente, que tenga la misma fuerza en la Parte requirente.

b. Los datos del procesado, imputado o condenado, sus datos filiatorios, características físicas y cualquier otro medio que permita en forma inequívoca su identificación y ubicación.

c. Una relación detallada de los hechos que motivan la solicitud de extradición con especial énfasis en el lugar, hora, fecha y circunstancias en que ocurrió y su adecuación al tipo penal correspondiente.

d. La calificación del (de los) tipo (s) penal (es) mencionado (s) y el texto legal que define y sanciona el delito.

requerida lo solicitare); 3) La exposición de los motivos que justifiquen la reextradición; y 4) Un acta en la cual la persona reclamada declare si acepta la reextradición o si se opone a ella.

Al revisar el expediente, la Sala advirtió que faltaban ciertos requisitos³, de los cuales importa destacar, a efectos de este análisis, el siguiente: “Un acta en la cual la persona reclamada declare si acepta la reextradición o si se opone a ella”.

Sin embargo, el órgano jurisdiccional aclaró que la aplicación del tratado debía hacerse en conjunto con la Constitución, que “... *garantiza el derecho a ser oído en todas las actuaciones judiciales; lo que implica el derecho a comunicarse verbalmente con la autoridad jurisdiccional*”.

Este derecho, continúa la Sala, implica la celebración de una audiencia, “... *que interpretada a favor del reo supone que sea en presencia tangible en la sede judicial...*”, tal como lo había decidido antes⁴, declarando improcedente la pretensión de ampliación de la extradición requerida por el Reino de España respecto de una ciudadana previamente extraditada, ya que era necesario convocar a una audiencia pública, situación que resultaba imposible porque la ciudadana ya había sido entregada a las autoridades judiciales españolas.

En ese momento, la Sala, ratificando que la celebración de la audiencia de extradición no podía materializarse, puesto que así como había sucedido en el caso anterior, el ciudadano Jérémie Fourny tampoco estaba en el país sino en Alemania, manifestó que conforme al tratado internacional aplicado, sería suficiente remitir “... *un acta en la cual la persona reclamada declare si acepta la reextradición o si se opone a ella*”.

Pero, consciente de las posibilidades que las Tecnologías de la Información y Comunicación ofrecen, expresó que la emisión de dicha acta debía tenerse como última opción ya que la telemática permitía la declaración a distancia del ciudadano Jérémie Fourny.

Esta modalidad de actuación procesal no es una creación *ad hoc* de la Sala de Casación Penal, sino que la ley y la jurisprudencia ya la contemplaban, incluso

e. Las normas que establecen el cálculo de la prescripción de la acción penal, para el caso de los procesados o imputados, o de la pena, para los condenados, previstas en la legislación de la Parte requirente, así como las actuaciones que pudieron interrumpir la prescripción del (de los) delito (s) o la pena, conforme a la legislación de la Parte requirente”.

³ “1. Las normas que establecen el cálculo de la prescripción de la pena, así como también las actuaciones que pudieron interrumpirla, para el ciudadano condenado JÉRÉMIE FOURNY, previstas en la legislación francesa.

2. La exposición de los motivos que justifiquen la reextradición.

3. Garantías emitidas por la República Francesa de que el ciudadano solicitado no podrá ser juzgado por hechos distintos a los señalados en la solicitud de extradición presentada, cometidos con anterioridad a la referida solicitud, y que no se le podrá imponer la pena de muerte ni penas perpetuas, en caso de revisión de la sentencia remitida (numeral 2 del artículo VI del convenio de extradición franco-venezolano)”.

⁴ Sentencia número 260 del 12 de agosto de 2014.

en el Derecho Comparado. De hecho, casi 10 meses después de la emisión de este fallo, el 12 de enero de 2016, se publicó en la Gaceta Judicial la Resolución 2016-001 sobre participación telemática de los sujetos procesales en las audiencias de la Sala de Casación Penal.

Así, destaca la Sala, conforme a la normativa vigente para entonces, que la Ley Orgánica del Tribunal Supremo de Justicia, aplicable supletoriamente al Convenio de Extradición entre la República Francesa y la República Bolivariana de Venezuela prevé que “... cada una de sus Salas favorecerá la utilización de las herramientas tecnológicas disponibles para la sustanciación de las causas sometidas a su conocimiento...” y establece expresamente: “... crear, mantener y actualizar... un mecanismo de comunicación e información electrónica disponible para todas las personas”.

Incluso, hay al menos doce leyes “... nacionales e internacionales que abonan al uso de la videoconferencia para celebrar la audiencia de reextradición del ciudadano...”⁵.

En el orden jurisprudencial, refiere la Sala, “... es abundante la casuística patria en el uso de la videoconferencia. Comenzando por la propia Sala Constitucional del Tribunal Supremo de Justicia...”⁶.

Además, la recepción legal y jurisprudencial del uso de la telemática para intervenir activamente en las audiencias procesales se fundamenta en que ella permite cumplir con el principio de inmediación, cuando fuere necesario, ya que: 1° El sujeto procesal que intervendrá en la audiencia mediante

5 El Estatuto de Roma de la Corte Penal Internacional; el Convenio de asistencia judicial en materia penal entre los Estados miembros de la Unión Europea; Convenio Iberoamericano sobre el Uso de la Videoconferencia en la Cooperación Internacional entre Sistemas de Justicia; La Ley Orgánica Procesal del Trabajo; la Ley de Protección de Víctimas, Testigos y demás Sujetos Procesales; la Ley Orgánica para la Protección de Niños, Niñas y Adolescentes; la Ley Orgánica de la Jurisdicción Contencioso Administrativa; la Ley Orgánica contra la Delincuencia Organizada y el Financiamiento del Terrorismo y el propio Código Orgánico Procesal Penal, permiten el uso de estas tecnologías en el ámbito procesal; el Decreto con Rango y fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas; 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 y la Ley de Infogobierno.

6 Así como también por el Juzgado Primero de Protección del Niño y del Adolescente de la Circunscripción Judicial del Estado Zulia; el Juzgado Tercero de Protección de Niños, Niñas y Adolescentes de la Circunscripción Judicial del Estado Zulia; el Tribunal Superior Tercero del Circuito Judicial del Tribunal de Protección de Niños, Niñas y Adolescentes de la Circunscripción Judicial del Área Metropolitana de Caracas y Nacional de Adopción Internacional; y, el Juzgado Segundo del Tribunal de Protección de Niños, Niñas y Adolescentes de la Circunscripción Judicial del Estado Zulia. Igualmente, “... en el ámbito del proceso penal se utiliza el sistema de videoconferencia ‘... entre el Palacio de Justicia de Caracas y la sede del Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), ubicada en Parque Carabobo, que permite la comparecencia virtual de los expertos en materia criminalística en la sala de juicio...’, como se informó en nota de prensa en la página de Internet del Tribunal Supremo de Justicia publicada el veintitrés (23) de diciembre de 2014”.

videoconferencia, o el objeto que se examina, puede ubicarse cerca de los magistrados para que estos perciban el contenido y la forma de la declaración; 2° No hay intermediarios subjetivos y objetivos; y, 3°. Los magistrados pueden comunicarse con el o los sujetos que intervienen en la audiencia.

Luego de desarrollar cada uno de los tres tópicos enumerados, la Sala de Casación Penal declaró “... *adecuado a derecho realizar la audiencia... por videoconferencia, desde la sede del órgano jurisdiccional que esté conociendo el proceso... o cualquier otro órgano jurisdiccional que tenga a bien considerar la autoridad competente de la referida República*”.

En consecuencia, solo si no fuera posible la audiencia telemática, concluyó la Sala, sería admisible un acta donde constara la declaración de Jérémie Fourny, a fin de garantizar el derecho a ser oído, “... dadas las características especiales del actual proceso jurisdiccional de reextradición”.

Para culminar, en la sentencia se ordenó notificar a la República Federal de Alemania que debía suministrar los documentos faltantes dentro del plazo de sesenta (60) días continuos a partir de su notificación por los medios diplomáticos, los cuales podía remitir, ratificando el criterio expresado en la sentencia número 791 emitida por la Sala de Casación Penal el once (11) de diciembre de 2015, en formato electrónico, por el sistema que estimare adecuado el Ministerio del Poder Popular para Relaciones Exteriores, siempre que usare firma electrónica dotada de un certificado garantizado por un Proveedor de Servicios de Certificación, debidamente acreditado conforme a lo previsto en el artículo 44 del Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas.

Luego de ser notificada, la República Federal de Alemania manifestó que enviaría el acta con la declaración del ciudadano requerido, prevista en el convenio bilateral franco-venezolano, rechazando la opción de audiencia telemática. En consecuencia, habiendo sido aprobados los requisitos de ley, el ciudadano francés fue extraditado mediante la sentencia número 344 del 6 de octubre de 2016.

Ahora bien, aun cuando la intervención telemática del ciudadano Jérémie Fourny no se realizó, el auto número 74/2016, de la Sala de Casación Penal, destaca por ampliar el acceso a la justicia mediante el uso de las tecnologías de información y comunicación, en este caso, para la reextradición.

2. Las audiencias de extradición en la Sala de Casación Penal

2.1. Fundamentación jurídica de la audiencia de extradición

El ordenamiento jurídico prevé la celebración de audiencias en dos de los cinco procedimientos por los que se tramitan las pretensiones y recursos que competen a la Sala de Casación Penal. Se trata del procedimiento de extradición, incluyendo las modalidades de reextradición y ampliación de extradición, y el

de casación⁷. En los otros tres procedimientos, como son el de interpretación, avocamiento y radicación, no está prevista la celebración de audiencias.

En materia de extradición, que es sobre lo que versa la sentencia bajo análisis, su regulación se encuentra en el numeral 4 del artículo 156 de la Constitución de 1999 (CRBV), en los tratados internacionales suscritos y ratificados por la República, y supletoriamente en el Decreto con Rango, Fuerza y Valor de Ley del Código Orgánico Procesal Penal de (DLCOPP), como lo ratifica el artículo 382 del citado texto adjetivo penal, a lo cual debe agregarse la Ley Orgánica del Tribunal Supremo de Justicia de 2010 (LOTSJ) y el Código Penal de 2005 (CP), en ese mismo orden, puesto que la primera ley es orgánica y posterior, y por tanto, de aplicación preferente a la ley penal ordinaria.

En este sentido, debe precisarse si se encuentra vigente algún convenio internacional bilateral suscrito y ratificado entre la República Bolivariana de Venezuela y el Estado correspondiente, o en su defecto, un tratado multilateral sobre la materia, entendiendo que el primero es ley especial respecto del segundo, aunque este será una análisis del caso concreto. Solamente si faltare alguna de estas normas, se deberá acudir a la normativa jurídica interna, interpretada en conjunto con el principio de reciprocidad.

La afirmación anterior se ratifica, en primer lugar, con el cambio expreso del orden de las fuentes jurídicas de la extradición, que en el Código Orgánico Procesal Penal de 2009 (COPP) se anteponía a los tratados internacionales⁸; mientras que en DLCOPP, el orden se invirtió, primando los tratados internacionales respecto de las disposiciones del texto adjetivo penal, aunado a que se recordó⁹ la aplicación preferente de la Constitución.

Además, otro argumento a favor de esta posición, radica en que de nada serviría pactar tratados internacionales para luego incumplirlos unilateralmente, argumentando la aplicación preferente del ordenamiento jurídico interno, en lugar de liberarse de las obligaciones del referido pacto mediante la vía natural, como es, la denuncia.

7 Sobre el tema ya nos pronunciamos en: Gustavo A. Amoni Reverón, “La audiencia de casación penal telemática en el Derecho Comparado. Parte II”. *Derecho Informático*, México: Popocatepetl editores, 2016; “La audiencia de casación penal telemática en el Derecho Comparado”, *Fodertics 5.0*, España, 2016 (en imprenta); “Posibles soluciones a problemas de la audiencia de casación penal telemática”, *Revista Derecho y Tecnología* (Nº 16), Venezuela: Universidad Católica del Táchira, 2015; “La audiencia de casación penal telemática en Venezuela”, *Fodertics 4.0: Estudios sobre nuevas tecnologías y justicia*, España: Comares, 2015; “Límites constitucionales a la audiencia telemática en el proceso penal venezolano”, *Revista de Derecho, comunicaciones y nuevas tecnologías* (Nº 12), julio-diciembre, Colombia: Universidad de Los Andes, 2014.

8 Artículo 391. La extradición se rige por las normas de este Título, los tratados convenios y acuerdos internacionales suscritos por la República.

9 Se utiliza el verbo “recordar” ya que aún a falta de esta previsión la norma fundamental es de aplicación preferente sobre la base de lo consagrado en los artículos 7, 334, 335 y la disposición derogatoria única de la Constitución.

Cuando la República Bolivariana de Venezuela dicta una ley aprobatoria de un tratado internacional, cumpliendo con todo el proceso de formación de las leyes, y además, con el requisito para que adquiriera vigencia, como es el canje o el depósito del instrumento legal, según el caso, constituiría un desconocimiento frontal a los compromisos internacionales, pretender modificar el tratado con base en normas de rango legal, alegando que se trata de leyes posteriores e incluso orgánicas, y por ello, aplicables con preferencia a la ley especial en materia de extradición en la que se erigen los tratados internacionales.

Distinto es el caso de la Constitución, que se aplica aún en contra de las previsiones internacionales. Esto se justifica por ser la norma de mayor grado dentro del ordenamiento jurídico, lo que la hace primar sobre cualquier otra, salvo las que ella misma establezca, como sucede con lo estipulado en el artículo 23¹⁰ en materia de derechos humanos.

Un aspecto importante, que trae como consecuencia la conclusión anterior, es que el procedimiento de extradición pasiva, de ampliación de la extradición o de reextradición, que se produce cuando la persona a extraditar estuviere en la República Bolivariana de Venezuela, en el primer caso, o fue trasladada desde Venezuela a otro país y estando allá se requiere autorización para juzgarla por delitos que no fueron solicitados o para extraditarla a un tercer país, respectivamente, es que, aun cuando en el eventual tratado internacional que existiere, se hubiere omitido la celebración de una audiencia, o incluso, si se negare expresamente, ella tendría que realizarse porque así lo impone la Constitución.

Se afirma que la audiencia solo aplicaría para el caso de extradición pasiva, ampliación de la extradición o reextradición, porque en la primera hipótesis, Venezuela es quien decidirá si priva de libertad a una persona y la traslada, aun en contra de su voluntad, al Estado requirente, y en las dos modalidades restantes, la persona hubiera tenido la ocasión de expresar su opinión ante la Sala de Casación Penal, para ejercer su derecho a ser oída, si aún estuviese en el país.

Este derecho también pudiera garantizarse si se presenta ante un tribunal en el país donde se encontrare, como ocurrió en el caso resuelto con la sentencia bajo análisis o mejor aún, mediante el uso de un sistema de comunicación audiovisual, telemático, bi o multidireccional, en tiempo real, como la telepresencia o la videoconferencia, según expresó la Sala en dicho fallo y lo recogió luego en la Resolución 2016-001.

Pero, si se tratare de un procedimiento de extradición activa, entendiendo que en el país solo se decidirá si procede requerir la extradición a otra nación, para juzgarlo o aplicarle una pena por estar fugado, será el Estado requerido el

¹⁰ “Los tratados, pactos y convenciones relativos a derechos humanos, suscritos y ratificados por Venezuela, tienen jerarquía constitucional y prevalecen en el orden interno, en la medida en que contengan normas sobre su goce y ejercicio más favorables a las establecidas en esta Constitución y en las leyes de la República, y son de aplicación inmediata y directa por los tribunales y demás órganos del Poder Público”.

que decidirá, según su ordenamiento jurídico, si celebrará o no una audiencia para que la persona solicitada en extradición pueda expresarse al respecto; y en todo caso, si la pretensión de extradición es para ser procesado, el ciudadano tendrá la oportunidad de asistir a las audiencias correspondientes, y si fuera para cumplir una pena, es porque ya fue oportunamente escuchado con las garantías debidas.

De hecho, lo expuesto también aplicaría si el tratado internacional regulare solo los requisitos de procedencia y no un procedimiento especial de extradición, ya que, por aplicación del DLCOPP, en los supuestos de extradición pasiva, reextradición y ampliación de la extradición, también debería efectuarse una audiencia pública, pero en este caso de conformidad con lo previsto en el artículo 390 *eiusdem* y no solo por aplicación directa de la Constitución.

2.2. El objeto de la audiencia de extradición

Otro aspecto que también justificaba la audiencia telemática de extradición, aunque para la fecha no estaba regulada, radica en que sería jurídicamente válida, independientemente de que su objeto fuera establecer hechos o debatir derechos.

En el primer caso, porque los postulados de la intermediación son posibles de este modo¹¹ y en el segundo, porque tratándose de un debate jurídico, la intermediación deviene dispensable.

Sin embargo, parece oportuno fijar el alcance de la discusión que pudiera abarcar la audiencia de extradición para lo cual debe revisarse el ordenamiento jurídico, partiendo desde la Constitución.

2.2.1. Constitución de la República Bolivariana de Venezuela

De acuerdo al numeral 3 del artículo 49:

Toda persona tiene derecho a ser oída en cualquier clase de proceso, con las debidas garantías y dentro del plazo razonable determinado legalmente, por un tribunal competente, independiente e imparcial establecido con anterioridad. Quien no hable castellano o no pueda comunicarse de manera verbal, tiene derecho a un intérprete.

Este derecho solo hace necesario el uso de un sentido: el oído, ningún otro; sin embargo, tal interpretación literal luce insuficiente para garantizar el derecho a la defensa. Según la experiencia, el intercambio de mensajes no se da solo por la vía verbal-auditiva sino que hay un lenguaje no-verbal que completa el

¹¹ Sobre el tema nos pronunciamos en: “El uso de la videoconferencia en cumplimiento del principio de intermediación procesal”. *Revista IUS* (Nº 31), México: Instituto de Ciencias Jurídicas de Puebla, 2013.

sistema comunicacional¹². De ahí que no bastaría la comunicación telefónica del imputado con los miembros del tribunal para estimar satisfecho este derecho “a ser oído”, donde indiscutiblemente, estaría siendo oído.

El derecho constitucional referido, interpretado a favor del imputado, puede entenderse, en su máximo nivel, como la facultad de exigir ser presentado, de modo físico tangible, ante un tribunal, para exponer lo que la persona juzgada estimare pertinente.

De esta norma no se desprende que tenga un contenido específico, sino que admite que pudiera tratarse de una discusión sobre los hechos o sobre derecho; por tanto, deberá revisarse el ordenamiento jurídico de rango infraconstitucional, que siguiendo el orden de las fuentes indicado con anterioridad, corresponde en primer lugar a los tratados internacionales, a fin de precisar si se exige una audiencia y cuál deberá ser su contenido.

En este sentido, se verificarán primero algunos tratados bilaterales y luego, otros multilaterales, para precisar si tales instrumentos le asignan determinado contenido a la audiencia de extradición.

2.2.2. Convenios bilaterales

2.2.2.1. Ley Aprobatoria del Convenio de Extradición entre el Gobierno de la República Bolivariana de Venezuela y el Gobierno de la República Francesa (2012).

Aplicado en la sentencia que se está analizando, tampoco prevé la celebración de una audiencia de extradición, salvo para el caso de reextradición. En esta oportunidad será necesaria “... *un acta en la cual la persona reclamada declare si acepta la reextradición o si se opone a ella*”.

Se entiende que esa acta recogerá las actuaciones que se realicen ante un tribunal y que la declaración no será vinculante para la procedencia de la pretensión, sino que se refiere a una oportunidad para que el requerido exponga lo que desee, de modo que el órgano jurisdiccional pueda decidir conociendo su criterio.

Además, el numeral 2 del artículo III del convenio refiere que no se concederá la extradición cuando persiga fines discriminatorios o pudiera ser sometida a trato cruel, inhumano o degradante, lo cual deberá probarse, siendo ajustado a derecho la contradicción probatoria en audiencia.

Así mismo, si se discutiere la identidad o nacionalidad (artículo V) del detenido y del solicitado en extradición, así como su nacionalidad.

¹² Al respecto, ver: Allan Pease y Barbara Pease, *El lenguaje del cuerpo, cómo interpretar a los demás a través de sus gestos*. (Murillo, I. Trad.) Amat., Barcelona, 2006; y Gonzalo Musitu et al. *Psicología de la comunicación humana*. Lumen, Buenos Aires, 1993

2.2.2.2. Tratado de Extradición celebrado entre los Estados Unidos de América y los Estados Unidos de Venezuela (1922¹³).

Se fijan requisitos de procedencia de la pretensión de extradición mas no se prevé una audiencia; no obstante, el artículo IX prescribe que *“Los gastos de... interrogación... del acusado serán abonados por el Gobierno que haya presentado la demanda de extradición”*, de donde se concluye que la persona solicitada en extradición deberá ser presentada ante un órgano jurisdiccional para responder a las preguntas que se estimen pertinentes a efectos de la tramitación del procedimiento de extradición.

Esta norma, en concordancia con el numeral 3 del artículo 49 constitucional y con el artículo 390 COPP, imponen que se celebre una audiencia de extradición.

La intervención del solicitado no limita la sentencia de la Sala de Casación Penal quien declarará la procedencia de la pretensión atendiendo a la verificación de las exigencias del convenio.

En este caso también se trata de una audiencia donde se discutirá el derecho, aunque pueda haber la misma discusión fáctica que se daría al amparo de los tratados anteriores.

2.2.2.3. Tratado de Extradición entre la República de Venezuela y el Reino de España (1990).

“Las partes contratantes se obligan, según las reglas y condiciones establecidas en los artículos siguientes...” a tramitar las pretensiones de extradición. Así inicia este pacto internacional, donde se advierte de modo diáfano que el procedimiento de extradición está regulado, por las disposiciones del presente instrumento jurídico y no por el derecho interno de cada Estado.

Por tal razón, visto que en el texto revisado no se incorpora una audiencia, aun así se celebrará con base en la Constitución y en el COPP. En ella se verificará la procedencia de la extradición, de modo que pudiera darse un debate sobre hechos en caso de discutirse si la *“...solicitud de extradición fue presentada con la finalidad de perseguir o castigar a la persona reclamada en razón de su raza, religión, nacionalidad u opiniones políticas o bien que la situación de aquella pueda ser agravada por estos motivos”*.

Como excepción a lo expuesto, en el tratado se exige una audiencia para que la autoridad judicial competente le informe de sus derechos, personalmente, al sujeto que consintiere, por escrito, su extradición.

¹³ (Aprobación legislativa: 12 de junio de 1922. Ratificación Ejecutiva: 15 de febrero de 1923.- Canje de ratificaciones: en Caracas, el 14 de abril de 1923).

2.2.3. Tratados multilaterales

2.2.3.1. Código de Derecho Internacional Privado o Código de Bustamante (1928).

No prevé una audiencia de extradición sino una serie de requisitos cuyo cumplimiento deriva en la procedencia de la pretensión extraditoria.

Por esta razón, los procesos de extradición que se tramiten bajo la regulación de este tratado multilateral, se rigen por las disposiciones constitucionales y el procedimiento del DLCOPP, conforme al cual, se debe celebrar una audiencia en la que se escucharán los argumentos que el Ministerio Público, los representantes del Estado requirente, el defensor y el acusado planteen a favor o en contra de la pretensión.

Se trata de debatir si se cumple o no con los requisitos pactados en el tratado internacional, lo que significa que se trata de una discusión jurídica; en la cual, igualmente pudiera haber contradicción sobre hechos inherentes a la procedencia de la pretensión, como se verá luego que pudiera suceder respecto de la nacionalidad e identidad de la persona requerida.

2.2.3.2. Convención Interamericana de Extradición (1981):

Establece la improcedencia de la pretensión en seis supuestos, donde pudiera ser necesaria la intermediación para debatir acerca de si el delito por el cual se requiere la extradición, es un delito común perseguido con una finalidad política o se tratare de una persecución discriminatoria o por la que peligrare la vida del solicitante¹⁴.

Otro argumento para sustentar la eventual discusión fáctica de la audiencia de extradición viene de la mano del artículo 16, que estatuye que la persona reclamada gozará en el Estado requerido de todos los derechos y garantías que concede la legislación de dicho Estado. En Venezuela, esto

¹⁴ “La extradición no es procedente; 1. Cuando el reclamado haya cumplido la pena correspondiente o haya sido amnistiado, indultado o beneficiado con la gracia por el delito que motivo la solicitud de extradición, o cuando haya sido absuelto o se haya sobreseído definitivamente a su favor por el mismo delito; 2. Cuando esté prescrita la acción penal o la pena, sea de conformidad con la legislación del Estado requirente o con la del Estado requerido, con anterioridad a la presentación de la solicitud de extradición; 3. Cuando el reclamado haya sido juzgado o condenado o vaya a ser juzgado ante un tribunal de excepción o ad hoc en el Estado requirente; 4. Cuando con arreglo a la calificación del Estado requerido se trate de delitos políticos, o de delitos conexos o de delitos comunes perseguidos con una finalidad política. El Estado requerido puede decidir que la circunstancia que la víctima del hecho punible de que se trata ejerciera funciones políticas no justifica por sí sola que dicho delito será calificado como político; 5. Cuando de las circunstancias del caso pueda inferirse que media propósito persecutorio por consideraciones de raza, religión o nacionalidad, o que la situación de la persona corra el riesgo de verse agravada por alguno de tales motivos; 6. Con respecto a los delitos que en el Estado requerido no puedan perseguirse de oficio, a no ser que hubiese querrela, denuncia o acusación de parte legítima”.

abarcaría el derecho a la audiencia judicial, que por tener rango constitucional, aun en caso de ausencia de esta disposición, seguiría formando parte del elenco de derecho de la persona solicitada en extradición, ampliación de la extradición o reextradición, presentada a Venezuela.

En la audiencia, como se expresó con anterioridad, se debatirán los argumentos de derecho sobre la procedencia o no de la pretensión extraditoria, pero también pudieran fijarse los hechos expresados, por lo que la importancia del principio de inmediación aumentará o disminuirá según el tópico en discusión.

Esta situación se hace más evidente cuando se trata del procedimiento de extradición simplificada, previsto en el artículo 21. En este caso, un Estado podrá conceder la extradición sin proceder con las diligencias formales de extradición siempre que no estuviere prohibido por la ley y la persona requerida accediere “... *por escrito y de manera irrevocable a su extradición después de haber sido informada por un juez u otra autoridad competente acerca de sus derechos a un procedimiento formal y de la protección que éste le brinda*”.

En este supuesto especial, la audiencia de extradición tiene por objeto que la Sala de Casación Penal le informe acerca de su derecho a un procedimiento formal de extradición y de la protección que este le brinda, luego de la cual, deberá manifestar por escrito estar dispuesto a ser extraditado.

De modo que el procedimiento de extradición simplificada incorpora una audiencia donde el solicitado podrá exponer, bien sea que consiente en su extradición, lo cual deberá manifestar por escrito, o que no desea ser extraditado, pasando entonces al procedimiento ordinario donde, incluso su negativa no es óbice para su extradición.

El aspecto relevante en este sentido se encuentra en que debe garantizarse que la audiencia del sujeto cuya extradición se pretende le permita al juzgador percibir ampliamente, desde la perspectiva sensorial, la manifestación de voluntad del solicitado, cuya aceptación o no del procedimiento simplificado, genera consecuencias diversas, para lo cual se requiere la mayor posibilidad valorativa por parte de los integrantes de la Sala de Casación Penal.

2.2.3.3. Convenio sobre Extradición (1911)

Este instrumento internacional prevé el compromiso de los Estados parte, de tramitar las pretensiones de extradición “...*de acuerdo con lo que se estipula en este Acuerdo*...”, donde tampoco establece la realización de una audiencia para que la persona solicitada tenga la oportunidad de expresar su punto de vista. Al igual que en los textos jurídicos anteriores, se fijan determinados requisitos de procedencia, cuya verificación le impone al Estado requerido el deber de extraditar.

En lo que corresponde a la audiencia, la falta de previsión relativa su celebración y de un procedimiento, en los casos que corresponda la aplicación de esta normativa, se deberá efectuar por disposición del DLCOPP (2012) en concordancia con la Constitución.

Ahora, en lo tocante a la posibilidad de discusión fáctica, el artículo IV prevé que *“tampoco se acordará la extradición si la persona contra quien obra la demanda, prueba que ésta se ha hecho con el propósito de juzgarle o castigarle por un delito político o hecho conexo con él”*, actividad probatoria que debería efectuarse en una audiencia pública, más aún, por tratarse de un procedimiento en única instancia.

2.2.4. Ordenamiento jurídico interno vigente para la fecha de emisión del fallo

2.2.4.1. Decreto con Rango, Valor y Fuerza de Ley del Código Orgánico Procesal Penal (2012).

El **artículo 390 prescribe** el procedimiento a seguir en caso de extradición, ante la ausencia de previsión procedimental en el tratado correspondiente. Con ocasión de la pretensión de extradición pasiva, el texto adjetivo penal incorpora una audiencia a la que concurrirán el Ministerio Público, la persona requerida en extradición, su defensor y el representante del gobierno requirente o su apoderado judicial, quienes expondrán sus alegatos. Concluida la audiencia, el Tribunal Supremo de Justicia decidirá, comprobando los requisitos de procedencia previstos en el tratado, o en su defecto, en otros tratados suscritos y ratificados por la República, en el ordenamiento jurídico interno o incluso, en el principio de reciprocidad.

La audiencia responde al principio de oralidad, y es la ocasión para que los interesados expongan verbalmente sus consideraciones sobre la pretensión extraditoria. La normativa no impide la incorporación de alegatos diferentes a los expresados en la pretensión de extradición.

La importancia de esta audiencia, radica, desde la óptica del solicitado, en servir de oportunidad para ser escuchado por los magistrados que integran la Sala. Desde el punto de vista de los demás intervinientes, esta es el momento para debatir, de forma verbal, sobre la procedencia de la pretensión extranjera.

En esta audiencia, no se indica si se debatirán hechos o derechos; y tampoco se prevé que la Sala de Casación Penal quedará limitada por la manifestación de voluntad del solicitado. Por tanto, visto que se trata de una oportunidad para escuchar los alegatos de los intervinientes, se concluye que se trata de una discusión de derecho, en la pudiera darse discusión sobre hechos del solicitado, donde se valorarán los argumentos con base en los requisitos de procedencia que se encuentran en los tratados internacionales,

por ser las normas donde se especifican los requisitos de procedencia de la extradición.

2.2.4.2. Código Penal

Se trata de la publicación jurídica de menor rango en el orden de las fuentes del derecho enumeradas. En su artículo 6 se estatuye que:

La extradición de un extranjero por delitos comunes no podrá acordarse sino por la autoridad competente, de conformidad con los tramites y requisitos establecidos al efecto por los Tratados Internacionales suscritos por Venezuela y que estén en vigor y, a falta de estos, por las leyes venezolanas.

El artículo reafirma el orden de las fuentes jurídicas de la extradición que se repite en el DLCOPP, colocando en primer lugar los tratados internacionales y solo en caso de ausencia, la normativa de derecho interna.

La regulación aludida no solo se refiere al fondo, o requisitos de procedencia, sino también al procedimiento a seguir, pues resulta lógico que si los Estados pactaron un procedimiento especial para tramitar la extradición entre ellos, se utilice este y no el que los Estados establezcan unilateralmente mediante otra norma aunque posea rango superior, salvo que se trate de la Constitución. En este último caso, primaria la norma fundamental.

2.2.5. Recapitulación

El procedimiento de extradición deberá ubicarse, primero, en los tratados internacionales suscritos y ratificados por la República. Si lo prevé, pero omite incorporar una audiencia, se entenderá incluida por disposición constitucional; pero si el tratado solo regular el fondo, entonces deberá usarse el procedimiento del DLCOPP, norma supletoria en el ámbito de la extradición, en concordancia con la CRBV.

Esta actividad procesal está orientada, en principio, a servir de debate jurídico, pero ciertos aspectos fácticos como la identidad del sujeto requerido, el posible carácter político que realmente se esconde tras la solicitud presentada sobre la base de la perpetración de un delito común, o la eventual sanción fundada en motivos discriminatorios, requieren ser alegados y probados en una audiencia pública, donde hubiere la oportunidad de controlar la prueba pertinente.

En definitiva, las normas legales revisadas no establecen el debate probatorio en la audiencia de extradición; sin embargo, su interpretación constitucionalizada pareciera imponerlo, cambiando el procedimiento que se viene aplicando hasta el momento, lo cual será esbozado brevemente en el epígrafe siguiente.

2.3. La extradición en la jurisprudencia de la Sala de Casación Penal

En la práctica judicial, las audiencias de extradición sirven para el debate sobre los alegatos de las partes¹⁵. En esta oportunidad, es común que el representante del Ministerio Público consigne escrito con la opinión de la Fiscalía General de la República¹⁶ así como también el defensor público¹⁷.

Luego, “... la Sala de Casación Penal, procederá a verificar la documentación aportada por el Estado requirente, a fin de constatar si la misma cumple con los requerimientos, tanto de forma como de fondo, para la procedencia de la solicitud de extradición presentada...”¹⁸.

En su mayoría, se trata de elementos comprobables por la Sala que no ameritan control probatorio en audiencia; sin embargo, se ha detectado en las decisiones de la Sala de Casación Penal que hay al menos dos afirmaciones que pueden ser contradichas y que requieren el establecimiento de hechos, para lo que resultaría indispensable el debate probatorio, conforme lo consagra el artículo 49 (numerales 1 y 3) de la Constitución. Se trata de los casos en los que se plantean dudas sobre la identidad y la nacionalidad del sujeto requerido. En lo que respecta al derecho al debate oral sobre las pruebas, los numerales 1 y 3 del artículo constitucional citado, prevén:

El debido proceso se aplicará a todas las actuaciones judiciales y administrativas; en consecuencia: 1. La defensa y la asistencia jurídica son derechos inviolables en todo estado y grado de la investigación y del proceso. Toda persona tiene derecho a ser notificada de los cargos por los cuales se le investiga, de acceder a las pruebas y de disponer del tiempo y de los medios adecuados para ejercer su defensa. Serán nulas las pruebas obtenidas mediante violación del debido proceso. Toda persona declarada culpable tiene derecho a recurrir del fallo, con las excepciones establecidas en esta Constitución y la ley... 3. Toda persona tiene derecho a ser oída en cualquier clase de proceso, con las debidas garantías y dentro del plazo razonable determinado legalmente, por un tribunal competente, independiente e imparcial establecido con anterioridad. Quien no hable castellano o no pueda comunicarse de manera verbal, tiene derecho a un intérprete.

El derecho a la defensa y más específicamente el derecho de acceso a las pruebas, aunado al derecho a ser oído por el tribunal competente no solo significa

¹⁵ Sentencias de la Sala de Casación Penal números 270 del quince (15) de julio de 2016, 329 del nueve (9) de agosto de 2016 y 341 del diez (10) de agosto de 2016.

¹⁶ Sentencias de la Sala de Casación Penal números 113 del dos (2) de marzo de 2016 y 119 del siete (7) de marzo de 2016.

¹⁷ Sentencia de la Sala de Casación Penal número 316 del cinco (5) de agosto de 2016 y 329 del nueve (9) de agosto de 2016.

¹⁸ Sentencia de la Sala de Casación Penal número 317 del cinco (5) de agosto de 2016.

el derecho a conocer las pruebas, sino el derecho a controlarla, para lo que resulta indispensable el debate ante la autoridad, judicial o administrativa, competente.

Partiendo de tal premisa, si en el proceso extraditorio se discute si la persona detenida es la misma que está siendo requerida en extradición, deberá permitirse el control de la prueba incorporada como resultado de la actividad investigativa, asegurándose que la persona detenida sea la misma solicitada¹⁹.

A modo de ejemplo, en la sentencia N° 204 del 31 de mayo de 2016, la Sala de Casación Penal decidió:

... una vez practicada una serie de diligencias se logró constatar tanto con la copia certificada consignada por el abogado..., con la notificación roja emanada de la oficina Interpol de Madrid, con la consulta de datos del ciudadano..., de la consignación que realizara la ciudadana... de la cédula de identidad, constancia de residencia, pasaporte, registro de nacimiento y registro de matrimonio y, del oficio procedente del Servicio Administrativo de Identificación Migración y Extranjería (SAIME) donde se indica que del chequeo realizado a las impresiones que aparecen al reverso de la cédula de identidad colombiana nro... del ciudadano BLADIMIR VILLEGAS CARO, portador de la cédula de identidad V..., no corresponden a datos e impresiones dactilares del ciudadano VILLEGAS PACHECO BLADIMIR.

En este sentido, se concluye que la persona que actualmente se encuentra detenida no es el ciudadano BLADIMIR JOSÉ VILLEGAS PACHECO, de nacionalidad venezolana, titular de la cédula de identidad nro..., sino BLADIMIR VILLEGAS CARO, cédula de ciudadanía colombiana nro..., no siendo la persona requerida por el Reino de España mediante la alerta roja internacional A-4362/7-2013 de fecha doce (12) de julio de 2013.

Durante el proceso, la Sala de Casación Penal recibió algunas pruebas, ordenó la evacuación de otras y al final, estableció que la persona detenida no era el sujeto requerido, por lo que no pudo declarar la procedencia o improcedencia

¹⁹ En la sentencia número 250 del 1° de julio de 2016 puede advertirse la labor investigativa previa a la audiencia de presentación del ciudadano detenido por presumirse que se trataba de una persona requerida en extradición por Canadá. En ese caso, el ciudadano Mario Pacheco, Sub Comisario Jefe de la División de Investigaciones de INTERPOL, Porlamar, del Cuerpo de Investigaciones Científicas, Penales y Criminalísticas, solicitó al Jefe del Área Técnica Policial: 1) una comparación dactiloscópica a las impresiones decadactilares reflejadas en la notificación roja alfanumérica con las reseñas realizadas por su Despacho al ciudadano detenido; 2) que se practicaran los registros fotográficos, y reseñas tipo PD-1, al ciudadano detenido; 3) que se realizara una experticia de reconocimiento legal a los siguientes documentos: a) una (1) licencia de conducir de tercer grado, a nombre de O'Neill Pirela, James Alexander; b) un (1) documento de identidad venezolano, con los datos: V-22.540.931; apellidos: O'Neill Pirela; nombres: James Alexander; c) una (1) tarjeta de débito número 627534000015101422, emitida por el Banco Exterior; d) una (1) tarjeta de crédito "visa" emitida por el Banco Provincial, número 5406280145674442, a nombre de James Alexander O'Neill Pirela. De este modo, habría pruebas para determinar que el ciudadano detenido era el mismo requerido.

de la pretensión de extradición dado que no se había ubicado a la persona solicitada sino que se había detenido, erróneamente, a otro sujeto.

En este caso se concluyó que la persona detenida no era quien estaba siendo requerida, pero si el Estado requirente hubiera querido controlar la experticia de la que surgió tal conclusión, o promover una experticia para contradecir aquella, hubiera tenido que admitirse y someterse a debate ambas pruebas, puesto que así lo impone la Constitución.

Es decir, se trata de un claro ejemplo una discusión fáctica que deberá decidir la Sala de Casación Penal y para la cual, en una interpretación constitucionalizada del Código Orgánico Procesal Penal, luce necesario el debate probatorio en audiencia.

En lo que concierne a la determinación de la nacionalidad, que es el otro aspecto sobre el cual se advirtió en la jurisprudencia revisada que pudiera darse un debate probatorio ante la autoridad competente, debe destacarse que en el supuesto específico de existir dudas sobre si la cédula de identidad se obtuvo de modo fraudulento, debe enfatizarse que la competencia para verificar la validez de dicho documento es administrativa y solo, posteriormente, sometida a control jurisdiccional, tal como lo prevé el artículo 24 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de Identificación (DLOI) de 2014²⁰.

De ello se da cuenta en la sentencia número 497 del 11 de diciembre de 2012, para cuyo pronunciamiento la Sala solicitó a la Fiscal General de la República que efectuara “...los trámites y actuaciones pertinentes para dilucidar la identidad y ciudadanía del ciudadano... solicitado en extradición... y, una vez concluidas tales actuaciones, sean enviados los resultados a esta Sala (con carácter de urgencia) para proceder a dictar la decisión correspondiente”.

En esa misma oportunidad, la Sala pidió información al Servicio Administrativo de Identificación, Migración y Extranjería (SAIME), el cual respondió que “... se dictó Decisión Administrativa para anular el referido serial [número de cédula de identidad de la persona solicitada en extradición] por haber sido obtenido por el ciudadano... [requerido en extradición] con fraude a ley... ya que su verdadera identidad es PARADA SUS CARLOS I JAIR, de nacionalidad colombiana”. (corchetes añadidos).

En este caso, la Sala concluyó que el solicitado no poseía la nacionalidad venezolana sino que era nacional, por nacimiento, de la República de Colombia, y visto que había obtenido el documento de identidad de modo fraudulento, le fueron anulados la cédula de identidad y el pasaporte venezolanos, lo que la llevó a declarar procedente la extradición pasiva solicitada²¹.

²⁰ G.O. N° 6.155 E. del 19 de noviembre de 2014.

²¹ Igualmente se advierte la tramitación del procedimiento administrativo para determinar la validez de la cédula de identidad, en la sentencia número 480 del 6 de diciembre de 2012, donde se deja constancia de la existencia del oficio No. 513 del once (11) de agosto de 2011, emitido por el Director General del Servicio Administrativo de Identificación, Migración y Extranjería del

Destaca en este supuesto, que el derecho a probar y a controlar la prueba se fija en sede administrativa, por ser un órgano de la Administración Pública el que está conociendo el procedimiento.

No obstante, en situaciones como esta debe prestarse atención a que el acto dictado por el SAIME pudiera ser recurrido en sede administrativa y luego accionado ante los órganos jurisdiccionales, así como también acordarse, en ambos casos, la suspensión temporal de efectos del acto que anuló la cédula de identidad, por lo que el procedimiento extraditorio pudiera verse alargado, generando un problema grave cuando el ciudadano requerido estuviere sometido a privación cautelar de libertad.

Otro supuesto donde la actividad probatoria, y por tanto el control de la prueba se da fuera del proceso de extradición ocurre en caso de pérdida de la nacionalidad venezolana por naturalización.

De acuerdo a los artículos 36 y 37 de la Ley de Nacionalidad y Ciudadanía de 2004 (LNC), la revocatoria de la nacionalidad venezolana por naturalización solo podrá hacerse mediante sentencia judicial, dictada en primera instancia, por los órganos jurisdiccionales en lo Contencioso Administrativo, y en alzada, por la Sala Política Administrativa del Tribunal Supremo de Justicia²².

Como consecuencia de ello, si se pusiera en duda la nacionalidad por naturalización de un ciudadano solicitado en extradición pasiva, habría que resolver tal situación ante los tribunales con competencia contencioso-administrativa, para dilucidar, posteriormente, dicha pretensión.

Resumiendo lo expuesto, la jurisprudencia de la Sala de Casación Penal mantiene la celebración de la audiencia de extradición, tal como lo prevé el

Ministerio del Poder Popular para las Relaciones Interiores y Justicia, mediante el cual se informa que "... se...[abrió] investigación la cual arrojó que el número de cédula de identidad que porta este ciudadano, no corresponde, siendo el verdadero titular de esta cédula el [ciudadano] Yurbin Noel Montilla Guanipa, por lo que se ha determinado que la cédula presentada por el accionante es falsa. Como consecuencia de ello se ha iniciado procedimiento sancionatorio de EXPULSIÓN...". En este caso, no bastó con la declaratoria de falsedad de la cédula de identidad del ciudadano requerido, tramitada por la Administración Pública, sino que también se inició el procedimiento administrativo de expulsión del territorio, el cual no se completó en virtud del proceso jurisdiccional de extradición llevado por la Sala de Casación Penal.

22 En la sentencia número 480, emanada de la Sala de Casación Penal, el 6 de diciembre de 2012, se evidencia la tramitación de la revocatoria de la carta de naturaleza de un ciudadano mediante procedimiento administrativo mas no en un proceso jurisdiccional: "Así, la Sala recibió comunicación No. 1378 del veintiocho (28) de noviembre de 2012, suscrita por el ciudadano FABRICIO ANTONIO PÉREZ MORÓN, Director General del Servicio Administrativo de Identificación, Migración y Extranjería del Ministerio del Poder Popular para las Relaciones Interiores y Justicia, donde manifestó: 'en atención al proceso de extradición pasiva en contra del ciudadano VERÁSTEGUI HERNÁNDEZ JORGE LUIS, de nacionalidad peruana... cumplo con informarle que... se determinó que el referido ciudadano, obtuvo la nacionalidad venezolana por naturalización con prescindencia total de los requisitos establecidos... De igual manera, se hace de su conocimiento que se ordenó el inicio de revocatoria de la Carta de Naturaleza... que fue publicada en Gaceta Oficial'...".

DLCOPP, como la oportunidad para exponer alegatos, pero en ella no se produce la evacuación probatoria con el control y debate que según se está proponiendo, lucen necesarios para el establecimiento de los hechos.

Lo que se plantea en este análisis constituye una propuesta interpretativa de la norma del DLCOPP que prevé la audiencia pública en materia de extradición y que implicaría una perspectiva distinta a la que ha desarrollado la Sala de Casación Penal, en especial, cuando hubiera dudas sobre la identidad y nacionalidad del sujeto requerido.

De lo expresado, deriva que la audiencia de extradición debiera permitir el control de la prueba en audiencia cuando se discuta la identidad de un sujeto, correspondiendo a los tribunales contencioso-administrativos, resolver las pretensiones contra los actos declarativos de la nulidad de la cédula de identidad.

Tal propuesta no se aplicaría en caso de nulidad de carta de naturaleza ya que ello sería el resultado de la intervención jurisdiccional, por lo que la autoridad de la cosa juzgada impediría a la Sala volver sobre tal aspecto.

2.4. La audiencia de extradición en la práctica de la Sala de Casación Penal

Resulta útil conocer qué ocurre en la práctica durante la celebración de una audiencia de extradición para precisar si es posible realizar dichos actos por medios electrónicos, o sustituir alguno por otra actuación que permita cumplir los mismos fines, como quedó regulado en la Resolución 2016-001.

Para ello, los días 18 y 25 de julio de 2016, así como también en fecha 4 y 10 de octubre del mismo año, se asistió a seis audiencias de extradición, para verificar en directo la actividad desempeñada por los intervinientes, lo cual se describe a continuación:

2.4.1. Procedimiento de ingreso a la Sala de Casación Penal

El día al fijado para la celebración de la audiencia de extradición, arriban el detenido con sus respectivos custodios, si fuere el caso, el o los defensores privados o en su defecto el defensor público designado para actuar ante la Sala de Casación Penal, los representantes del Estado requirente, el fiscal del Ministerio Público designado para actuar ante la Sala de Casación Penal y en su caso, el intérprete público.

Los funcionarios auxiliares de la Secretaría de la Sala de Casación Penal verifican la identidad y notifican a la Secretaria de la Sala acerca de las personas ausentes, para elaborar el acta de audiencia.

El procedimiento de verificación de información consiste en requerir la cédula de identidad, y el carnet de inscripción en el Instituto de Previsión Social del Abogado, o el documento que acredita la condición con la que actúan, bien sea

intérprete público, representante consular o diplomático, o algún otro, de acuerdo al caso.

Posteriormente, el alguacil le comunica al funcionario de seguridad que se encuentra en la entrada de la Sala de Audiencias que puede permitir el ingreso a la Sala de los intervinientes, previa solicitud de los equipos de telefonía celular, los cuales serán custodiados y devueltos al retirarse de la Sala de Audiencias.

Una vez dentro, la Secretaría de la Sala se acerca a los defensores, a la víctima y al intérprete, informándoles del procedimiento a seguir. Explica el tiempo y los turnos de intervención, manifestándole a la víctima que puede hablar libremente y que el objeto de la audiencia no es establecer los hechos delictivos por los que está siendo solicitado ni su responsabilidad penal, sino que se trata de discutir la procedencia de la pretensión de extradición extranjera.

Luego de esto, la Secretaría autoriza el acceso al público para dar inicio a la audiencia, aspecto que se abordará luego de comentar, brevemente, la distribución de la sala de audiencias.

2.4.2. Topografía de la sala de audiencias de la Sala de Casación Penal

Los representantes del Estado requirente, cuya ausencia no detiene el curso de la audiencia, se ubican a la derecha del estrado (y a la izquierda del público, sentado frente al estrado, área donde se encuentran los Magistrados integrantes de la Sala de Casación Penal). A su derecha se encuentra el representante del Ministerio Público (sentados de espalda al público), el o los defensores, el requerido y el intérprete, cuando corresponda (igualmente de espalda a público y de frente a los magistrados).

En el sector localizado a la izquierda de los magistrados (y a la derecha del público, exactamente frente a los representantes del Estado requirente, en el otro extremo de la sala de audiencias), se incorpora un funcionario de la Guardia Nacional, la Secretaría de la Sala, un auxiliar de Secretaría y el alguacil.

En la entrada de la Sala se encuentra un funcionario de seguridad del Tribunal Supremo de Justicia, y en la entrada de la antesala de la Sala de Audiencias, donde se encuentra la sala de espera, se ubica otro, con los intervinientes de las otras audiencias fijadas para ese mismo día²³.

Todos los participantes cuentan con mesas, en las que se incorporan tantas sillas individuales como fueren necesarias, equipadas con un solo micrófono movable, y dotadas de una botella de agua pequeña por persona.

La sala de audiencias dispone de diez filas de asientos ascendentes para el público, quien se ubica frente a los magistrados, separados por un espacio plano y ligeramente más bajo donde se encuentra el resto de las personas anteriormente identificadas, con excepción de los magistrados sentados en el estrado, situado en un nivel más alto.

²³ Normalmente las audiencias de extradición se realizan los días lunes, iniciando a las 10:30 am y culminando a las 12:30, aproximadamente.

El estrado cuenta con un micrófono para cada magistrado e igualmente está dotado de una botella de agua mineral por persona.

2.4.3. Desarrollo de la audiencia de extradición pasiva

En una audiencia presenciada el 4 de octubre de 2016 y en tres audiencias del 10 de octubre del mismo año, se pudo verificar que una vez ingresadas las partes y el público, la Secretaria avisa con un gesto afirmativo al funcionario que se encuentra en la sala de deliberación, situada detrás del estrado, quien hace contacto visual con ella desde una compuerta de la que dispone la pared que separa ambas áreas.

Los magistrados ingresan, y en ese momento, el alguacil se levanta e indica a los presentes que deben ponerse de pie. Luego de haberse sentado los juzgadores, el alguacil comunica en clara, alta e inteligible voz: “pueden tomar asiento”.

El magistrado presidente saluda y le indica a la ciudadana Secretaria que sirva leer el acta que contiene los motivos de la audiencia.

A continuación, toma la palabra la Secretaria de la Sala dando lectura al acta donde se deja constancia de los presentes y ausentes, y los motivos de la audiencia.

Luego, el Magistrado Presidente le otorga el derecho de palabra a los representantes del Estado requirente (quienes no acudieron en los seis casos presenciados), al Ministerio Público, al defensor, repitiendo el ciclo salvo que manifestaren no desear intervenir nuevamente, o no hacerlo en ningún momento en el caso de los representantes del Estado requirente, quienes pudieran acudir, únicamente en calidad de observadores.

Por último tiene el derecho palabra la persona solicitada quien expone lo que desee.

En todo momento, el intérprete público se encuentra al lado del solicitado para traducirle en caso de requerirlo. Sobre ello, las audiencias comentadas transcurrieron sin necesidad de intervención del intérprete, a quien se observó antes, y en una ocasión durante la audiencia preguntarle al solicitado si estaba entendiendo el debate que se producía en español, a lo cual asintieron con la cabeza.

Durante la intervención de los representantes del Ministerio Público y de la Defensa Pública, expresaron que consignarían documento contentivo de sus alegatos, y así lo hicieron, para lo cual se acercó el alguacil hasta sus asientos, recibiendo y entregando a la Secretaria de la Sala de Casación Penal.

Asimismo, es importante destacar que a fin de asegurar el cumplimiento de los 10 minutos que tienen las partes para la primera intervención y de los 5 minutos que disponen para la segunda (réplica y contrarréplica), lo cual les es advertido por el Magistrado Presidente cuando les concede el derecho de palabra, el alguacil, por indicación de la Secretaria de la Sala, quien lleva el control del

tiempo previa autorización del presidente de la Sala, se acerca hasta el interviniente y le muestra un cartel donde se lee que le restan dos minutos, luego un minuto y finalmente que se le acabó el tiempo de su exposición, según corresponda. Aunque tales situaciones no ocurrieron en las audiencias descritas, ha sido observada en otras audiencias de extradición por parte de quien desarrolla este análisis.

Un aspecto que es importante destacar es que todas las intervenciones se realizan, normalmente, mediante micrófono, y en caso de separarse del mismo sin usar un tono de voz adecuado al tamaño del área, el alguacil se dirige hacia el participante, acercándose y invitándolo a incrementar el volumen, situación que puede realizar *motu proprio* el alguacil o por indicación de la Secretaría o de alguno de los magistrados, como se ha observado en otras audiencias a las que se tuvo la ocasión de asistir.

Luego de la exposición del solicitado, el Magistrado Presidente, en las tres audiencias verificadas, indicó que la Sala de Casación Penal se acogería al lapso de quince días, previsto en el artículo 390 del Código Orgánico Procesal Penal, para decidir.

Los magistrados, se levantan al tiempo que el alguacil exclama: “de pie, por favor”, y en cuanto se retiran, se permite salir de la Sala, no sin antes recordarle a los intervinientes que deben acudir a la Secretaría a leer y firmar el acta.

2.5. La participación telemática en la audiencia de extradición

La importancia del auto número 74 emitido el 19 de febrero de 2016 por la Sala de Casación radica en ser el primero donde la Sala de Casación Penal reconoce la posibilidad de acceder a la sede del Tribunal Supremo de Justicia por medios telemáticos y no solo de la forma que se viene realizando: acudiendo en presencia tangible hasta la sede judicial.

Este fallo constituye un antecedente directo de la resolución 2016-001, por la que se amplían los modos de participación, incluyendo el uso de la telemática, dejando atrás el hecho de que la única opción para participar en la audiencia de extradición, era acudir hasta el edificio del máximo tribunal del país.

La decisión, por sus características, facilita el acceso a la justicia tanto en los procedimientos de extradición como en los de casación, ya que en ambos casos, la jurisprudencia ha sostenido que la discusión se limita a asuntos de derecho y el ritual a seguir durante la audiencia es el mismo.

Incluso, el hecho de pronunciarse a favor de la posibilidad de inmediación, respalda la propuesta que sostenemos de admitir el debate probatorio en el procedimiento de única instancia en el que se configura la extradición, así como el uso de la videoconferencia que viene utilizándose para la declaración de expertos durante la fase de juicio.

Ya para aquel momento, las razones para considerar que es válido participar en la audiencia de extradición y de casación penal mediante el uso de la telemática son de tipo normativo, jurisprudencial y fáctico.

2.5.1. Fundamentos normativos para admitir la audiencia de extradición telemática antes de la Resolución 2016-001 de la Sala de Casación Penal

En el ámbito de la normativa de derecho, la Constitución prevé el derecho de acceso a la justicia, en el encabezado del artículo 26, el cual reitera imponiendo al Estado el deber de garantizar una justicia accesible, en el único aparte del mismo artículo, tal insistencia redundante en que las personas debemos contar con la posibilidad de valernos de la administración de justicia, para tutelar nuestros intereses jurídicos, en la mayor medida posible y de manera progresiva²⁴.

Para acceder a la justicia deben existir las condiciones para llegar hasta el lugar donde se encuentre quien imparta la justicia. Esto se puede lograr trasladándose de modo tangible hasta ese lugar, y adicionalmente, mediante el uso de las tecnologías de información y comunicación.

Permitir el acceso telemático a la justicia significa ampliar las opciones que actualmente están limitadas a hacerlo «en carne y hueso» a la sede jurisdiccional, creando, sin eliminar aquella, la oportunidad de decidir ejercer el derecho a la defensa por los medios tradicionales o telemáticos, siempre que permitan cumplir con tal fin.

De hecho, la Constitución consagra el deber del Estado de reconocer el interés público de la tecnología, la innovación y sus aplicaciones, así como los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo del país²⁵.

Una aplicación de la tecnología es facilitar el acceso a la justicia, de modo que si se puede lograr tal cometido usando las TIC, sería inconstitucional omitirlo.

Tan importante resulta la evolución de las instituciones mediante el uso de la tecnología que su estudio es obligatorio en los centros educativos del país²⁶, vinculando aún más la ciencia del Derecho con las aplicaciones de las TIC, como lo reconoció la Sala en la decisión bajo análisis.

En lo concerniente al ámbito infraconstitucional, tanto los tratados internacionales referidos como el ordenamiento jurídico interno, eran suficientemente amplios como para admitir la inclusión de las TIC en el desarrollo de la audiencia de extradición, dado que no se excluía esta posibilidad, ni si quiera por inferencia de las disposiciones jurídicas.

En el Código de Derecho Internacional Privado o Código de Bustamante (1928) la audiencia se rige por la Constitución y DLCOPP. En cuanto a la

²⁴ Artículo 19 de la CRBV.

²⁵ Artículo 110 CRBV.

²⁶ Artículo 108 CRBV.

Constitución, el uso de las TIC resulta compatible con el derecho a ser oído, el cual no impide el uso de la telemática, ya que una persona puede hacerse escuchar y ser percibida, por el juzgador, claramente, usando la telepresencia, videoconferencia o alguna otra tecnología audiovisual, bi o multidireccional, en tiempo real con calidad suficiente para tal fin, como lo previó luego la sentencia..

No obstante, entendiendo que es un derecho fundamental, su interpretación a favor del procesado supone que si este quisiera ser presentado directamente de forma tangible ante el juez, o magistrados de la Sala de Casación Penal, en el caso que se estudia, ello limitaría el uso de la telemática, no pudiendo obligarlo a ello.

Respecto del DLCOPP, el artículo 390 prevé que concurrirán los convocados a la audiencia a exponer sus alegatos. Actuación que entonces era posible mediante el uso de la telemática, la cual permite presentarse, de forma electrónica, ante los magistrados de la Sala de Casación Penal para exponer sus alegatos, pues se trata del uso de los sentidos de la vista y el oído, que la tecnología posibilita usar a distancia.

En lo que concierne al Convenio sobre Extradición (1911) y a la Convención Interamericana de Extradición (1981), la audiencia se desarrolla por la misma regulación, por lo que le serían aplicables los comentarios previos. Sin embargo, en el último texto está prevista la extradición simplificada, donde hay una norma especial que prevé que la persona haya sido informada por un juez u otra autoridad competente acerca de sus derechos a un procedimiento formal y de la protección que este le brinda. Nuevamente se trata del uso de dos sentidos: el oído y la vista, que tal como se expresó antes, pueden satisfacerse por conducto de la telemática.

Por su parte, en los convenios bilaterales revisados, el Tratado de Extradición entre la Republica de Venezuela y el Reino de España (1990), al igual que la Convención Interamericana de Extradición, guarda silencio sobre la celebración de una audiencia, por lo que se aplicaría la CRBV y el DLCOPP; así mismo, cuenta con una extradición simplificada en los mismos términos de la Convención Interamericana de Extradición, por lo que la conclusión previa le resulta aplicable.

En la Ley Aprobatoria del Convenio de Extradición entre el Gobierno de la República Bolivariana de Venezuela y el Gobierno de la República Francesa (2012), al faltar la previsión de una audiencia de extradición se aplica la CRBV y el DLCOPP, con las consecuencias sobre el uso de las TIC ya comentadas.

Lo mismo sucede con el Tratado de Extradición celebrado entre los Estados Unidos de América y los Estados Unidos de Venezuela (1922²⁷) donde tampoco se fija una audiencia; pero en este caso se alude a unos “...*gastos de... interrogación... del acusado...*”. De nuevo se trata del uso de la vista y del

27 (Aprobación legislativa: 12 de junio de 1922. Ratificación Ejecutiva: 15 de febrero de 1923.- Canje de ratificaciones: en Caracas, el 14 de abril de 1923).

oído para el cual la telemática ha encontrado soluciones válidas desde el punto de vista de la calidad necesaria para servir de opción a la presencia tangible.

Atendiendo al ordenamiento jurídico interno, la regulación prevista en el Decreto con Rango, Valor y Fuerza de Ley del Código Orgánico Procesal Penal (2012), como se ha comentado, no prevé la audiencia telemática pero su redacción tampoco permite concluir que la prohíbe, situación que también se advierte en el Código Penal y que permitió dictar la Resolución 2016-001 de la Sala de Casación Penal.

2.5.2. Fundamentos jurisprudenciales que llevaron a admitir la audiencia de extradición telemática

La Sala de Casación Penal ha tramitado la audiencia de casación penal como una oportunidad para tenga lugar una discusión de derecho, mas no se ha valido de ella para discutir el material probatorio y establecer hechos controvertidos como la identidad de la persona detenida o si la extradición se está usando para fines por los cuales sería improcedente.

Esta modalidad, que se ajusta plenamente a una interpretación literal de la CRBV y del DLCOPP, favorece el uso de la telemática en la audiencia, ya que tratándose de una exposición de argumentos y un debate sobre estos, no habría razones para excluir el uso de las TIC para que los interesados pudieran intervenir en la audiencia de extradición.

Incluso, si la Sala admitiera la interpretación propuesta de admitir el control de la prueba y usar la audiencia de extradición para generar un debate sobre los hechos que requieran establecerse, como la identidad del solicitado, o si la extradición es solicitada por un delito común pero en realidad con ella se pretende perseguir delitos políticos o ejercer actos discriminatorios, el uso de la telemática aún sería posible puesto que la intermediación necesaria para ello puede lograrse con la tecnología existente.

Así lo asentó la Sala Constitucional en 2001²⁸ y lo reiteró la Sala de Casación Penal en el auto que se está comentando cuando afirmó expresamente que las TIC posibilitan cumplir con los tres aspectos de la inmediación, como son: 1. La proximidad entre el juez y el sujeto u objeto de la evaluación para poder percibir el contenido y la forma de la declaración o el objeto que se examina; 2. La ausencia de intermediarios subjetivos y objetivos; y, 3. La bilateralidad o bidireccionalidad que le permite al juzgador comunicarse con el o los sujetos que intervienen en la audiencia interrogando, limitando, aclarando y conduciendo el debate o la declaración, según el caso.

Decisión que viene a respaldar lo que se ha decidido en el país en tribunales de protección de niños y adolescentes, desde 2006²⁹; en la propia Sala

28 <http://historico.tsj.gob.ve/decisiones/scon/agosto/1571-220801-01-1274%20.htm>

29 <http://zuliala.tsj.gob.ve/decisiones/2006/abril/521-27-6460-480.html>

Constitucional, desde 2011³⁰; y en tribunales penales desde 2014³¹; al admitir el uso de la videoconferencia para lograr la intervención telemática de quienes fueren convocados.

2.5.3. Fundamentos fácticos para admitir la audiencia de extradición telemática

Las actuaciones que se realizan en las audiencias de extradición ya podían producirse mediante la telemática, desde tal momento. Desde la identificación de los intervinientes hasta el control de las intervenciones, pasando por lo principal que es exposición de los alegatos ante los magistrados, así como también que los juzgadores puedan interrogarlos, son actos que por limitarse al uso de la vista y del oído no encuentran obstáculos insalvables en su ejercicio telemático.

En este sentido, a propósito de las audiencias presenciadas, se realizan actos jurídicos previos, concomitantes y posteriores cuya posibilidad de materialización telemática derivará en la eficacia del uso de las TIC para su celebración.

Como actos previos, están la identificación de las participantes, la ubicación de los participantes en la sala de audiencias y la explicación del procedimiento por parte de la Secretaria de la Sala.

La identificación se realiza observando documentos, lo cual, igualmente puede realizarse a distancia, por parte de los mismos funcionarios que lo hacen en la Sala de Casación Penal o bien por parte del funcionario judicial, administrativo, diplomático o consular autorizado para ello, bien sea desde una sede nacional oficial o desde recinto público o privado desde donde el Magistrado Presidente, como director del debate, autorizare la participación, siempre que el lugar tenga el orden y silencio requerido para guardar las solemnidades de la audiencia.

El hecho de no haber otro método de identificación en la sala de audiencias más allá de ver la cédula de identidad y el carnet que corresponda según el caso permiten concluir que la identificación también es posible usando medios telemáticos, aspecto que regula la Resolución 2016-001 en un título autónomo sobre la identificación de los intervinientes..

En este punto es importante considerar que si la declaración se hiciera desde recinto no oficial venezolano, está la opción de enviar uno o más funcionarios para comprobar la identidad del interviniente y velar porque actúe con respeto a la autoridad, que es la opción guatemalteca por la que se optó en la Resolución 2016-001.

Si declarare desde un centro de privación de libertad, podrá disponer de hasta tres defensores distribuidos entre el lugar donde estuviere y la sala de audiencias, como lo prevé la normativa italiana.

³⁰ <http://historico.tsj.gob.ve/decisiones/scon/enero/01-27111-2011-09-0912.html>

³¹ <http://historico.tsj.gob.ve/informacion/notasdeprensa/notasdeprensa.asp?codigo=12148>

Si se tratare de defensores públicos, el defensor que intervendrá en la audiencia será el designado para actuar ante la Sala mientras que el que estuviere presente en el lugar desde donde se emitieren los alegatos velará por garantizar que la intervención se hiciera sin coacción sobre el interviniente, aspecto que también recogió la Resolución 2016-001 justo antes de finalizar el año.

En segundo lugar, antes de la audiencia el solicitado pudiera querer conversar con su defensor. Ello también es posible dotando de un medio de comunicación privado al solicitado y a su defensor, como un teléfono celular, si ambos estuvieren separados, y así lo establece la tantas veces aludida resolución 2016-001.

En caso de ser necesario un intérprete, este deberá colocarse junto al solicitado, o en su defecto, contar con un medio de comunicación con el defensor y el solicitado, como pudiera ser otro teléfono celular, para traducirles a ambos, y así lo estatuye la Resolución.

El tercer acto que tiene lugar antes de iniciar la audiencia consiste en ubicar a las personas en la Sala, lo cual, se sustituiría por ajustar las cámaras, si fuere necesario, para que el interviniente por medios telemáticos tuviere una visión de los magistrados, de las otras partes así como también, de la sala de audiencias en general. Igualmente, sería necesaria la instalación de los televisores o proyectores con calidad y tamaño suficientes para aproximarse a las características de la presencia tangible en la mayor medida posible.

Todo ello sería posible puesto que las dimensiones de la sala de audiencias son suficientes para introducir los equipos necesarios a fin de celebrar la audiencia de extradición por medios telemáticos.

Por último, antes de iniciar, la Secretaria de la Sala explica el procedimiento de la audiencia y su contenido. Dado que se trata de instrucciones verbales, las mismas se pueden dictar por medios telemáticos.

Luego de los actos previos, corresponde practicar la audiencia. En ella, las potestades de ordenación por parte del Magistrado Presidente pueden cumplirse en un entorno electrónico, asignando la palabra a cada interviniente según el orden pertinente.

Así mismo, el aviso que hace el alguacil sobre el tiempo restante para intervenir en la audiencia así como su terminación, pueden cumplirse con un sistema informático especial o simplemente mostrando el cartel a la cámara. Incluso, en el caso extremo de desorden por parte de un participante a distancia desde fuera de un recinto oficial venezolano, siempre está la opción de desconectar la voz o el video, como si se retirare de la audiencia a quien perturbare su desarrollo.

Durante la audiencia también es común que los representantes del Ministerio Público y de la Defensoría Pública consignen escritos. Si estuvieren fuera de la Sala de Audiencias podrán remitirlos posteriormente o hacerlo por mensajería electrónica, dotados de firma electrónica certificada, de los cual dará cuenta en el expediente la Secretaria de la Sala.

Ahora bien, resulta oportuno destacar que las intervenciones, prácticamente en su totalidad, se generan mediante el micrófono que forma parte del sistema de sonido instalado en la sala de audiencias, por tanto, en lo que respecta al sentido del oído, sería igual percibir la declaración en presencia tangible o cibernética, ya que en ambas circunstancias, los magistrados no percibirán las intervenciones de viva voz.

En lo tocante a la percepción visual, la calidad de video y el tamaño de la imagen debe ser lo suficientemente apta para permitir a los magistrados percibir el lenguaje no verbal de quien interviene, y no solo su prosodia³² y contenido. Así quedó demostrado en la reunión celebrada el 17 de enero de 2017 para la discusión de la Resolución 2016-001 donde los Magistrados de la Sala de Casación Penal, los Defensores y Fiscales ante la Sala tuvieron la oportunidad de conversar sobre dicho instrumento de derecho y presenciaron una breve intervención de quien escribe, en su condición de abogado adscrito a la Sala de Casación Penal, valiéndose para ello de un sistema de videoconferencia, con lo cual se mostraron las ventajas y desventajas de la tecnología.

Por último, con posterioridad a la audiencia los participantes deberán firmar el acta que documenta lo ocurrido. En este caso, el artículo 153 COPP prevé que si alguno de los presentes no quisiera o no pudiere firmar, por ejemplo por estar participando por medios telemáticos, la Secretaria de la Sala dejará constancia de ello, con total validez de dicha acta, situación que prevé la Resolución en estos términos.

En síntesis, no se consiguen aspectos de la audiencia de extradición que las TIC no puedan suplir, por el contrario, se erigen en un mecanismo útil para ampliar las posibilidades de acceso a la justicia y de allí la importancia de este auto que se está comentando, que sirvió para resolver, en un caso concreto, aspectos prácticos sobre la participación telemática en las audiencias de extradición.

Antes de concluir, hay un aspecto más que fue abordado en el auto 74/2016 que resulta impretermitible enfatizar: el uso de firma electrónica para transmitir mensajes de datos entre Estados, con lo cual se cumple con la normativa legal sobre mensajes de datos y firmas electrónicas de 2001.

3. Conclusión

El auto 74/2016 de la Sala de Casación Penal constituye una decisión vital en el ámbito procesal telemático, ya que aumenta el ejercicio del derecho de acceso a las sedes judiciales cuando incorpora la opción de usar la videoconferencia para celebrar la audiencia de reextradición, como se planteó en esta ocasión, donde el ciudadano estaba fuera del país.

³² Sobre el tema, ver: Elsa Mora Gallardo y Rosa Amelia Asuaje: *El canto de la palabra: una iniciación al estudio de la prosodia*, Mérida. Universidad de Los Andes, 2009.

A pesar de no haberse dado la participación telemática del solicitado en la audiencia, en el auto se sentaron las bases para afianzar a la videoconferencia como un sistema válido para ejercer el derecho fundamental a la defensa en el proceso penal dando origen, antes de finalizar el año, a la reiterada Resolución 2016-001 del 12 de diciembre de 2016.

En efecto, y manteniéndonos en el ámbito de competencia de la Sala de Casación, los argumentos del citado órgano juzgador pueden extrapolarse a otros sujetos procesales, en las audiencias que se convoquen a propósito de los procedimientos de extradición pasiva, ampliación de la extradición y de casación penal, incluso, si la persona que participará estuviere en el país, que fue uno de los principios que guió la Resolución.

Para ello, la Sala se apoyó en la normativa constitucional y legal, así como en la jurisprudencia, donde se ha previsto el uso de las TIC para facilitar la tutela de los intereses jurídicos mediante el ejercicio de la función jurisdiccional.

En el auto analizado, bien sea que se trate de una audiencia para debatir aspectos de derecho, como se ha entendido que sucede en materia de casación y extradición, o de hecho, como pudiera ocurrir en los casos excepcionales de incorporación de prueba testimonial en la audiencia de casación previstos en el DLCOPP o en caso de acogerse la propuesta planteada en este escrito en materia de extradición, resultaría factible la intervención procesal telemática, y así se previó en la Resolución sobre participación telemática de diciembre de 2016.

Siendo una discusión de derecho, solo se requiere conocer los argumentos a considerar y tener la oportunidad de pronunciarse sobre ellos, así como de repetir el ciclo tantas veces como se permita, que en el caso de la audiencia de extradición, e igualmente en la casación, se da una sola vez; es decir, las partes exponen sus alegatos, luego hay una oportunidad de réplica por parte del representante del país requirente y del Ministerio Público, de contrarréplica para el defensor, finalizando con la intervención del solicitado, si lo desearan, en cada caso.

Todas esas actuaciones son ejecutables por medio de la telepresencia, la videoconferencia o algún otro sistema telemático, audiovisual, bi o multidireccional, en tiempo real, puesto que los sujetos procesales pueden verse, hablarse, oírse, preguntarse y responderse como si estuvieran en el mismo lugar, siempre que la calidad audiovisual y de conexión, así lo permitieren, términos que hicieron eco en la normativa sublegal ya estudiada.

Por otra parte, si se diere una discusión fáctica, la participación telemática también sería válida puesto que los elementos de la inmediación son ejecutables por este medio, descartándose, por ahora, el uso del sentido del tacto, el gusto y el olfato, los cuales, no juegan un papel importante, salvo algún caso especial para el que ello fuera necesario.

Asimismo, la normativa jurídica constitucional, internacional y legal que rigen en el ámbito de la extradición no excluyen el uso de la telemática para intervenir

en la audiencia de extradición³³, sino que de su redacción se admite cualquier forma de participación en la que fuera posible ejercer cabalmente el derecho a la defensa, mediante el cumplimiento de las garantías que apareja el debido proceso previsto en la Constitución y la ley.

Lo anterior, contaba con respaldo jurisprudencial, incluso para el establecimiento de los hechos, de ahí que su uso hubiera resultado ajustado a derecho, y con mayor razón, en los casos de discusiones jurídicas como la que viene ocurriendo en el ámbito de la extradición, situación que pudiera cambiar conforme se sugiere considerar en este análisis.

En definitiva, el auto 74/2016 de la Sala de Casación Penal se erige en el antecedente medular de la Resolución 2016-001 al impulsar la corriente que desde entonces ha cobrado fuerza en la jurisprudencia patria, y que ya es un hecho en muchos sectores del derecho comparado, como es, permitir el acceso a los órganos jurisdiccionales mediante el uso de TIC, que la Sala continuó extendiendo a todas las audiencias que se celebren ante ella, actualizando conforme a los adelantos del siglo XXI, el derecho de acceso a la justicia que consagra la Constitución de la República Bolivariana de Venezuela.

³³ Elemento que la Resolución 2016-00001 previó expresamente con posterioridad.

Valor probatorio de los mensajes de datos y firmas electrónicas en la Sala Civil del Tribunal Supremo de Justicia venezolano

Alejandra de los A. León Parada*

SUMARIO: I. Introducción. II. Análisis de la prueba electrónica y su procedimiento de evacuación. III. Características que deben contener las pruebas electrónicas. IV. Conclusiones.

Resumen

El presente trabajo lleva por objetivo investigar respecto a los avances de la Sala de Casación Civil del Tribunal Supremo de Justicia, en relación a los correos y mensajes electrónicos.

Para ello el método empleado será la investigación en textos de distintos autores de diferentes nacionalidades, utilizando el método comparativo de sus estudios con el Decreto Ley de Mensajes de Datos y Firmas Electrónicas de fecha 10 de febrero de 2001, y su aplicación en la jurisprudencia nacional, y con ello precisar la aplicación de ésta por los particulares en sus distintas relaciones diarias.

De esta manera, concluiremos que efectivamente se está aplicando la citada ley y verificando los distintos avances que se vienen advirtiendo en el proceso civil, en actuaciones tales como la pruebas, pues el derecho debe ir frente a los desarrollos tecnológicos que experimenta la sociedad venezolana.

Palabras Claves: Correo electrónico. Mensajes de datos. Actos procesales.

Abstract

The present work aims to investigate the progress of the Civil Cassation Chamber of the Supreme Court of Justice, in relation to e-mails and emails.

Recibido: 21/1/2017 • Aceptado: 10/2/2017

* Abogado, especialista en Derecho Procesal y Tributario. Caracas. alejaleon32@hotmail.com

The method used will be the research in texts of different authors of different Nationalities, using the comparative method of their studies with the Decree Law of Electronic Data and Signatures dated February 10, 2001, and its application in national jurisprudence, and with it the application of this by the individuals in their different daily relations.

In this way, we will conclude that the aforementioned law is effectively being applied and verifying the different advances that are being noticed in the civil process, in actions such as the proofs, since the law must go against the technological developments experienced by Venezuelan society.

Keywords: E-mail. Data Messages. Procedural acts.

I. Introducción

De forma paralela a las sucesivas aplicaciones de la tecnología informática en distintos sectores de la experiencia jurídica se ha producido, en los países avanzados, una progresiva promulgación de normas jurídicas que tienen como objeto inmediato reglamentar diferentes aspectos de la informática.

En proporción a ello se está creando la Informática jurídica, es decir, un conjunto de aplicaciones de la informática en el ámbito del Derecho, en la que la informática pasará a ser instrumento del mismo. En virtud de ello se empieza a forjar en nuestros días una nueva disciplina jurídica, *el Derecho de la informática o Derecho informático*, que debe englobar el conjunto de leyes, normas y principios encaminados a disciplinar la utilización de la informática y la telemática en el que la informática es el objeto del derecho¹.

En ese sentido y, con la utilización de las nuevas tecnologías en las relaciones comerciales, en nuestra sociedad, se va abandonando el soporte de los mensajes sobre papel, se le reemplaza por soportes magnéticos o electrónicos. Sin temor a dudas, la evolución social, así como las actividades y las interrelaciones comerciales, han llevado a una globalización mundial, que necesariamente requiere de la regularización de las mismas por parte del Derecho, así como éste regula las relaciones de las conductas humanas se requiere y es necesario que pase a controlar o reglar tales actividades que de antemano ya están siendo relajadas en nuestra realidad.

Así pues, en relación con este tipo de conductas entre los miembros de una sociedad que está regulada por el Derecho, por una Constitución que emerge el requerimiento de que estas conductas que son llevadas a cabo por medios electrónicos e informáticos deban ser normadas por el mismo, conductas que se ven reflejadas en contratos electrónicos, facturas electrónicas, mensajes,

¹ Jaime ROUANET MOSCARDÓ. *Valor Probatorio Procesal del Documento Electrónico*. Mérida. Pág. 163-164.

acuerdos e incluso pudieran darse transacciones, todas estas figuras jurídicas regladas por nuestras leyes patrias, pero que su soporte está o debe estar plasmados en papel y en esta nueva era tecnológica ya están siendo plasmados en medios informáticos, y es en ese sentido que en virtud de nuestros postulados constitucionales previstos en los artículos 26 y 257 de la Constitución de la República Bolivariana de Venezuela, tales como la tutela judicial efectiva, en protección a derechos colectivos y difusos, y con el objeto de que el derecho vaya de la mano con la evolución socio informativa.

Es en ese aspecto en el que surge la inquietud de hacer un análisis jurisprudencial de la evolución que ha venido desarrollando la Sala Civil del Tribunal Supremo de Justicia de la República Bolivariana de Venezuela, respecto de algunos documentos de carácter electrónico a la luz de la Ley sobre Mensajes de Datos y Firmas Electrónicas.

II. Análisis de la prueba electrónica y su procedimiento de evacuación

Los puntos esenciales de los cuales parte la jurisprudencia de la Sala Casación Civil para precisar el análisis probatorio de los documentos referidos a correos electrónicos en esencia es el artículo 4 del Decreto Ley de Mensajes de Datos y Firmas Electrónicas de fecha 10 de febrero de 2001², el cual textualmente expresa:

Artículo 4: Los Mensajes de Datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos, sin perjuicio de lo establecido en la primera parte del artículo 6 de este Decreto-Ley. Su promoción, control, contradicción y evacuación como medio de prueba se realizará conforme a lo previsto para las pruebas libres en el Código de Procedimiento Civil.

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.

Al respecto de la citada norma se desprende, 1) los mensajes que han sido formados y transmitidos por medios electrónicos, éstos tendrán la misma eficacia probatoria de los documentos escritos, 2) su promoción, control, contradicción y evacuación deberá regirse por lo que el legislador ha establecido para las pruebas libres en el Código de Procedimiento Civil.

Así, por ejemplo, para tramitar la impugnación de la prueba libre promovida, corresponderá al juez emplear analógicamente las reglas previstas en el referido texto adjetivo sobre medios de prueba semejantes, o implementar los mecanismos

² Decreto Ley de Mensajes de Datos y Firmas Electrónicas. Ley Sobre Mensajes de Datos y Firmas Electrónicas; Gaceta Oficial de la República Bolivariana de Venezuela, N° 37.076 del 13 de diciembre de 2000.

que considere idóneos en orden a establecer la credibilidad del documento electrónico.

En concordancia con la previsión anterior, los artículos 7 y 395 del Código de Procedimiento Civil, que enuncian el principio de libertad probatoria, son del siguiente tenor:

Artículo 7.-Los actos procesales se realizarán en la forma prevista en este Código y en las leyes especiales. Cuando la ley no señale la forma para la realización de algún acto, serán admitidas todas aquellas que el juez considere idóneas para lograr los fines del mismo».

Artículo 395.-Son medios de prueba admisibles en juicio aquellos que determina el Código Civil, el presente Código y otras leyes de la República. Pueden también las partes valerse de cualquier otro medio de prueba no prohibido expresamente por la ley, y que consideren conducente a la demostración de sus pretensiones. Estos medios se promoverán y evacuarán aplicando por analogía las disposiciones relativas a los medios de pruebas semejantes contemplados en el Código Civil, y en su defecto, en la forma que señale el Juez...

En sentencia de la Sala Casación Civil, N° 472 de fecha 19 de julio de 2005, expediente N°2003-000685, caso: Producciones 8 ½, C.A. contra el Banco Mercantil (Banco Universal)³, en relación con la interpretación de las citadas normas precisó lo siguiente:

El citado artículo 7 faculta al juez para la creación de formas cuando para la realización del acto nada haya establecido el legislador al respecto. Y, el artículo 395 consagra el principio de libertad de los medios de prueba, conforme al cual es insostenible restringir la admisibilidad del medio probatorio seleccionado por las partes, con excepción de aquellos legalmente prohibidos o que resulten inconducentes para la demostración de sus pretensiones; con lo cual le otorgó a las partes la posibilidad de promover pruebas distintas a aquellas reguladas en el ordenamiento jurídico. Sin embargo, dispone en el único aparte del referido artículo que el juez debe crear la forma para la tramitación de la prueba libre en aquellos casos en los que el medio de prueba libre no pueda ser promovido ni evacuado conforme a los medios de prueba tradicionales.

En efecto, en la Exposición de Motivos de nuestro vigente Código de Procedimiento Civil⁴, fue expresado:

..Se consideró conveniente introducir una ampliación de estos medios de prueba, con el propósito que el debate probatorio sea lo más amplio posible, y

³ www.tsj.gob.ve/decisiones/scc/julio

⁴ Código de Procedimiento Civil. Publicada en Gaceta Oficial de la República de Venezuela N° 4.209 (Extraordinaria) del 18 de septiembre de 1990.

de que las partes puedan aportar cualquier otro medio no regulado expresamente por el Código Civil, haciendo posible de este modo una mejor apreciación de los hechos por parte del juez, y la posibilidad de una decisión basada en la verdad real y no solamente formal, procurándose además, de ese modo, una justicia más eficaz.

Se asocia así el Proyecto en este punto, a la corriente doctrinal y positiva, hoy dominante en esta materia, de permitir el uso de medios de prueba no regulados expresamente en el Código Civil, pero que son aptos, sin embargo, para contribuir al triunfo de la verdad y a la justicia de la decisión...»⁵.

El autor Jesús Eduardo Cabrera, al referirse a los medios de prueba libres, señala:

...está formado por todos aquellos instrumentos capaces de trasladar hechos al proceso y que no están contemplados en ninguna ley, a ellos se refiere el principio de libertad de medios de pruebas o de libertad de prueba como también se le llama.

(Omissis)

Los medios legales de prueba, generalmente, están regulados por normas que establecen requisitos para su promoción. Si estas normas no se cumplen o se infringen, la proposición del medio es ilegal. Los medios libres, al contrario, por ser creación de las partes, no tienen ni pueden tener, para su promoción, requisitos particulares establecidos en la ley. En principio, la única valla para su admisión por ilegalidad, es que la ley los prohíba expresamente.

(Omissis)

Los medios libres pueden ser o parecidos a los legales, o sin ninguna afinidad con ellos. En el primer caso, quién los promueve debe hacerlo en forma análoga a los medios regulados por la ley. En virtud de lo dispuesto en el artículo 4 del CC, creemos que se puede hacer la promoción de los medios libres, aplicando por analogía, lo dispuesto en las leyes, siempre que el propuesto sea semejante al regulado por éstas a pesar de que el artículo 395 del CPC ordena que se apliquen para la promoción y evacuación de los medios libres, las disposiciones análogas relativas a los medios tradicionales contemplados en el Código Civil.

(Omissis)

La situación es distinta cuando el medio libre ofrecido no es igual, ni en su esencia ni en su forma, al legal, sino parecido, como sería el caso, por ejemplo, de un experimento judicial distinto a la reconstrucción de hechos.

...los medios de prueba libres, ellos deben ser promovidos en el término de promoción; el juez para su evacuación queda facultado para aplicar formas análogas de medios semejantes, o para crear formas si el medio tiene una conexión lejana o carece de ella, con las pruebas tradicionales del CC.

El Juez no va ab initio –antes de la impugnación- a señalar formas análogas o creadas por él para la contradicción, ya que tal proceder no tiene lógica si tomamos en cuenta que ésta sólo procede a instancia de parte, por lo consiguiente, el

⁵ Congreso de la República, Comisión Legislativa, *Exposición de Motivos y Proyecto de Código de Procedimiento Civil*, Imprenta del Congreso de la República, Caracas, 1984, p. 38

Magistrado –salvo muy particulares materias- debe esperar que surja la impugnación ante el medio libre, para regularla según su criterio.

...Hay que distinguir la foto, como reproducción o prueba autónoma, donde el juez analiza la imagen, de la foto ilustrativa, destinada a complementar o aclarar una declaración...

Cuando lo que se produce como medio de prueba independiente, es una foto sin fines ilustrativos hay que distinguir si ella es promovida por las partes, quienes directamente la consignan en autos, o si ella es el resultado de la prueba de reproducciones del Art. 502 CPC. En el primer caso, el promovente tiene la carga de alegar y demostrar su identidad y su credibilidad, mientras que en el segundo, el funcionario debe aportar todo lo concerniente para que las partes puedan ejercer el derecho de defensa...

Los medios meramente representativos, sean ellos documentos o se les asigne otra naturaleza, pueden contener en su cuerpo, o ir acompañados de explicaciones escritas sobre sus circunstancias, tales como autoría, fecha de su confección, identificación de las personas, animales, lugares o cosas que en ellos aparecen, etc. Si las explicaciones escritas son auténticas, no hay problema probatorio alguno, y sólo la impugnación activa funcionará contra ellas; pero si estas no lo son, ellas se comportan como documentos escritos (por formar parte de cuerpos adheribles a los autos, que en lo que respecta a la recepción de la escritura, tienen la misma características que el resto del género), que de atribuirse a la contraparte y serles opuestos formalmente, quedarán sujetos a reconocimientos...

Cuando el medio meramente representativo no ilustra sino que se le trae como un medio autónomo, establecida la identidad y credibilidad del mismo, el Juez lo observa para extraer de él cualquier elemento que permita fijar los hechos controvertidos, así las partes no lo hayan señalado con precisión en su promoción. Detalles de las fotos, de los videos, de las películas cinematográficas, no establecidas por las partes, pero que aparecen en el medio, podrán ser valorados por el Juez, ya que es el medio el que reporta la imagen, que es su contenido al proceso; y es esa imagen la que el sentenciador aprecia. Las reproducciones (Art. 502 CPC), así como las fotos, películas, videos y otros medios semejantes que produzcan las partes estarán sujetas a la apreciación judicial, hasta sus detalles.

Como la identidad y credibilidad del medio meramente representativo, la mayoría de las veces se prueban con testigos, el promovente de la prueba debe ser cuidadoso para no convertir a dicho medio en un aditamento del testimonio, caso en que éste será lo que se aprecia. Por ello en anterior ocasión (1986), alertamos sobre el punto, cuando dijimos: *“Por lo dicho, un gran número de pruebas libres para adquirir eficacia probatoria, no se bastarían a sí mismas, sino que formarán parte de un concurso de medios que las apoyarán y permitirán al Juez conocer su veracidad y relación cierta con la causa”*.

Muchas de estas pruebas requerirán de la ayuda de la prueba testimonial para lograr sus fines, funcionando como un todo inseparable con el testimonio. El medio de prueba libre que se quiere hacer valer, se propone como tal, pero varios de los aspectos relativos a su autenticidad y veracidad se demuestran con testigos, quienes deponen sobre estos hechos y no sobre el fondo del litigio.

Esta situación hace imprescindible que cuando se proponga una prueba libre, se indique expresamente dentro de la promoción de prueba cuales son los testigos que van a deponer sobre su autenticidad y fidelidad...creemos que el promovente –al menos- debe indicar cuáles son los testigos que va a utilizar para probar la autenticidad y fidelidad del medio libre.

...El que promueve tiene la carga de probar la conexión medios-hechos litigiosos y así mismo, de hacer creíble dicha prueba. Para lograr los fines anteriores, el promovente se valdrá de todos los medios posibles y de presunciones...»⁶.

En este orden de ideas, el tratadista Ricardo Henríquez La Roche sostiene:

...La regla general es que cualquier medio probatorio es válido y conducente al nacimiento de la prueba, salvo que esté expresamente prohibido por la ley. Como la ley no puede regularlos a todos por su diversidad o porque su invención y práctica es la posterior a la legislación, deben aplicarse siguiendo la analogía que tengan con los medios probatorios típicos, previstos en el Código Civil y regulados en su modo y oportunidad por la ley adjetiva. La falta de aplicación por analogía de estas reglas da lugar a la irregularidad de la prueba atípica y a su consiguiente ineficacia procesal; siendo incluso denunciante en casación (Art. 320, segundo párrafo)...

Si el juez considera que no hay semejanza entre la prueba libre y el medio probatorio previsto por el Código Civil, o considera que la semejanza es accidental y que la aplicación analógica de las normas sustantivas típicas distorsionaría la esencia y la finalidad de la prueba atípica, así lo motivará en el auto que dicte y procederá a fijar la forma de promoción y de evacuación (o calificar la promoción ya hecha), de acuerdo a lo señalado en la parte final de este artículo 395. De hecho así lo prevé en términos generales –como fundamento de la parte final de esta disposición- artículo 7°...⁷.

En igual sentido, el autor José Pedro Barnola Quintero indica:

...La ampliación del número de medios de prueba admisible al extenderse dicha admisibilidad a medios de prueba consagrados en leyes distintas a las del Código Civil, como ha sido tradicional en este punto. Igualmente se consagra la posibilidad de emplearse en el proceso cualquier otro medio de prueba no prohibido por la ley. En este sentido, reflejo del Código Modelo Iberoamericano de Derecho Procesal, resulta la disposición del artículo 395 del Código de Procedimiento Civil venezolano. Dicha disposición consagra que estos otros medios de prueba se promueven y evacúan aplicando por analogía las disposiciones relativas a los medios de prueba semejantes contemplados en el Código Civil, o atendiendo a la disciplina judicial de las formas procesales, al

⁶ CABRERA, Jesús Eduardo. *Control y Contradicción de la Prueba Legal y Libre*. Editorial Jurídica Alva S.R.L, Caracas, 1998, Tomo I, p. 41, 304-308, Tomo II, p. 121, 140, 143, 146-147.

⁷ HENRÍQUEZ LA ROCHE, Ricardo, *Código de Procedimiento Civil, Tomo III*, Centro de Estudios Jurídicos del Zulía, Caracas, 2000, p. 225-226.

estatuir que en defecto de normas la evacuación se llevará a cabo en la forma que señale el juez...⁸.

Por su parte, el autor Antonio Rosich Sacan, en su obra, "*Impugnación por falsedad del medio de prueba audiovisual*", expresa:

...Los audiovisuales son medios probatorios propios, previstos en el artículo 395 del CPC...

(Omissis)

El audiovisual como medio capaz de captar hechos trasladados a los efectos probatorios, no escapa a la posibilidad de ser alterado en su forma y contenido.

(Omissis)

Podemos definir la falsedad audiovisual como "la falta de conformidad del audiovisual con la realidad» la cual puede referirse al contenido o a la forma.

No basta que un medio de probatorio pueda trasladar los hechos del mundo exterior a un proceso judicial. Se requiere que el medio de prueba se encuentre en capacidad de incorporar debidamente los hechos al proceso para que los mismos cumplan con su función primordial, lo cual no es otra que demostrar la veracidad o falsedad de los hechos controvertidos. El medio de prueba debe, por sí mismo, bastar para que los hechos que trae al juicio (y especialmente la prueba de los hechos) cumplan con la tarea de fijar como ciertos dentro de la mente sentenciadora del juez, su existencia y veracidad.

Para que esta labor de fijación se cumpla se requiere que el medio de prueba contenga en sí dos elementos fundamentales, como son la identidad y la credibilidad del medio, en relación a los hechos del proceso.

(Omissis)

Vigente desde mucho antes de la promulgación del CPC de 1987, la institución de la impugnación en Venezuela ha pasado desapercibida, o tal vez descuidada por gran parte de la doctrina y la jurisprudencia patria. Prueba de ello resulta la persistente confusión que en el foro se observa en relación a este medio de contradicción de las pruebas.

Modernamente la doctrina contemporánea ha distinguido en la institución de la impugnación, como medio de contradicción de las pruebas, dos subtipos claramente definidos. Así la impugnación ha sido desarrollada en relación a la dirección en que se orienta el ataque al medio. Aquella que tiene por objeto la erradicación de medios obtenidos en detrimento de la ley o ilegitimidad por el promovente, ha sido denominada impugnación por ilegitimidad del medio de prueba. Por otro lado, aquella que busca eliminar la eficacia probatoria del medio de prueba por contener falsedades, es conocida como impugnación por falsedad del medio de prueba.

Tramitación de la impugnación por falsedad de la prueba audiovisual.

Hemos destacado anteriormente la especial situación en torno a este novedoso medio de prueba. Corresponde ahora resolver el dilema de la tramitación

8 BARNOLA QUINTERO, José Pedro. *XIX Jornadas Iberoamericana de Derecho Procesal. Derecho Probatorio Nuevas Tendencias*, INVEDEPRO, Caracas, 2004, P. 519-520.

del mecanismo impugnatorio que permita la contradicción del no promovente durante la evacuación de la prueba.

No obstante, tenemos distintas alternativas aplicables al trámite impugnatorio. Debemos consecuentemente explanarlas para adoptar entre ellas la que consideramos más efectiva a los fines de la presente investigación.

Como señalamos en diversas oportunidades, el problema sustancial en torno a la impugnación radica en la ausencia de formas procesales legalmente establecidas. Así el CPC no aporta regulación expresa de los trámites impugnatorios, ni en cuanto a la consagración de la impugnación como medio de contradicción de la prueba, ni la fijación de lapsos ni oportunidades para su tratamiento.

Para solventar esta laguna legal, encontramos una doble salida que el mismo CPC nos plantea. Primeramente el artículo 395 del texto aludido, al referirse a los medios de prueba libre, en su único aparte señala: ...

Vemos, pues, como el propio texto de la norma permite la aplicación analógica de formas legales semejantes contempladas en el CC, en cuanto a la promoción y evacuación de estos medios (lógicamente, incluimos el control y contradicción de la prueba en este enunciado). Asimismo, se faculta expresamente al juez para señalar las formas de tramitación de este tipo de pruebas, en caso de ausencia de formas análogas.

Entonces, el Juez tiene dos salidas claras, por una parte la analogía aplicada por mandato expreso del artículo 395 del CPC en concordancia del artículo 4 del CC; y por la otra, la implementación de formas propias para la tramitación en el proceso de los medios de prueba libres, también recogida en el contenido del artículo 395 del CPC, aunado a la facultad para crear formas legales que le confiere el artículo 7 del mismo texto adjetivo...⁹.

Como puede observarse, la doctrina es conteste al considerar respecto a la tramitación de las pruebas libres que no se asimilan a los medios probatorios tradicionales, estableciendo lo siguiente:

1. El promovente de un medio de prueba libre representativo, esto es, fotografías, películas cinematográficas, audiovisuales, y otras de similar naturaleza, tiene la carga de proporcionar al juez, durante el lapso de promoción de pruebas, aquellos medios probatorios capaces de demostrar la credibilidad e identidad de la prueba libre, lo cual podrá hacer a través de cualquier medio probatorio.

2. El juez en la oportunidad de pronunciarse sobre la admisibilidad de dicha prueba debe hacerlo en conformidad con lo previsto en los artículos 7 y 395 del Código de Procedimiento Civil, establecer la manera en que ésta se sustanciará; y en caso de que el medio de prueba libre sea impugnado, debe implementar en la tramitación la oportunidad y forma en que deba revisarse la credibilidad e

⁹ ROSICH SACAN, Antonio, *Revista de Derecho Probatorio* 8, “Impugnación por Falsedad del Medio de Prueba Audiovisual”, Editorial Jurídica Alva S.R.L., Caracas, 1997, p. 160, 169, 171, 174, 175, 180, 186, 180, 190.

idoneidad de la prueba; pues sólo cumpliendo con esa formalidad por delegación expresa del legislador cumple el proceso su finalidad, que es un instrumento para alcanzar la justicia según lo dispone el artículo 257 de nuestra Carta Magna, al mismo tiempo, se garantiza el debido proceso y derecho de defensa de las partes.

3. Una vez cumplidas estas formalidades, el sentenciador determinará en la sentencia definitiva –previo al establecimiento de los hechos controvertidos–, si quedó demostrada la credibilidad y fidelidad de la prueba libre en cuestión; caso contrario, desestimaré dicha prueba, pues si bien se trata de medios probatorios que no prejuzgan sobre el fondo del litigio, son indispensables para que una vez establecidas dichas circunstancias, el juez pueda establecer con plena libertad los hechos que se desprenden de la prueba conforme al sistema de la sana crítica.

Por consiguiente, la Sala dejó establecido que es obligatorio para los jueces de instancia fijar la forma en que deba tramitarse la contradicción de la prueba libre que no se asemeje a los medios de prueba previstos en el ordenamiento jurídico, pues así lo ordenan los artículos 7 y 395 del Código de Procedimiento Civil; de lo contrario se estaría subvirtiendo la garantía del debido proceso, con la consecuente infracción del derecho de defensa de las partes.

De acuerdo con lo antes expuesto se puede precisar que una vez promovidas las pruebas atinentes a correos electrónicos, en cabeza del juez nace el deber la obligación de precisar el procedimiento necesario para la evacuación de la prueba, y se establece que en caso de impugnación o contradicción de la prueba el juez igualmente está en el deber de precisar el procedimiento de conformidad con lo previsto en los artículos 7 y 395 del Código de Procedimiento Civil.

Ahora bien, una vez precisado el procedimiento de promoción y evacuación de las pruebas electrónicas, es menester fijar los siguientes aspectos:

III. Características que deben contener las pruebas electrónicas a fin de que sean incorporadas al proceso

Al respecto resulta pertinente precisar que el documento electrónico o mensaje de datos es un medio de prueba atípico, cuyo soporte original está contenido en la base de datos de un PC o en el servidor de la empresa y es precisamente sobre esto que versa la prueba.

El TSJ venezolano, en sentencia N° 769, fecha 24 de octubre de 2007, caso: DISTRIBUIDORA INDUSTRIAL DE MATERIALES C.A. (DIMCA), contra ROCKWELL AUTOMATION DE VENEZUELA C.A. Sala de Casación Civil¹⁰), ha determinado que:

10 www.tsj.gob.ve/decisiones/scc/octubre

los documentos electrónicos no pueden ser exhibidos, pues la manera en que son almacenados los datos electrónicos, impide que puedan ser presentados a juicio –por lo menos de manera práctica de fácil acceso–, pues ellos están en la base de datos de un PC o en el servidor de la empresa, razón por la cual se estaría frente a la necesidad de una experticia para verificar la autoría de los documentos que se emitan con tales características y si estos están en poder del adversario, hasta tanto se ponga en funcionamiento la Superintendencia de Servicios de certificación Electrónica-.

Aunque esta fue la opinión del TSJ, es importante aclarar que la Superintendencia de Servicios de Certificación Electrónica, ya estaba en funcionamiento para la fecha de la referida sentencia.

Respecto al documento electrónico como medio de prueba el artículo 7 de la Ley de Mensajes de Datos y Firmas Electrónicas, establece lo siguiente:

...Artículo 7: 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....

De acuerdo con la norma precedentemente transcrita, podemos evidenciar lo que en principio venimos comentando en relación a que los documentos electrónicos no pueden ser exhibidos, pues la manera en que son almacenados impiden que puedan ser presentados en juicio, por ello se desprende la otra característica referida a que es un medio de prueba atípico.

Ahora bien, en virtud de su imposibilidad de ser presentados en juicios, debemos precisar que el documento electrónico como bien hemos demostrado a lo largo de este análisis, ...está previsto en la Ley sobre Mensajes de Datos y Firmas Electrónicas de 2001, y en sentido amplio, 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)¹¹.

También es catalogado 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, o 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 como otro documento que actúa como medio para su traslado al expediente.

¹¹ *Id.*

Por su parte, la Ley de Mensajes de Datos y Firmas Electrónicas considera, en su artículo 2, al documento electrónico o mensaje de datos - lo denomina como “...*toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio...*”.

En ese sentido y en virtud de estas características de los mensajes de datos y firmas electrónicas, de acuerdo con los artículos 2 y 9 del Decreto-ley, que establecen:

Artículo 2: A los efectos del presente Decreto-Ley, se entenderá por:

Firma Electrónica: 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.

Artículo 9: Las partes podrán acordar un procedimiento para establecer cuándo el Mensaje de Datos proviene efectivamente del Emisor. A falta de acuerdo entre las partes, se entenderá que un Mensajes de Datos proviene del Emisor, cuando éste ha sido enviado por:

1. El propio Emisor.
2. Persona autorizada para actuar en nombre del Emisor respecto de ese mensaje.
3. Por un Sistema de Información programado por el Emisor, o bajo su autorización, para que opere automáticamente».

Conforme con las referidas normas, para considerar que el mensaje transmitido con firma electrónica es cierto, es preciso que cuente con el certificado electrónico, definido en el mismo dispositivo como “Mensaje de Datos proporcionado por un Proveedor de Servicios de Certificación que le atribuye certeza y validez a la Firma Electrónica”.

Asimismo, a falta de acuerdo entre las partes, sobre el procedimiento para establecer cuándo el mensaje de datos proviene efectivamente del emisor, se tomará en cuenta cuando éste ha sido enviado por: el propio emisor; la persona autorizada para actuar en nombre del emisor respecto de ese mensaje; por un Sistema de Información programado por el Emisor o bajo su autorización, para que opere automáticamente.

A pesar de que la Sala Civil del TSJ afirmó que la Superintendencia de Servicios de Certificación Electrónica no había sido creada en el caso de la sentencia comentada anteriormente, también declaró que ante la falta de certificación electrónica, los correos electrónicos o mensajes de datos, agregados en formato impreso por la demandada a las actas procesales, deben ser analizados conforme a lo previsto en el único aparte del artículo 4 del Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas, cuyo contenido es del siguiente tenor: “...*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 consecuencia y de acuerdo con la citada ley especial, el valor probatorio de los mensajes de datos, es asimilable al de los documentos escritos y están sujetos a las regulaciones que plantea el artículo 395 del Código de Procedimiento Civil en lo referido a la prueba libre, por lo que el juez superior cebra apreciarlos con el mismo valor que se les da a las copias o reproducciones fotostáticas.

De acuerdo a lo antes expuesto podemos establecer que los correos electrónicos pueden ser llevados al expediente donde consta el juicio, ya sea en copia fotostática o reproducciones fotográficas y tendrán el mismo valor probatorio que dispone el artículo 429 del Código de Procedimiento Civil, el cual expresa:

Artículo 429: Los instrumentos públicos y los privados reconocidos o tenidos legalmente por reconocidos, podrán producirse en juicios originales o en copia certificada expedida por funcionarios competentes con arreglo a las leyes. Las copias o reproducciones fotográficas, fotostáticas o por cualquier otro medio mecánico claramente inteligible, de estos instrumentos, se tendrán como fidedignas si no fueren impugnadas por el adversario, ya en la contestación de la demanda, si han sido producidas con el libelo, ya dentro de los cinco días siguientes, si han sido producidas con la contestación o en el lapso de promoción de pruebas. Las copias de esta especie producidas en cualquier otra oportunidad, no tendrán ningún valor probatorio si no son aceptadas expresamente por la otra parte.

Conforme con esta norma, las copias fotostáticas o reproducidas por cualquier medio mecánico, se reputarán fidedignas, siempre que se cumplan con ciertas condiciones, entre ellas, que no sean impugnadas por la contraparte, ya en la contestación a la demanda si han sido producidas con el libelo, ya dentro de los cinco días siguientes, si han sido producidas con la contestación o en el lapso de pruebas.

IV. Conclusiones

En ese sentido podemos precisar las siguientes conclusiones en relación a las características de los Mensajes de Datos y Firmas Electrónicas:

- 1) Son pruebas atípicas. (art. 7 de la ley in comento).
- 2) No pueden ser exhibidos en juicio.
- 3) Están en la base de datos de un PC o en el servidor de la empresa. (Art. 7 de la Ley in comento).
- 4) Requieren de una experticia para su verificación.

En razón de estas características pueden ser llevados a juicio, mediante copias fotostáticas o reproducidas por cualquier medio mecánico, la consecuencia sería reputarlas como fidedignas.

Ahora bien, –la excepción- en los casos en que la contraparte no esté de acuerdo con dicha prueba, la Sala ha considerado que los medios para de los cuales se servirá el juez es apreciándolos u otorgándoles el mismo valor que se les da a las copias o reproducciones fotostáticas, en tanto que su promoción y evacuación se efectuará aplicando por analogía las disposiciones relativas a los medios de pruebas semejantes contemplados en el Código Civil, según lo estatuido en el artículo 395 del Código de Procedimiento Civil. (Sentencia N° 460 de fecha 05 de octubre de 2011, Caso: Transporte Doroca, C.A. contra Cargill de Venezuela, S.R.L.¹²).

No obstante, este valor y eficacia probatoria dependerá del adversario del promovente, quien tendrá la carga de impugnar dichos documentos, esto debe hacerlo en los siguientes actos procesales: en la contestación de la demanda si son producidos por la parte actora, o cinco días después de la contestación de la demanda si son presentados por la parte demandada, o cinco días después de la promoción de pruebas, caso contrario se reputarán fidedignas, conforme lo previsto en el artículo 429 del Código de Procedimiento Civil.

Respecto a ello, la Sala en sentencia N° 274 de fecha 30 de mayo de 2013, caso: Orión Realty, C.A. contra Franklin del Valle Rodríguez Roca¹³, señaló que “...las figuras idóneas establecidas para controlar los mensajes de datos lo son, la tacha de falsedad establecida en el artículo 443 del Código de Procedimiento Civil en concordancia con el artículo 1.381 del Código Civil, el desconocimiento o reconocimiento de los instrumentos que expresa el artículo 444 eiusdem, o la figura del cotejo prevista en el artículo 445 ibídem...”.

Significa que así como se ha previsto que los mensajes y datos al ser consignados en el expediente deben ser valorados como pruebas libres igualmente se prevé el mismo medio de impugnación para tales pruebas.

A pesar de las consideraciones del TSJ, es importante recordar que la Superintendencia de Servicios de Certificación Electrónica, ya está en funcionamiento a disposición del público en general, Suscerte es el organismo público del Estado venezolano responsable de gestionar, alertar y monitorear los incidentes informáticos, mediante el VenCERT y el CENIF, los cuales forman parte del Sistema Nacional de Seguridad Informática que establece la Ley de Infogobierno. La Ley de Mensaje de Datos y Firmas Electrónicas, promulgada en el año 2001, es otro aspecto nodal que el gobierno electrónico de Venezuela impulsa a través de SUSCERTE, organismo proveedor de la certificación de la firma electrónica y todo lo relacionado con este ámbito.

Es el organismo encargado de coordinar e implementar el Modelo Jerárquico de la Infraestructura Nacional de Certificación Electrónica, acredita, supervisa y controla a los Proveedores de Servicios de Certificación (PSC), administra

¹² www.tsj.gob.ve/decisiones/scc/octubre

¹³ www.tsj.gob.ve/decisiones/scc/mayo

La Autoridad de Certificación Raíz del Estado Venezolano. Es responsable del desarrollo del Sistema Nacional de Seguridad Informática, tiene como alcance proveer estándares y herramientas para implementar una tecnología de información óptima al Poder Público y al Poder Popular, a fin de brindar un mejor funcionamiento y proporcionar niveles de seguridad óptimos y confiables.

En conclusión y de acuerdo al breve análisis de la evolución en la valoración de la prueba referida a mensajes de datos y correos electrónicos se evidencia que la Sala Civil se está equiparando de manera calmada pero contundente en su admisión en juicios civiles.

Visión social de la prueba. Especial referencia a los medios electrónicos

Desirée J. Ríos M.*

SUMARIO: 1. Introducción. 2. Derecho procesal social. 3. La prueba. 4. La prueba electrónica. Doctrina y jurisprudencia de la Sala de Casación Social del Tribunal Supremo de Justicia. a) Como prueba documental. b) Como prueba libre. 5. Reflexiones finales.

Resumen

La consagración de los derechos sociales en la Constitución de la República Bolivariana de Venezuela ha influenciado definitivamente la elaboración de normas sustantivas y procesales, logrando así un sistema armónico de protección de estos especiales derechos. Ello categóricamente se proyecta a todos los medios de prueba incluidos los electrónicos, los cuales deben analizarse atendiendo a las normas y principios establecidos en las leyes procesales tales como valoración mediante reglas de la sana crítica (libre convicción razonada), el principio de primacía de la realidad, interpretación de la conducta de las partes en la producción de medios de prueba y las normas sobre prueba documental y libre previstas para esta materia.

Palabras claves: Derecho Procesal. Pruebas electrónicas. Mensaje de datos. Documentos. Prueba libre.

Recibido: 21/1/2017 • Aceptado: 15/2/2017

* Abogada egresada de la Universidad Central de Venezuela mención *Magna Cum Laude*. Especialista en *Derecho Procesal* Universidad Central de Venezuela, Centro de Estudios de Postgrado, Facultad de Ciencias Jurídicas y Políticas. 2005. *Mención Honorífica*. Doctoranda en Ciencias Mención Derecho Universidad Central de Venezuela, Centro de Estudios de Postgrado, Facultad de Ciencias Jurídicas y Políticas. Profesora de Pregrado y Postgrado en Derecho Procesal. Facultad de Ciencias Jurídicas y Políticas, Universidad Central de Venezuela. Miembro del Instituto Iberoamericano de Derecho Procesal. Abogada del Tribunal Supremo de Justicia Sala Político Administrativa y Sala de Casación Social. Jueza (suplente) en materia contencioso administrativo.

Abstract

The positivization of social rights in the Constitution of the Bolivarian Republic of Venezuela has definitely influenced the development of substantive and procedural rules, thus achieving a harmonious system of protection of these special rights. This categorically is projected to all means of evidence including electronic, which must be analyzed according to the norms and principles established in procedural laws such as valuation by rules of free reasoned conviction, the principle of primacy of the reality, interpretation of the conduct of the parties in the production of evidence and the norms on documentary and free evidence provided for this matter.

Key words: Procedural law. Digital evidence or electronic evidence. Data message. Documents. Free-proof.

1. Introducción

Las idea que queremos presentar la hemos denominado visión social de la prueba, para ello comenzaremos con una comparación en cuanto a las diferencias que hay en los procedimientos de corte social, en relación con el típico procedimiento civil, y una vez vislumbrado ello estudiaremos *la prueba*, para entonces analizarla en los procesos sociales haciendo énfasis en los medios informáticos. Asimismo realizaremos comentarios de algunas sentencias de la Sala de Casación Social del Tribunal Supremo de Justicia vinculadas con este tema tan vigente para nosotros los abogados y abogadas.

2. Derecho procesal social

A raíz de la entrada de vigencia de la Constitución de la República Bolivariana de Venezuela¹ donde la República se constituye en un Estado democrático y social de Derecho y de Justicia, podemos destacar una gran elaboración legislativa en materia de derechos sociales y de ahí resaltaremos la positivización de los mismos como elemento determinante para el surgimiento del derecho social procesal.

El Derecho Procesal, en su concepción general, podemos verlo como un derecho instrumental que busca la realización de la justicia y la solución de los conflictos intersubjetivos que pueden darse en una sociedad, en virtud de la prohibición del ejercicio del derecho por mano propia.

¹ Constitución de la República Bolivariana de Venezuela. Gaceta Oficial Extraordinario N° 5.453 de la República Bolivariana de Venezuela del 24 de marzo de 2000. Enmienda N° 1. Gaceta Oficial Extraordinario 5.908 del 19 de febrero de 2009.

El proceso – dice Niceto Alcalá Zamora y Castillo² –

so pena de encerrarnos en un círculo vicioso, no surge del proceso sino de una situación extra y meta procesal que él está llamado a canalizar y resolver. Esta situación originadora del proceso, puede ser denominada litigio, entendida la palabra en la dirección de Carnelutti (“conflictos de intereses calificado por la pretensión de uno de los interesados y la resistencia del otro”) pero en términos más amplios o sea añadimos ahora, como conflicto jurídicamente trascendente y susceptible de solución.

El proceso no es un fin en sí mismo, es un medio para alcanzar la justicia material como lo dispone el artículo 257 de la Constitución de la República Bolivariana de Venezuela. Mauro Capelletti expresa que la instrumentalidad del Derecho procesal es para tutelar el derecho denominado sustancial (público o privado). En tal sentido, cada sistema procesal será más perfecto en cuanto se adapte a la finalidad de las normas sustantivas sin mayores incoherencias o discrepancias³.

Históricamente se ha vinculado el estudio del Derecho Procesal como ciencia general, al denominado Derecho Civil ya que, al tratar de explicar su naturaleza, se le ha asociado al contrato y al cuasi contrato, siendo superadas dichas concepciones *ius privatistas* por otras teorías como la relación jurídica procesal y la de la situación jurídica que han desarrollado otros conceptos e instituciones que han permitido ubicar a esta ciencia en el campo del Derecho Público.

Al proceso civil (de corte privatista) se le atribuyen principios fundamentales como: a) la dialéctica o principio de contradicción; b) la igualdad procesal; c) verdad procesal; d) impulso de oficio por el juez; principio de que las partes están a derecho; e) principio de mediación con algunas fases de inmediatez; f) principio dispositivo; g) principio de concentración procesal; h) principio de preclusión; i) principio de economía procesal; j) principio de publicidad, entre otros.

Esta es la puerta –dice Capelletti– de como la ideología entra al proceso, por cuanto la o las ideologías forman parte del derecho sustancial, con importante reflejo en los principios procesales y las pruebas.

Con variantes mayores o menores, el proceso tradicional civil (*ius commune*) tiene las siguientes características que lo delinear. Siguiendo a Capelletti ellas son:

2 ALCALÁ-ZAMORA Y CASTILLO. “Proceso, Autocomposición y Autodefensa” (*Contribución al estudio de los fines del proceso*). Textos Universitarios Universidad Nacional Autónoma de México (UNAM). Institutos de Investigaciones Jurídicas. Dirección General de Publicaciones. Segunda Edición. 1970. pp. 12 y ss.

3 CAPETELLI, Mauro: “Proceso, Ideologías, Sociedad” - EJE A - Buenos Aires. - 1974 - trad. por Sentís Melendo, S. y Banzhaf, T. A.

Característica **primera**: dicho procedimiento asignaba un predominio absoluto, o más bien un verdadero monopolio, al elemento escrito. “**Quod non est actis non est in mundo**” [Lo que no está en los autos no está en el mundo]; las actividades procesales no expresadas en autos o actas escritos, eran jurídicamente inexistentes, y una decisión basada en elementos diversos de los escritos era ella misma absolutamente nula.

La **segunda característica** era la de desalentar toda relación personal, directa y pública, del órgano decisor con las partes, los testigos, los expertos y las demás fuentes de información (lugares y cosas). El juez, como se ha visto, debía basar su decisión exclusivamente en los autos y actas escritos, y no en sus impresiones personales. ¿Por qué entonces no confiar la preparación de los autos y actas a personas diversas del juez? He aquí en efecto que actuarii, notarii y otros personajes tomaron el lugar del juez en el examen de los testimonios in camera, traduciendo (inevitadamente, con frecuentes alteraciones) las palabras vivas al lenguaje escrito, por lo común al latín. El tribunal se topaba con los “papeles” recién al final del procedimiento. La consecuencia obvia era un verdadero y propio muro erigido entre el juez y las demás personas co-implicadas en el proceso. Con ese muro se tornaba inevitable el aislamiento del juez (que por lo común era usualmente un “doctor”, participe en cuanto tal del minúsculo segmento dirigente de la sociedad de la época) de los hechos y de la realidad social.

La **tercera característica** estaba representada por el así llamado sistema de la prueba legal, según el cual la valoración de las pruebas era establecida por ley, de manera abstracta y matemática. Un testigo no hacía prueba –“testis unus testis nullus”-, con una sola excepción el Papa. El testimonio no contradicho de dos personas, o bien, tratándose de testes de auditu (testigos de oídas), de cinco o siete personas, hacía prueba plena, vinculante para el tribunal. El testimonio de mujeres, prescindiendo de su número, era o inadmisible o valorado como prueba insuficiente, que necesitaba ser integrada por el testimonio de por lo menos un hombre. En la jerarquía de los valores testificales, el noble prevalecía sobre el no noble, el eclesiástico sobre el laico, el rico sobre el pobre, el viejo sobre el joven, el cristiano sobre el hebreo. Toda prueba estaba legalmente predeterminada en proporciones aritméticas: probatio plena, probatio semiplena, un cuarto o un octavo de prueba. El juez, en suma, debía contar las pruebas, más bien que pesarlas: sistema por lo demás perfectamente justificado si se piensa que él no veía a los testigos, no observaba el comportamiento de éstos, no podía apreciar la solidez de sus percepciones, ni verificar la sinceridad de sus declaraciones. La ley operaba en lugar del juez: obviamente, de manera abstracta, apriorística, formal. El número, el sexo, la edad, el estado social y económico, la religión: éstos y otros similares eran los elementos que “hacían” la verdad, no la veracidad o la malicia constatadas y valoradas en el caso concreto.

Una **cuarta característica** estaba representada por el desenvolvimiento fragmentario y discontinuo del procedimiento. A falta de una presencia directa del juez, las partes, o antes bien sus abogados, eran los amos incontrolados del desenvolvimiento del proceso. Abusos, tácticas dilatorias y reenvíos eran el resultado normal. En el intento de hacer frente a esos abusos, la ley a menudo imponía su orden, prescribiendo al curso del procedimiento etapas y términos

fijos y perentorios –un tratado del siglo XIII- enumeraba dieciocho de éstos en un procedimiento ordinario entumeciendo así el ya fragmentario carácter del procedimiento.(...) La **quinta y última característica**: la enorme duración de los procesos civiles⁴.

Ahora bien, como el proceso tiene carácter instrumental ya que tutela normas sustantivas que reflejan la ideología en un momento determinado, al modificarse normas constitucionales y en consecuencia normas legales deben necesariamente replantearse los procedimientos, en especial, los que tutelan derechos sociales.

Un elemento importante a tener en cuenta en los procesos jurisdiccionales sociales es la idea de igualdad prevista en la Constitución de la República Bolivariana de Venezuela (art. 21) que preceptúa que

la ley garantizará las condiciones jurídicas y administrativas para que la igualdad ante la ley sea real y efectiva; adoptará medidas positivas a favor de personas o grupos que puedan ser discriminados, marginados o vulnerables; protegerá especialmente a aquellas personas que por alguna de las condiciones antes especificadas, se encuentren en circunstancia de debilidad manifiesta y sancionará los abusos o maltratos que contra ellas se cometan.

La concepción de la igualdad dentro de un marco del Estado Social supone que debe darse igual trato jurídico a personas que están en la misma situación, debe pues tomarse en cuenta, la posición social real en que se encuentran los diferentes sujetos de derecho. Ello se puede lograr, mediante normas dictadas por el legislativo y también por el Poder Judicial en su función hermenéutica⁵, para hacer efectivo el mandato constitucional.

De esta forma, se rompe con ese mito de igualdad del Derecho privado “igualdad de las partes” ante la ley, en el contrato y desde luego en el proceso, frente a las desigualdades sociales evidentes y las injusticias que sufren determinado sectores vulnerables tales como los trabajadores, los consumidores, los niños, niñas y adolescentes, los arrendatarios y quienes cultivan o trabajan la tierra, entre otras áreas.

La modificación en las normas constitucionales, tal como se indicó, ha influido decisivamente en las normas procesales que regulan esta materia, haciendo surgir para la doctrina una nueva área denominada derecho procesal social⁶ o derecho social procesal, destinada a dar tutela a los derechos sociales.

⁴ Ídem.

⁵ La doctrina (con algunas críticas) señala como mecanismo para lograr dicha equiparación la denominada discriminación positiva entre ellos Ronald Dworkin. La discriminación inversa. “Los derechos en serio”. 2a. ed. Ariel, Barcelona, 1999. p.327 y ss. Título original: *Taking rights seriously*.

⁶ González Díaz Lombardo, Francisco. “El Derecho procesal social”. *Revista de la Facultad de Derecho de la UNAM*. Jul-Doi 1975. Num 99. Tomado de <http://www.juridicas.unam.mx/publica/librev/rev/facdermx/cont/99/dtr/dtr10.pdf>

Ahora, las competencias de la jurisdicción social en Venezuela comprenden la materia laboral, agraria y la de niños, niñas y adolescentes; y está integrada por la Sala de Casación Social, y demás tribunales con competencia en las referidas materias.

En Sala de Casación Social se manejan fundamentalmente estas tres competencias materiales: la laboral -donde hay el principal número de causas- y en ejercicio de ésta atribución se conoce: la casación, los controles de la legalidad y el contencioso administrativo laboral; el derecho agrario donde se conoce la casación agraria y el contencioso administrativo agrario y en materia de niños, niñas y adolescentes la cual conoce de casación y los controles de la legalidad.

Importante es destacar de estas competencias sus principios previstos en las leyes especiales.

Los principios procesales que caracterizan el proceso laboral previsto en la Ley Orgánica Procesal del Trabajo⁷ son fundamentalmente: gratuidad, inmediación, oralidad (más que un principio es una regla que garantiza la inmediación), *in dubio pro operario* (para normas sustantivas y procesales) concentración, no restricción a vicios clásicos de la sentencia como en la Casación Civil, facultades oficiosas del juez; principio de primacía de la realidad (para normas sustantivas e interpretación de la dinámica procesal), conciliación y mediación (vinculados con la inmediación), más los comunes a otros procesos por ser de rango constitucional como el derecho a la defensa, tutela judicial efectiva juez natural, entre otros. En materia de prueba debemos destacar el establecimiento de la sana crítica (libre convicción razonada) como regla de valoración de las pruebas, la inclusión de medios de prueba como la declaración de parte y la inversión legal de la carga de la prueba. En este sentido la citada ley dispone:

Artículo 2. El juez en sus decisiones no podrá contrariar los principios de uniformidad, brevedad, oralidad, publicidad, gratuidad, celeridad, **inmediatez, concentración, prioridad de la realidad de los hechos y equidad.**

Artículo 3. El proceso será oral, breve y contradictorio, y sólo se apreciarán las pruebas incorporadas en el proceso, conforme a las disposiciones de esta Ley. Se admitirán las formas escritas previstas en esta Ley.

Artículo 4. Los actos del proceso serán públicos, salvo que expresamente esta Ley disponga lo contrario o el tribunal así lo decida por razones de seguridad, de moral o de protección de la personalidad de alguna de las partes.

Artículo 5. Los jueces, en el desempeño de sus funciones, tendrán por norte de sus actos la verdad, están obligados a inquirirla por todos los medios a su alcance y a no perder de vista la irrenunciabilidad de derechos y beneficios acordados por las leyes sociales a favor de los trabajadores, así como el carácter tutelar de las mismas; y por tal causa, tienen que intervenir en forma activa en

7 Gaceta Oficial Número 37.504 del 13-08-02.

el proceso, dándole el impulso y la dirección adecuados, en conformidad con la naturaleza especial de los derechos protegidos.

Artículo 6. El juez es el rector del proceso y debe impulsarlo personalmente, a petición de parte o de oficio, hasta su conclusión. A este efecto, será tenida en cuenta, también a lo largo del proceso, la posibilidad de promover la utilización de medios alternativos de solución de conflictos, tales como la conciliación, mediación y arbitraje. **Los jueces que han de pronunciar la sentencia deben presenciar el debate y la evacuación de las pruebas de las cuales obtienen su convencimiento.**

Parágrafo Único: El juez de juicio **podrá ordenar el pago de conceptos, como prestaciones o indemnizaciones, distintos de los requeridos cuando éstos hayan sido discutidos en el juicio y estén debidamente probados, o condenar al pago de sumas mayores que las demandadas, cuando aparezca que éstas son inferiores a las que corresponden al trabajador, de conformidad con esta Ley y con lo alegado y probado en el proceso, siempre que no hayan sido pagadas.**

Artículo 7. Hecha la notificación para la audiencia preliminar, las partes quedan a derecho y no habrá necesidad de nueva notificación para ningún otro acto del proceso, salvo los casos expresamente señalados en esta Ley.

Artículo 8. La justicia laboral será gratuita; en consecuencia, los tribunales del trabajo no podrán establecer tasas, aranceles, ni exigir pago alguno por sus servicios. Los registradores y notarios públicos no podrán cobrar tasas, aranceles, ni exigir pago alguno en los casos de otorgamiento de poderes y registro de demandas laborales.

Artículo 9. **Cuando hubiere duda** acerca de la aplicación o la interpretación de una norma legal, o en caso de colisión entre varias normas aplicables al mismo asunto, **se aplicará la más favorable al trabajador.** En caso de duda sobre la apreciación de los hechos o de las pruebas, se aplicará igualmente la que más favorezca al trabajador. La norma adoptada se aplicará en su integridad.

Artículo 10. Los jueces del trabajo apreciarán las pruebas según las reglas de la sana crítica; en caso de duda, preferirán la valoración más favorable al trabajador.

Artículo 11. Los actos procesales se realizarán en la forma prevista en la ley; en ausencia de disposición expresa, el juez del trabajo determinará los criterios a seguir para su realización, todo ello con el propósito de garantizar la consecución de los fines fundamentales del proceso. A tal efecto, el juez del trabajo podrá aplicar analógicamente disposiciones procesales establecidas en el ordenamiento jurídico, teniendo en cuenta el carácter tutelar de derecho sustantivo y adjetivo del derecho del trabajo, cuidando que, la norma aplicada por analogía no contraría principios fundamentales establecidos en la presente Ley”. (Destacado nuestro).

En materia de niños, niñas y adolescentes tenemos que los principios procesales que caracterizan a esta área son: defensa del interés superior de los niños, las niñas y los adolescentes, celeridad, confidencialidad, imparcialidad, igualdad de las partes, debido proceso, derecho de defensa, juez natural (comunes a todos los demás procesos por ser de rango constitucional), posibilidad de actuar de oficio en materia probatoria y para dictar medidas cautelares, realizar

diligencias preliminares. También en materia de prueba el establecimiento de la sana crítica (libre convicción razonada) como regla de valoración de las pruebas y la inclusión de medios de prueba como la declaración de parte, al igual que en materia del trabajo; la posibilidad de valorar las conductas procesales de las partes en juicio en la colaboración de la prueba y la opinión del niño, niña o adolescente, entre otros.

Así, la Ley Orgánica para la protección de Niños, Niñas y Adolescentes establece⁸:

Artículo 450 “Principios. La normativa procesal en materia de protección de niños, niñas y adolescentes tiene como principios rectores, entre otros, los siguientes:

a) Oralidad. El juicio es oral y sólo se admiten las formas escritas previstas en esta Ley.

b) **Inmediación**. El juez o jueza que ha de pronunciar la sentencia debe presenciar el debate y la incorporación de las pruebas de las cuales obtiene su convencimiento salvo los casos que la Ley permita la comisión judicial para la evacuación de algún medio probatorio necesario para la demostración de los hechos controvertidos, pruebas que serán discutidas en la audiencia de juicio. Sólo se apreciarán las pruebas incluidas en la audiencia, conforme a las disposiciones de esta Ley.

c) Concentración. Iniciado el debate, éste debe concluir en el mismo día. Si ello no fuere posible continuará durante el menor número de días consecutivos.

d) Uniformidad. Las controversias que se susciten entre partes en reclamación de algún derecho se tramitan por los procedimientos contenidos en esta Ley, aunque por otra leyes tengan pautado un procedimiento especial.

e) Medios alternativos de solución de conflictos. El juez o jueza debe promover, a lo largo del proceso, la posibilidad de utilizar los medios alternativos de solución de conflictos, tales como la mediación, salvo en aquellas materias cuya naturaleza no la permita o se encuentre expresamente prohibida por la ley.

f) Publicidad. El juicio oral tiene lugar en forma pública, pero se debe proceder a puertas cerradas total o parcialmente, cuando así lo establezca la ley o determine el juez o jueza por motivos de seguridad, de moral pública o de protección de la personalidad de alguna de las partes o de alguna persona notificada para participar en él, según la naturaleza de la causa.

La resolución será fundada y debe constar en el acta del debate. Desaparecida la causa de la clausura, puede ingresar nuevamente el público. Lo anterior no obsta el carácter público del expediente, el cual no puede ser objeto de reserva, salvo las excepciones establecidas en esta Ley.

g) Simplificación. Los actos procesales son breves y sencillos, sin ritualismos ni formalismos innecesarios.

⁸ Gaceta Oficial N° 5.859 Extraordinario del 10 de diciembre de 2007 y su reforma Parcial publicada en Gaceta Oficial Extraordinario N° 6.185 del 08 de junio de 2015.

h) Iniciativa y límites de la decisión. El juez o jueza sólo puede iniciar el proceso previa solicitud de parte, pero puede proceder de oficio cuando la ley lo autorice y en sus decisiones debe atenerse a lo alegado y probado en autos.

i) Dirección e impulso del proceso por el juez o jueza. El juez o jueza dirige el proceso y debe impulsarlo de oficio hasta su conclusión.

j) **Primacía de la realidad.** El juez o jueza debe orientar su función en la búsqueda de la Verdad e inquirirla por todos los medios a su alcance. En sus decisiones prevalecerá la realidad sobre las formas y apariencias.

k) **Libertad probatoria. En el proceso, las partes y el juez o jueza, pueden valerse de cualquier medio de prueba no prohibido expresamente por la ley y el juez o jueza lo apreciará según las reglas de la libre convicción razonada.**

l) Lealtad y probidad procesal. Las partes, sus apoderados, apoderadas, abogados y abogadas deben actuar en el proceso con lealtad y probidad. El juez o jueza debe tomar todas las medidas necesarias establecidas en la ley, tendentes a prevenir o a sancionar las faltas a estos deberes en el proceso.

m) Notificación única. Realizada la notificación del demandado o demandada para la audiencia preliminar, las partes quedan a derecho, sin necesidad de nueva notificación para ningún otro acto del proceso, salvo los casos expresamente señalados en esta Ley.

n) Defensa técnica gratuita. Las partes que así lo requieran contarán con asistencia o representación técnica gratuita en todo estado y grado de la causa a fin de garantizar la mejor defensa de sus derechos e intereses, a tal efecto las partes podrán solicitar los servicios de la Defensa Pública o el juez o jueza podrá designar a un Defensor Público o Defensora Pública cuando lo estime conducente”. (Destacado nuestro).

En materia agraria, los principios procesales gozan de similares características, es decir, de simplificación, intermediación, oralidad, actuación oficiosa del juez, brevedad, concentración, entre otros. Veamos⁹:

Artículo 22. Para la ejecución de sus competencias, los organismos agrarios actuarán conforme a los principios constitucionales de la **seguridad alimentaria, utilidad pública y función social de la tierra**, el respeto de la propiedad privada, la promoción y protección de la función social de la producción nacional, la promoción de la independencia y **soberanía agroalimentaria de la nación, el uso racional de las tierras y los recursos naturales y la biodiversidad genética.**

Artículo 23. Los jueces y juezas competentes de la jurisdicción agraria, el Instituto Nacional de Tierras, la Corporación Venezolana Agraria, el Instituto Nacional de Desarrollo Rural y cualquiera de los órganos agrarios, podrán desconocer la constitución de sociedades, la celebración de contratos y, en general, la adopción de formas y procedimientos jurídicos, cuando sean realizados con el propósito de efectuar fraude a las normas contenidas en el presente

⁹ Ley de Tierras y Desarrollo Agrario. Gaceta Oficial N° 5.991, Extraordinario de fecha 29 de julio de 2010.

Decreto Ley. Igualmente sobre aquellos que se les pretenda usar para efectuar similar fraude, aún cuando se hubieren celebrado con anterioridad.

Los hechos, actos o negocios jurídicos simulados o realizados con la intención de efectuar fraude al presente Decreto Ley, no impedirán la aplicación de la norma evadida o eludida, ni darán lugar a los beneficios o ventajas que se pretendan obtener con ellos. Artículo 155. Los procedimientos previstos en el presente Título se regirán por los principios de inmediación, concentración, brevedad, oralidad, publicidad y **carácter social del proceso agrario**.

Artículo 187. La forma escrita de los actos sólo será admitida en los casos expresamente consagrados en las disposiciones del presente título y **cuando deban practicarse pruebas antes del debate oral que requieran el levantamiento de un acta**.

Los principios de oralidad, brevedad, concentración, inmediación y publicidad son aplicables al procedimiento ordinario agrario.

Las disposiciones y formas del procedimiento oral son irrenunciables, no pudiendo relajarse por convenio de las partes ni por disposición del juez. Su incumplimiento será causa de reposición de oficio o a instancia de parte.

Artículo 188. La causa se sustanciará oralmente en audiencia o debate. (...)

Artículo 191. Los jueces y juezas agrarios podrán ordenar la práctica de cualquier medio probatorio que consideren necesario para el mejor esclarecimiento de la verdad».

Artículo 192. Los jueces y juezas agrarios podrán ordenar de oficio la evacuación de pruebas que hayan sido promovidas por las partes y no hubiesen sido evacuadas.

Artículo 193. En todo estado y grado del proceso las partes podrán acordar, previa aprobación del juez, la abreviación y concentración de los actos a fin de reducir los términos y lapsos procesales.

Artículo 205. Los jueces o juezas podrán decretar providencias y autos tendentes a esclarecer y aligerar de oficio los trámites de actuaciones y pruebas. Igualmente, podrán dar por terminados los actos de examen de testigos y de posiciones juradas cuando lo consideren pertinente. Podrán igualmente solicitar asesoramiento técnico con el objeto de requerir dictámenes a funcionarios expertos, sin carácter vinculante para el juez o jueza”. (Destacados nuestros)

En este contexto, pensamos que este derecho procesal social, no está atado o debe seguir las formas tradicionales rígidas de los procesos civiles o mercantiles, pero más allá consideramos que, en cualquier tipo de proceso que no sea de los de típico corte social, si estuviere involucrado algún derecho social, la interpretación del juez debe ser distinta, atendiendo al contexto de un estado social donde los intereses individuales ceden ante los colectivos o sociales.

Así, estimamos que las normas que contienen derechos sociales deben protegerse en cualquier tipo de proceso, no siendo de aplicación exclusiva de los tribunales laborales, agrarios o de niños, niñas y adolescentes.

3. La prueba

En todo proceso por su estructura lógica es de vital importancia la prueba de las alegaciones para la convicción del juzgador.

La prueba está presente en todas las manifestaciones de la vida humana, de ahí que la prueba podamos verla en un sentido común y en un aspecto técnico, en donde varía según la clase de actividad o la ciencia en la cual se estudie. Así, pudiéramos decir, que el derecho procesal se apropia de la prueba y la emplea para sus fines.

En este orden de ideas, nos dice el profesor Jairo Parra Quijano que la noción de prueba aparece unida a todas las actividades de tipo social. Puede afirmarse que es una necesidad que surge desde que el hombre vive en sociedad. El niño, desde temprana edad, empieza a realizar experimentos que quiere hacer ver a sus padres como demostración de sus habilidades, a fin de que estos den muestras de admiración y aprobación. En todas las ciencias reconstructivas, la prueba tiene una importancia fundamental, pues permite conocer el pasado; pero en el campo del derecho este aspecto es vital para saber quién tiene la razón. En el mundo del proceso, la prueba es fundamental, ya que estando destinada a producirle certeza al juez, no se puede prescindir de ella sin atentar contra los derechos de las personas. El juez reconstruye los hechos tal cual como se supone ocurrieron y los subsume en la norma general y abstracta prevista por el legislador. Sin esta labor, sería imposible la aplicación de las normas. La prueba, entonces tiene una función social, una función humana-individual y una función jurídica (hacer posible saber cómo sucedieron los hechos, para aplicar las normas)¹⁰.

Couture dice que en su acepción común, la prueba es la acción y el efecto de probar; y probar es demostrar de algún modo la certeza de un hecho o la verdad de una afirmación. La prueba es, en todo caso, una experiencia, una operación, un ensayo, dirigido a hacer patente la exactitud o inexactitud de una proposición¹¹.

¹⁰ “Manual de Derecho Probatorio”. Décima primera Edición. Ediciones Librería del Profesional. Santafé de Bogotá, Colombia. 2000.

¹¹ Definición: 1. En general, dicese de todo aquello que sirve para averiguar un hecho, yendo de lo conocido hacia lo desconocido. 2. Forma de verificación de la exactitud o error de una proposición. 3. conjunto de actuaciones realizadas en juicio, con el objeto de demostrar la verdad o falsedad de las manifestaciones formuladas en el mismo. 4. Medios de evidencia, tales como documentos, testigos, etc., que crean al juez la convicción necesaria para admitir como ciertas o rechazar como falsas las proposiciones formuladas en juicio. *Etimología*. Del bajo latín *proba*, -*ae* “prueba”, postverbal del verbo *probo*, -*are* “probar”, denominativo de *probus*, -*a*, -*um*. Este adjetivo significaba originalmente “que marcha resto”, después “bueno, honesto, probo”. El verbo *probare*, por lo tanto, significaba “encontrar bueno”, de donde “aprobar, probar” y también “de mostrar”. Traducción. Francés, *Preuve*; Italiano, *Prova*; Portugués, *Prova*; Ingles, *proof*, *Evidence*; Alemán, *Beweis*. Couture, Eduardo. Vocabulario Jurídico. “Vocabulario Jurídico”. Buenos Aires, 1976

Para Michele Taruffo la prueba es el instrumento que utilizan las partes desde hace siglos para demostrar la veracidad de sus afirmaciones, y del cual se sirve el juez para decidir respecto a la verdad o falsedad de los enunciados fácticos. En términos muy generales, se entiende como prueba cualquier instrumento, método, persona, cosa o circunstancia que pueda proporcionar información útil para resolver dicha incertidumbre. Según esta definición, son prueba tanto los instrumentos para adquirir información que están expresamente regulados por la ley (las denominadas pruebas típicas) como aquellos que la ley no regula expresamente (las denominadas pruebas atípicas) pero que, sin embargo, pueden servir para fundar la decisión sobre los hechos¹².

Para hablar entonces de medios de prueba en este tipo de procesos, ubiquémonos en lo que denominamos inicialmente *visión social de la prueba*. Esta idea la proyectamos a varios aspectos, ellos son: las oportunidades procesales de promoción o incorporación de la prueba en la búsqueda de la verdad material; los medios de prueba que es el objeto este estudio; la carga de la prueba (tema interesantísimo pero que no abordaremos en esta ocasión) y la valoración de la prueba. Es decir, dada la especial regulación constitucional y legal de los derechos sociales la interpretación de la prueba, su forma de incorporación y valoración debe ir acompañada de los principios propios de esta área del derecho.

4. La prueba electrónica. Doctrina y jurisprudencia de la Sala de Casación Social del Tribunal Supremo de Justicia

Dentro del universo de pruebas posibles a promover en estos procesos sociales para demostrar la verdad de las afirmaciones realizadas a través de los alegatos, están los medios electrónicos.

Los *medios electrónicos* forman parte de nuestra vida cada vez más hacemos usos de estas herramientas tecnológicas en esta sociedad globalizada, empleamos y nos comunicamos a través de los diversos dispositivos electrónicos, es decir, a través de aquellos mecanismos, equipos o sistemas que permiten producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otras; por medio de ellos se crean documentos sin soporte físico.

Con el avance de la tecnología hay un universo de pruebas electrónicas videos, chats, redes sociales, páginas web los e mails, entre otras y el problema que se nos plantea es cuando necesitamos de los mensajes, de los videos o de los documentos realizados o contenidos en medios electrónicos para demostrar

¹² TARUFFO, Michele, "La Prueba". Artículos y Conferencias. Monografías Jurídicas Universitarias. Editorial Metropolitana 2008, Chile. p. 59. Y La Prueba de los Hechos Editorial Trotta Madrid. 2002.

afirmaciones en un determinado proceso; es decir, la pregunta es cómo los promovemos. Las formas más comunes en este tipo de procedimientos es realizarlo a través de la prueba documental o a través de la prueba libre¹³.

a) Como prueba documental

Si se incorpora al juicio la prueba electrónica como (medio) documento contamos en nuestra legislación con el Decreto con Fuerza de Ley de Mensaje de Datos y Firmas Electrónicas¹⁴, las normas de la prueba documental previstas en la Ley Orgánica Procesal del Trabajo para documentos públicos y privados con sus respectivas impugnaciones –arts. 80 al 94- (aplicables a los juicios de niños, niñas y adolescentes), el Decreto con Rango Valor y Fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre Órganos y Entes del Estado¹⁵, las normas de valoración previstas en la Ley Orgánica para la Protección de Niños, Niñas y Adolescentes; las normas sobre pruebas previstas en la Ley de Tierras y Desarrollo Agrario y, por último, el Código de Procedimiento Civil y el Código Civil como normas generales a las cuales se acuden cuando no hay previsión expresa de la ley. Así, por este camino tenemos regulación para dar respuestas a las partes que promuevan este tipo de documentos.

En cuanto a la prueba documental tenemos que la voz documento deriva del latín *docere* que significa dar a conocer, un documento en sentido general es un acto humano que representa un hecho. Dice Hernando Devis Echandía¹⁶ en su obra que, en sentido estricto, es documento toda cosa que sea producto de un acto humano, perceptible con los sentidos de la vista y al tacto, que sirve de prueba histórica indirecta y representativa de un hecho cualquiera. Puede ser declarativo-representativo, cuando contenga una declaración de quien lo crea u otorga o simplemente lo suscribe, como es el caso de los escritos públicos o privados; pero puede ser únicamente representativo (no declarativo), cuando no contenga ninguna declaración, como ocurre en los planos, cuadros o fotografías. Por lo tanto, el documento no es siempre un escrito.

Continúa exponiendo este autor que

ha existido la tendencia a identificar los conceptos de documento e instrumento o escrito, como si todos los documentos consistieran en escritos; esto es consecuencia de que el C. C. de Napoleón y los que en éste se basan, se refieren

¹³ En el presente estudio nos referiremos a los medios electrónicos, en general, como medios de prueba promovidos por las partes y no como herramienta a emplearse en las diversas etapas de los juicios vg. como los medios de reproducción audiovisual y los dispositivos que los contienen tales como CD.

¹⁴ N° 1.204 Gaceta Oficial No 37.076 de fecha 13 de diciembre de 2000.

¹⁵ N° 9.051. Gaceta Oficial No 39.945 de fecha 15 de junio de 2012.

¹⁶ DEVIS ECHANDIA, Hernando, "Teoría General de la Prueba Judicial" T. I, 4ta. Edic. Biblioteca Jurídica Dike, Medellín.

únicamente a los últimos, distinguiéndolos en instrumentos públicos y privados. Pero, como de lo acabado de exponer se concluye, existen numerosos documentos que no consisten en escritos, como planos, dibujos, cuadros, fotografías; radiografías, películas, cintas magnetofónicas y discos con grabaciones de conversaciones y sonidos de cualquier clase, y similares, cuya naturaleza documental no es posible desconocer y se acepta generalmente con la jurisprudencia y doctrina modernas de todos los países, por lo cual no hace falta que la ley los autorice expresamente, porque se deben considerar incluidos en el género aceptado de la prueba documental pública o privada, según el origen que tengan.

Partiendo de las premisas señaladas, el documento electrónico se ha definido como un instrumento que contiene una información escrita, audiovisual formado por un medio informático o electrónico¹⁷.

Soto Caldera¹⁸ define el documento electrónico como toda aquella representación del pensamiento y de la voluntad del hombre materializado en soportes magnéticos de acceso inmediato, capaz de trasladarse de un lugar a otro por medio de redes telemáticas.

El Decreto con Rango Valor y Fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre Órganos y Entes del Estado, define en su artículo 4 al documento digitalizado a diferencia del Decreto con Fuerza de Ley de Mensaje de Datos y Firmas Electrónicas. En este artículo se dice que el documento digitalizado es aquel que contiene dato o información acerca de un hecho o acto, capaz de causar efectos jurídicos.

La exposición de motivos del Decreto con Fuerza de Ley de Mensaje de Datos y Firmas Electrónicas, establece que

el principal objetivo de este Decreto-Ley es adoptar un marco normativo que avale los desarrollos tecnológicos sobre seguridad en materia de comunicación y negocios electrónicos, para dar pleno valor jurídico a los mensajes de datos que hagan uso de estas tecnologías. Nuestra legislación actual establece, que cuando un acto o contrato conste por escrito, bastará como prueba el instrumento privado con las firmas autógrafas de los suscriptores. Dentro de este contexto el Decreto-Ley Sobre Mensaje de Datos y Firmas Electrónicas, pretende crear mecanismos para que la firma electrónica, en adelante, tenga la misma eficacia y valor probatorio de la firma escrita, siempre y cuando cumpla con los requisitos mínimos establecidos en este Decreto-Ley.

¹⁷ Desde luego debemos tener presente la clasificación de los documentos en públicos, privados y administrativos.

¹⁸ Citado por Jurado, Alberto. Valor probatorio del documento electrónico. Cuestiones Jurídicas, Revista de Ciencias Jurídicas de la Universidad Rafael Urdaneta, Vol. Nro. 1 (enero-Junio 2011) <http://www.uru.edu/fondoeditorial/revista/pdf/rcj/v5.n1/valor%20probatorio.pdf>

Asimismo expresa que

en términos generales, la legislación actual no reconoce el uso de los medios electrónicos de manera expresa y en caso de un litigio, el juez o tribunal, tendrá que allegarse de medios de prueba libre y acudir a la sana crítica para determinar que una operación realizada por medios electrónicos es o no válida. Esta situación ha originado que empresas y personas se sientan inseguras de realizar transacciones por medios electrónicos, debido a la incertidumbre legal en caso de controversias. Por ello se hace indispensable dar valor probatorio al uso de medios electrónicos en los procesos administrativos y judiciales, sin que quede al arbitrio del juez considerar su validez probatoria, en caso de controversia, debido a una ausencia de regulación expresa. Así tenemos que entre las principales disposiciones contenidas en el Decreto-Ley Sobre Mensajes de Datos y Firmas Electrónicas, se encuentran disposiciones que regulan: El mensaje de datos. La firma electrónica. Los certificados electrónicos. Los proveedores de servicios de certificación.

Ahora, los principales problemas que presenta este medio al ser considerado documento son la inmaterialidad y la ausencia de firma, lo cual puede resumirse en la palabra *autenticidad* del medio.

Algunas precisiones respecto a esto. El artículo 8 del Decreto-Ley Sobre Mensajes de Datos y Firmas Electrónicas expresa en cuanto a ello que

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. Cuando la ley requiera que ciertos actos o negocios jurídicos consten por escrito y su soporte deba permanecer accesible, conservado o archivado por un período determinado o en forma permanente, estos requisitos quedarán satisfechos mediante la conservación de los Mensajes de Datos, siempre que se cumplan 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.

Asimismo, la firma coadyuva con la autenticidad del medio y la indicada ley dispone que su objeto

es 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. El presente Decreto-Ley será aplicable a los Mensajes de Datos y Firmas Electrónicas independientemente de sus características tecnológicas o de los desarrollos

tecnológicos que se produzcan en un futuro. A tal efecto, sus normas serán desarrolladas e interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los Mensajes de datos y Firmas Electrónicas. La certificación a que se refiere el presente Decreto-Ley no excluye el cumplimiento de las formalidades de registro público o autenticación que, de conformidad con la ley, requieran determinados actos o negocios jurídicos. (art.1).

En cuanto a los documentos que contengan *mensajes de datos* y que cumplan con lo establecido en la ley tienen, como ella misma dice, su regla de valoración, esto es, el propio texto establece un sistema legal que busca impedir la arbitrariedad del juez en esta materia. En efecto, el artículo 4 *eiusdem* dispone que los mensajes de datos tienen la misma eficacia probatoria que la ley otorga a los documentos escritos, sin perjuicio de lo establecido en la primera parte del artículo 6 de este Decreto-Ley. 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.

De tal forma que, los correos electrónicos, páginas web y cualquier otro documento electrónico, así como sus copias almacenadas en los diversos dispositivos sus impresiones pueden ser considerados como pruebas documentales, pues dichos medios representan un hecho que puede demostrar una afirmación en juicio determinado.

Para la firma electrónica el artículo 16 *eiusdem* dispone que la firma electrónica que permita vincular al signatario con el mensaje de datos y atribuir la autoría de éste, tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa. A tal efecto, salvo que las partes dispongan otra cosa, la firma electrónica deberá llenar los siguientes aspectos:

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 en cada momento.
3. No alterar la integridad del Mensaje de Datos. La Firma Electrónica podrá formar parte integrante del Mensaje de Datos, o estar inequívocamente asociada a éste; enviarse o no en un mismo acto.

Asimismo señala la citada Ley que la firma electrónica que no cumpla con los requisitos señalados no tendrá los efectos jurídicos que se le atribuyen, sin embargo, podrá constituir un elemento de convicción valorable conforme a las reglas de la sana crítica.

Esto es, como se indicó, en nuestro ordenamiento hay normas que permiten dar respuesta al justiciable cuando la prueba informática es promovida a través de la prueba documental. La dificultad se presenta para los juzgadores cuando los documentos electrónicos no cumplen con esos requisitos, entra allí la necesaria labor interpretativa.

b) Como prueba libre

En Venezuela el sistema de promoción de medios es mixto, es decir, se pueden promover todos los medios previstos en las leyes y cualquier otro que sea necesario para la demostración de las afirmaciones. Esto segundo se conoce como sistema libre de promoción de medios.

Las pruebas libres son entonces aquellas cuya promoción, reproducción, contradicción o control no está expresamente regulada, pero de las cuales pueden también las partes valerse siempre que no estén prohibidas expresamente por la ley, y que consideren conducente a la demostración de sus pretensiones. Estos medios se promoverán y evacuarán aplicando por analogía las disposiciones relativas a los medios de pruebas semejantes contemplados en las leyes de la República, y en su defecto, en la forma que señale el Juez.

Es decir, aquí el tema es cuando la prueba no puede ser incorporada a través del medio documento y requiere de otros mecanismos auxiliares para buscar la autenticidad tales como experticias, inspecciones judiciales o prueba de informes.

En este sentido, el Decreto-Ley Sobre Mensajes de Datos y Firmas Electrónicas citado establece en su artículo 4 que la promoción de un mensaje de datos, control, contradicción y evacuación como medio de prueba, se realizará conforme a lo previsto para las pruebas libres en el Código de Procedimiento Civil; así, observamos que la ley prevé un sistema de valoración para el documento (medio escrito), derivado del principio de equivalencia funcional asumido en la ley, pero a la vez regula la incorporación del medio como si se tratara de una prueba libre; lo cual en nuestro modo de ver confunde los sistemas de valoración (tarifa) con los sistemas de promoción para el mismo medio de prueba; quizás el origen de esto se deba a la desconfianza del legislador en el juez señalada en la citada exposición de motivos¹⁹.

Sin embargo, reiteramos, siempre será necesaria la labor hermenéutica del juzgador o juzgadora para dar respuesta al caso concreto, puesto que la mayoría de los medios electrónicos promovidos en juicio siempre se ven afectados en su autenticidad y no es sencilla la función de quien juzga, en virtud de que, le corresponde hacer interpretación sistemática de las normas especiales sobre medios electrónicos con las normas particulares de cada área de los derechos sociales.

En este orden de ideas, pasaremos a comentar algunas sentencias de la Sala de Casación Social donde se dan respuesta a estos problemas (bien sea como prueba documental o libre).

¹⁹ Señala el referido texto: “*Por ello se hace indispensable dar valor probatorio al uso de medios electrónicos en los procesos administrativos y judiciales, sin que quede al arbitrio del juez considerar su validez probatoria, en caso de controversia, debido a una ausencia de regulación expresa*”.

1. Sentencia N° 0264 del 5 de marzo de 2007. Se trata de un recurso de casación con ocasión al juicio que por cobro de diferencia de prestaciones sociales (horas extras) intentó el ciudadano Luis Alberto Nava Jiménez contra la sociedad mercantil C.A. VENCEMOS., en dicho recurso se denunció, entre otras normas la infracción, por error de interpretación, del artículo 4 del Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas y la falta de aplicación de los artículos 12 y 17 *eiusdem*. Para resolver la denuncia la Sala expresó:

Por otra parte, alega la formalizante que se infringió por errónea interpretación el artículo 4 del Decreto con fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas, así como la falta de aplicación del artículo 12 *eiusdem*, conjuntamente con el artículo 17 *ibidem*, puesto que la recurrida calificó los correos internos de la empresa demandada, que fueron consignados en forma impresa, promovidos por la parte actora, “simplemente de correos electrónicos”, supeditando su eficacia probatoria al hecho de que el mensaje de datos esté asociado a algún mecanismo de seguridad que permita identificar el origen y autoría del mismo; sin tomar en consideración que de conformidad con la citada ley especial su valor es similar al de los documentos escritos y están sujetos a las regulaciones que plantea el artículo 395 del Código de Procedimiento Civil, en lo referido a la prueba libre, por lo que debió apreciarlos con el mismo valor que se les da a las copias o reproducciones fotostáticas; asimismo alega el recurrente que deben ser apreciadas de conformidad a la sana crítica y que en aplicación del artículo 12 de la mencionada Ley, que consagra que el mensaje de datos se tendrá por emitido en donde el emisor tenga su domicilio y por recibido en el lugar donde el destinatario tenga el suyo, el juzgador debió concluir que los mensajes internos de la compañía demandada se emitieron y recibieron en las instalaciones de la misma.

Ahora bien, respecto a tal medio probatorio, en la recurrida se expresó: (...)

5. LOTUS NOTES (Correo interno de la empresa C.A. VENCEMOS), promovida con el objeto de demostrar que el actor trabajaba fuera de su jornada normal, las cuales fueron impugnadas por la parte demandada en al (sic) audiencia de juicio.

Vista la prueba promovida, este Juzgado observa que se trata de una prueba tecnológica, la cual tiene características muy especiales, dada la forma de generación de dichos documentos.

El uso de las Tecnologías de Información y Comunicaciones (TICs) trae consigo al correo electrónico como una nueva forma de documentar los hechos derivados de las relaciones laborales, que al momento de ser utilizado como medio de prueba influye especialmente en la actividad probatoria del Proceso Laboral; considerando que dentro del proceso será necesario estudiar el contenido del documento, no sólo en cuanto al hecho histórico que representa, sino en cuanto a la licitud en la obtención del correo electrónico que no vulnere los derechos

constitucionales sobre la privacidad en las comunicaciones de la parte contra quien se opone, la pertinencia y el soporte material de presentación, a fin de determinar si el mensaje es íntegro, confidencial y auténtico, si se trata de original o copia, si contiene firma electrónica con certificado. (...)

Así, dentro de las empresas se han implementado modos de comunicación electrónica, a través de las denominadas redes Intranet, que son instalaciones de redes internas dentro de la misma corporación, como las denominadas Intranets o por medio de dos o más redes entre las diferentes empresas, como es el caso de las redes Extranets, ambas son aplicaciones de Internet para campos específicos. (...)

En concreto, se puede promover un correo electrónico como prueba documental, es decir, de forma impresa o grabada en un disquete, siendo que en el presente caso se promovió de forma impresa, pero su eficacia probatoria dependerá de que el mensaje de datos esté asociado a algún mecanismo de seguridad que permita identificar el origen y autoría del mismo (como es el caso de una firma electrónica) y tendrá la misma fuerza probatoria que un documento privado; pero, si en la elaboración, envío o recepción del correo electrónico no se utilizó ningún método de seguridad que garantice el origen o autoría del mensaje, se ha considerado que ello imposibilita su aprovechamiento en juicio.

Por otra parte, se observa que el actor trata de demostrar que trabajó horas extraordinarias, y no indicó en la demanda la jornada normal de trabajo a los efectos de calcular los excesos reclamados, sin embargo, la parte demandada señaló en la contestación de la demanda que la jornada de trabajo era de 7:00 am a 12 pm y de 1:00 pm. a 5:00 pm, por lo que a falta de indicación expresa de la parte actora, se tiene como cierta la jornada indicada por la demandada; por lo que la jornada comprende la cantidad de 9 horas diarias y 45 horas a la semana, no excediendo la jornada del máximo permitido para los trabajadores de confianza, que establece el artículo 198 de la Ley Orgánica del Trabajo, que establece un máximo de 11 horas diarias.

Por todas las consideraciones expuestas, al haberse promovido los correos electrónicos de forma impresa, y sin haber demostrado su autenticidad, confidencialidad e integridad del mensaje a través de medios de prueba auxiliares como la exhibición, la inspección judicial o la prueba de experticia, no se les puede otorgar valor probatorio, máxime cuando fueron impugnados por la parte demandada; quedando excluidos del debate probatorio».

De la transcripción precedente, se evidencia el análisis exhaustivo que fue realizado por el sentenciador de alzada para la apreciación de los mensajes de datos que fueron promovidos en el presente caso, así como su valoración con fundamento en la sana crítica; no obstante constituyó la razón determinante para que el juzgador no les otorgara valor probatorio el hecho de que no se demostró su autenticidad, puesto que no se encontraban asociados a ningún mecanismo de seguridad que permitiera identificar el origen y autoría de los mismos; sin embargo, además de los motivos referidos a la correcta evacuación

de dicha prueba, el sentenciador concluyó que la misma no era idónea para demostrar lo pretendido por el promovente, a saber, que trabajó horas extraordinarias, puesto que recibía y enviaba mensajes de datos fuera de la jornada ordinaria, ya que no se puede evidenciar mediante la misma que los correos que le fueron enviados hayan sido recibidos de forma inmediata.

Por tal razón, se considera que el pronunciamiento realizado por el sentenciador de alzada respecto a la prueba indicada, no infringe las normas alegadas como violadas.»

2. Sentencia del 4 de febrero de 2014²⁰, se trata de un recurso de casación con ocasión al juicio que por cobro de prestaciones sociales y otros conceptos laborales (comisiones) siguió el ciudadano Julio César Revette Guillén, contra la sociedad mercantil Auto Premium, C.A.. En este caso se denunció que la recurrida dio por demostrado que el demandante percibía el pago de comisiones y que los mencionados documentos fueron impugnados por ser producidos en copia simple; que si bien es cierto que la parte actora insistió en hacerlos valer y produjo los originales, también es cierto que la parte demandada los desconoció y aquella no promovió el cotejo como lo establece el artículo 87 de la Ley Orgánica Procesal del Trabajo; que por esa razón el sentenciador debió desechar los mencionados documentos; ya que de haberlos desechado habría concluido que la parte actora no logró demostrar el salario variable alegado.

La Sala entendió que si bien el juez no había aplicado las normas de la prueba documental para el desconocimiento de este medio, el mencionado error no era determinante en el fallo, pues la recurrida estableció que el demandante devengaba un salario mixto con base en los recibos de pago de salario producidos por la demandada y otras pruebas como la testimonial y la de experticia promovidas por la actora y los recibos de pago de salario producidos por la propia demandada.

Así en cuanto a la prueba de experticia en el software de la empresa se señaló que del texto de la recurrida se desprende que la demandada no solo se negó a suministrar colaboración para la práctica de la experticia, sino que realizó actuaciones tendientes obstaculizar su práctica, en esas circunstancias, el Sentenciador, haciendo uso de su soberana apreciación, aplicando la sana crítica, interpretó la conducta de la demandada como una precisión de las afirmaciones de la parte actora en relación con las comisiones devengadas por el trabajador.

Así, la Sala concluyó:

Analizada la transcripción, se observa que la recurrida concluyó que el trabajador demandante recibía el pago de comisiones, soportando su conclusión en que: 1) la demandada por una parte alegó que aquel solo devengaba un salario fijo que se correspondía con el mínimo fijado por el Poder Ejecutivo

²⁰ <http://historico.tsj.gob.ve/decisiones/scs/febrero/160816-0060-4214-2014-11-1200.HTML>

Nacional, pero, por otra, en los recibos de pago producidos para demostrar su afirmación, no consta que el trabajador devengase el salario mínimo, sino que percibía sumas adicionales que la demandada denominaba complementos de salario; 2) la demandada obstaculizó la práctica de la experticia promovida por la parte actora, con la que se pretendía obtener los reportes de ventas de repuestos de la demandada y las comisiones generadas por dichas ventas y; 3) los testigos promovidos por la actora fueron contestes en afirmar que la demandada pagaba comisiones a los vendedores». Por las razones que anteceden, la denuncia se declaró improcedente.

3. Sentencia N° 905 del 7 de octubre de 2015²¹. Este caso versó sobre un recurso de casación con ocasión a la demanda que por cobro de acreencias laborales siguió el ciudadano Luis Rafael Pulido Salazar contra PDV Marina, S.A. En dicho caso se denunció la infracción de los artículos 4 del Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas y 78 de la Ley Orgánica Procesal del Trabajo, al *ad quem* haber valorado indebidamente pruebas promovidas por la demandante, las cuales fueron enervadas en juicio por la demandada.

En este caso la Sala estableció al analizar la situación:

Quien recurre señala, que la decisión del juez superior expresa lo que se transcribe a continuación:

(...) observa esta Alzada que en relación con los documentos promovidos macados con la letras «E», «G», «I», «J», «K», «M», «N», «Ñ», «O», «P», «Q», «T», «U», «V» y «W» (...) los mismos contienen correos electrónicos o mensajes de datos, los cuales fueron producidos en las actas procesales en formato impreso, por lo cual tienen «la misma eficacia probatoria atribuida en la ley a las copias o reproducciones fotostáticas», a tenor del único aparte del artículo 4° del Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas. Ahora bien, dichos mensajes de datos promovidos en formato impreso, resultan absolutamente inteligibles y los mismos no fueron desconocidos en su contenido por la parte contraria, la cual, erróneamente se limitó a tratar de impugnar tales mensajes de datos alegando que no pudo constatar su origen del servidor de la demandada, a través de la inspección Judicial realizada por el Tribunal A Quo, siendo que tal exigencia no está basada en norma legal alguna. Siendo ello así se les otorga valor probatorio de conformidad con el artículo 4° del Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas.» (Sic)

En este contexto, manifiesta que en la oportunidad de la audiencia de juicio, la empresa enervó todos y cada uno de los correos electrónicos que promovió la accionante en copias simples impresas a través de la impugnación de éstos, y como se ha sostenido, las copias fotostáticas o reproducidas por cualquier

21 <http://historico.tsj.gob.ve/decisiones/scs/octubre/181594-0905-71015-2015-14-880.HTML>

medio mecánico se reputarán fidedignas, siempre que se cumpla con ciertas condiciones, entre las cuales se encuentra, que no sean impugnadas por la contraparte en la oportunidad que corresponda.

En este orden de argumentación, alega que las copias impresas fueron impugnadas como se evidencia del video de la audiencia de juicio, quedando las mismas sin valor probatorio, porque si bien no promovió un medio complementario para verificar la emisión certificada de los mismos, el Tribunal de la causa acordó de oficio y a favor del accionante una inspección judicial en la sede de la empresa, donde no se demostró lo afirmado.

Finalmente, en sintonía con lo expuesto, el formalizante sostiene que el ad quem otorgó valor probatorio a las impresiones, y con fundamento en ellas, declaró el supuesto reconocimiento por parte de PDV Marina, S.A., del carácter de trabajador del ciudadano Luis Rafael Pulido Salazar, quien prestó servicios como abogado independiente en libre ejercicio como profesional, con una relación estrictamente civil, lo cual fue demostrado en la presente causa.

Para decidir se formulan las consideraciones siguientes:

(...)

El artículo 4 del Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas, dispone:

Artículo 4.- Los Mensajes de Datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos, sin perjuicio de lo establecido en la primera parte del artículo 6 de este Decreto-Ley. Su promoción, control, contradicción y evacuación como medio de prueba, se realizará conforme a lo previsto para las pruebas libres en el Código de Procedimiento Civil. (Destacado de la Sala)

Por su parte, el artículo 78 de la Ley Orgánica Procesal del Trabajo, expresa:

Artículo 78. Los instrumentos privados, cartas o telegramas, provenientes de la parte contraria, podrán producirse en el proceso en originales. Estos instrumentos podrán también producirse en copias o reproducciones fotostáticas o por cualquier otro medio mecánico, claramente inteligible, pero los mismos carecerán de valor probatorio, si la parte contra quien obra los impugnase y su certeza no pudiese constatarse con la presentación de los originales o con auxilio de otro medio de prueba que demuestre su existencia. (Destacado de la Sala)

Sobre el valor probatorio de las impresiones de los correos electrónicos, esta Sala en sentencia [Nro. 717 de fecha 2 de julio de 2010, (caso: Eleudo Ramón Pereda Urdaneta contra Suplidora Venezolana, C.A. (SUPLIVENCA)], estableció:

Los documentos aquí cuestionados son mensajes de datos, reproducidos en formato impreso.

Sobre los mensajes de datos, el Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas, en su artículo 4, dispone que tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos, y que su promoción, control, contradicción y evacuación como medio de prueba, se realizará conforme a lo previsto para las pruebas libres.

Asimismo, la citada norma dispone 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.

De manera que, con independencia de que al mensaje de datos se haya asociado o no una firma electrónica que identifique al emisor, su reproducción en formato impreso debe considerarse siempre como una copia fotostática.

Con respecto a la eficacia probatoria de las copias fotostáticas, el artículo 78 de la Ley Orgánica Procesal del Trabajo establece que carecerán de valor probatorio, si la parte contra quien obran los impugnare y su certeza no pudiese constatarse con la presentación de los originales o con auxilio de otro medio de prueba que demuestre su existencia. (Destacado de la Sala)

De la decisión anterior, se desprende que los correos electrónicos tienen la misma eficacia probatoria de una copia o reproducción fotostática, debiendo realizarse su control, contradicción y evacuación, de la forma prevista para los documentos escritos, por lo que el formato impreso de dicho medio electrónico se asemeja a una copia fotostática.

El juzgador de alzada, al momento de valorar los correos electrónicos consignados por la parte actora como medio de prueba, expresó lo siguiente:

(...) Observa esta Alzada que (...) el mismo no fue desconocido en su contenido por la parte contraria (...), se le otorga valor probatorio de conformidad con el artículo 4° del Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas. Y así se establece. (SIC) (Destacado de la Sala)

Esta Sala de Casación Social evidencia, que las documentales consignadas por el ciudadano Luis Rafael Pulido Salazar, en formato impreso, se tratan de correos electrónicos suscritos por su persona y dirigidos a PDV Marina, S.A., sin intervención de la demandada, los cuales fueron valorados por el juzgador de alzada por tener la misma eficacia probatoria que el de una copia o reproducción fotostática.

Al respecto, es necesario hacer referencia al principio de alteridad de la prueba, según el cual nadie puede procurarse una prueba a su favor sin la intervención de una persona ajena, distinta a quien pretende aprovecharse del medio, lo que implica excluir del análisis probatorio las pruebas emitidas unilateralmente por la parte promovente, principio éste que debe aplicar el juzgador aun cuando no medie impugnación de la parte no promovente. [Sentencia de la

Sala de Casación Social Nro. 313 de fecha 31 de marzo de 2011, (caso: Dani Rafael Valor contra SIDERÚRGICA DEL ORINOCO, C.A. “SIDOR”)].

En este sentido, si bien se tratan de correos electrónicos consignados en formato impreso, a los cuales se les debe dar la misma eficacia probatoria que los documentos privados, como fue expuesto supra, al ser documentales que emanan de la propia parte actora sin presentar sello ni señal de recepción de la empresa, no podía el ad quem atribuirles valor probatorio, toda vez que vulneran el principio de alteridad de la prueba. De este modo, incurre el juzgador de alzada en el vicio delatado por el recurrente en casación, lo que conlleva a declarar con lugar la presente denuncia. Así se decide. (...)”

4. En un recurso de casación con ocasión a un juicio de divorcio²², se denunció la infracción por falta de aplicación de los artículos 4, 7 y 9 del Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas, en concordancia con el artículo 1.371 del Código Civil y la violación por falsa aplicación del artículo 6 de la misma Ley.

En este caso la recurrida no le otorgó valor probatorio a los correos electrónicos los cuales fueron presentados como prueba del hecho jurídico controvertido (el abandono y excesos, sevicias e injuria grave que hace imposible la vida en común); y expresó el recurrente que de haber apreciado tales documentales, la alzada habría determinado que la demandada aceptó que la dirección de correo electrónico del cual emanaron los mensajes era suya, confesión que genera la aplicación del artículo 9 del Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas, el cual textualmente señala que:

Las partes podrán acordar un procedimiento para establecer cuándo el Mensaje de Datos proviene efectivamente del Emisor. A falta de acuerdo entre las partes, se entenderá que un Mensaje de Datos proviene del Emisor, cuando éste ha sido enviado por: 1. El propio Emisor. 2. Persona autorizada para actuar en nombre del Emisor respecto de ese mensaje. 3. Por un Sistema de Información programado por el Emisor, o bajo su autorización, para que opere automáticamente”.

Para analizar esta denuncia la Sala estableció:

Indica, que la alzada en cuanto a la experticia sobre los correos electrónicos promovidos por el actor a fin de demostrar las causales de divorcio invocadas (abandono voluntario, excesos, sevicia e injurias graves), expresamente señaló lo que de seguidas se transcribe:

²² <http://historico.tsj.gob.ve/decisiones/scs/noviembre/183172-1065-241115-2015-15-244.HTML>

(...) en lo que respecta a la causa controvertida, luego de leer la conclusión que arrojó el dictamen pericial, se desprende que no se pudo comprobar la identidad de la persona quien emitió los mensajes de correo electrónico pues los mismos carecen de firma electrónica, a pesar de que se constató que no fueron modificados ya que mantuvieron la integridad respecto a la fuente de la data original contenida en los servidores de la empresa Hotmail (sic).

(Omissis).

En base a todo lo expuesto, al artículo 4 transcrito y al artículo 16 eiusdem que reza: ‘(...) La Firma (sic) Electrónica (sic) que permita vincular al Signatario (sic) con el Mensaje (sic) de Datos (sic) y Atribuir (sic) la autoría de éste, tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa (...)’, esta Alzada (sic) desecha la presente prueba (...). (Énfasis del recurrente).

La prueba de experticia es desechada por la alzada, al considerar que la misma, por las razones antes referidas, no le genera convicción para la resolución de la presente controversia.

Ahora bien, más allá de la convicción que genere la prueba promovida, el medio por sí solo, contiene elementos concretos que responden a interrogantes que se pretenden esclarecer precisamente con la prueba indicada, en este caso con la experticia realizada a los correos electrónicos promovidos por el actor a fin de demostrar las causales de divorcio por él invocadas.

En este sentido, se desprende que una vez promovida tales documentales la demandada expresamente se opone a ellos alegando que «reconoce como suyo la dirección de correo electrónico, aportada o mencionada por la contraparte, pero igualmente desconocemos formalmente (...) estas copias impresas, pues es conocido por todos que los correos electrónicos, pueden ser alterados en su redacción por cualquier persona (...)».

De la oposición efectuada, se desprende que la demandada objeta la posibilidad de que los correos hayan sido alterados, más no afirma que los mismos efectivamente fueron modificados en su redacción o que tales misivas no hayan sido redactadas por ella.

Hecha la impugnación, la parte actora insiste en la experticia promovida para que la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) verifique la veracidad de los correos, experticia que concluye que los correos «mantuvieron la integridad respecto a la fuente de la data original contenida en los servidores de la empresa hotmail», es decir, que los mismos no fueron alterados en su contenido.

Siendo así, el artículo 9 del Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas, dispone expresamente que: (...)

Es decir, que reconocido por la demandada que la dirección de correo electrónico le pertenece, y constatado por el experto que los mismos no fueron alterados en su redacción, posibilidad a la que hace referencia la demandada, en aplicación de la norma antes transcrita debe entenderse que tales documentales provienen del emisor, y por lo tanto cumplen con el objeto de la prueba verificándose que los mensajes electrónicos promovidos no fueron modificados en su escritura.

En razón de lo anterior, constata esta Sala la falta de aplicación del artículo 9 del Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas en la que incurre la alzada, resultando procedente la presente denuncia. Así se decide.

Declarada con lugar la delación alegada, la Sala, al analizar el fondo de la controversia estableció:

(...)

Prueba de experticia

Se libró oficio a la Superintendencia de Servicio de Certificación Electrónica (SUSCERTE), a ser practicada sobre la computadora o PC de la demandada a los fines de verificar el origen, destino y veracidad del contenido de los correos electrónicos promovidos por el actor. El informe del experto fue recibido el 22 de septiembre de 2014, suscrito por el ciudadano Johnny José Bonaci Valderrama, quien fue debidamente juramentado en calidad de especialista en Informática Forense, a fin de que ratifique el contenido y firma del informe en cuanto a la experticia realizada a los correos electrónicos enviados en las siguientes fechas: 25/01/2012, 24/07/2012, 11/09/2012, 26/02/2013 y 27/02/2013. (Folios 116-128 de la primera pieza del expediente) desde la cuenta coaching_rs@yahoo.com a la cuenta larraingolf@hotmail.com.

Tal y como fue resuelto en el recurso de casación intentado, la demandada se opuso a los correos electrónicos promovidos, sin embargo, de la oposición efectuada, se desprende que la accionada objeta la posibilidad de que los correos hayan sido alterados, más no afirma que los mismos efectivamente fueron modificados en su redacción o que tales misivas no hayan sido redactadas por ella.

Pues bien, la prueba de experticia practicada, concluye, lo siguiente.

(...) Luego de haber analizado el material colectado mediante la aplicación del procedimiento forense ante descrito, cumpla con informar que aun cuando no se pudo comprobar la identidad de la persona quien emitió los mensajes de correo electrónico, debido a que no están firmados electrónicamente (...) se pudo constatar a través de la validación de las cabeceras y cuerpos de los cinco (5) correos electrónicos promovidos en el escrito de prueba, lo siguiente:

1. Integridad de la información enviada en los correos electrónicos:

Los correos electrónicos marcados desde 'B' hasta 'F', no fueron modificados, manteniendo su integridad respecto a la fuente de la data original contenida en los servidores de correo de la empresa hotmail (...).

Esta Sala le otorga valor probatorio de conformidad con lo establecido en el artículo 450 literal k) de la Ley Orgánica para la Protección de Niños, Niñas y Adolescentes en concordancia con el artículo 92 de la Ley Orgánica Procesal del Trabajo, evidenciándose que los correos electrónicos promovidos no fueron modificados o alterados en su redacción, manteniendo su integridad respecto a la fuente de la data original contenida en los servidores de correo de la empresa hotmail, es decir, resultan veraces, desprendiéndose de éstos los constantes conflictos, la ruptura grave de la relación y el irrespeto de los cónyuges”.

5. Reflexiones finales

La consagración de los derechos sociales en la Constitución de la República Bolivariana de Venezuela ha influenciado definitivamente en la elaboración de normas sustantivas y procesales sociales, logrando así un sistema armónico de protección de estos especiales derechos. Ello categóricamente se proyecta a todos los medios de prueba incluidos los electrónicos, los cuales deben analizarse atendiendo a las normas y principios establecidos en las leyes procesales tales como valoración mediante reglas de la sana crítica (libre convicción razonada), el principio de primacía de la realidad, interpretación de la conducta de las partes en la producción de medios de prueba y las normas de la prueba documental y libre previstas para esta materia.

Consideramos importante que a futuro se incluyan disposiciones normativas propias de la jurisdicción social para los medios de prueba electrónicos, con la idea de no seguir en lo posible aplicando las normas actuales que son generales y cuya tendencia es a la prueba documental negocial característica de otros tipos de procedimientos, que si bien tiene aplicación en esta área no es el único medio electrónico que se puede promover en los procedimientos sociales.

Significativos y valiosos han sido los esfuerzos que desde el año 2000 ha realizado la Sala de Casación Social del Tribunal Supremo Justicia, a través de sus magistrados y magistradas para que se dictaran normas ajustadas a la jurisdicción social, al considerar que no podían seguir aplicándose únicamente las normas del Código Civil y del Código de Procedimiento Civil, para la resolución de problemas a relaciones jurídicas que por su naturaleza son asimétricas. Así, atendiendo al mandato constitucional del artículo 21 de la Constitución de la República Bolivariana de Venezuela se ha venido dictando leyes y decisiones judiciales buscando la igualdad jurídica en forma efectiva, y empleado al proceso como un mecanismo para la realización de justicia.

El uso de las nuevas tecnologías en el procedimiento contencioso administrativo en Venezuela

Belinda Paz Calzadilla*

SUMARIO: I. Introducción. II. Uso de la tecnología en el ámbito de las citaciones y notificaciones. 1. Planteamiento general. 2. Tipos de emplazamientos: 2.1. Citación de la parte demandada 2.1.1. Demandados con las prerrogativas procesales de la República. 2.1.2. Demandados sin prerrogativas. 2.2. Notificaciones dirigidas a la PGR, Procurador del Estado y Síndicos Procuradores Municipales. 2.3. Emplazamientos al Poder Popular. 2.4. Otros emplazamientos. III. Uso de las tecnologías en las audiencias. IV. Empleo de la tecnología en el ámbito de las diligencias probatorias. V. Conclusiones

Resumen

Este ensayo analiza el uso de las nuevas tecnologías en la gestión judicial, especialmente en relación con la realización de la actividad procesal vinculada a las pretensiones que se ventilan ante la Jurisdicción Contencioso Administrativa. Para ello hemos escogido tres fases o actuaciones procesales: las citaciones, notificaciones y demás emplazamientos; las audiencias preliminares y la evacuación de las diligencias probatorias. En cada una de estas etapas encontramos experiencias prácticas del Juzgado de Sustanciación de la Sala Político Administrativa, relacionadas con la incorporación de los medios electrónicos. La identificación de las dificultades y la precisión sobre la potencialidad de las herramientas previstas en los diferentes textos legales son el primer paso para encontrar soluciones a corto, mediano y largo plazo. Bajo esta visión y en un método descriptivo, se busca ofrecer alternativas para lograr la paulatina incorporación de estos mecanismos.

Recibido: 21/1/2017 • Aceptado: 15/2/2017

* Abogada (UCAB), especialista en derecho administrativo (UCAB), especialista en derecho procesal constitucional (UMA) con diplomado en derecho procesal (JUDEX). Juez de Sustanciación de la Sala Político Administrativa. belindapaz7@hotmail.com

Palabras claves: Medios electrónicos, notificaciones electrónicas, uso de tecnología en los procesos judiciales.

Abstract

This essay examines the use of new technologies in judicial management, especially in relation to the bond with procedural activity to the actions that are filed in the contentious administrative jurisdiction. For this purpose we have chosen three phases or procedural actions: citations, notifications and other ways of notifications; the preliminary hearings and, finally, evidence. In each of these stages or actions we find practical experiences, mainly carried out by the Juzgado de Sustanciación de la Sala Político Administrativa, related to the incorporation of electronic means. The identification of the difficulties and the precision of the benefits of the tools provided in the different legal texts are the first step in finding short-, medium- and long-term solutions. Under this vision, and based on a descriptive method, we seek to offer alternatives to achieve the gradual incorporation of these mechanisms.

Key words: Electronic means. Electronic notifications. Use of technology in judicial processes.

I. Introducción

El Derecho como ciencia social dirigido a normar las reglas de conducta de una sociedad está llamado a adaptarse a las nuevas realidades que cada vez imponen retos mayores. El uso progresivo de la tecnología en todos los campos de la gestión pública viene causando importantes avances.

De hecho en Venezuela el empleo de los medios electrónicos por parte de la Administración está regulado, entre otros cuerpos normativos, en la Ley Orgánica de Administración Pública (LOAP, 2014)¹ que al hacer referencia a la implementación de estos mecanismos refiere en su artículo 11, lo siguiente:

Artículo 11: Los órganos y entes de la Administración Pública deberán utilizar las tecnologías que desarrolle la ciencia, tales como los medios electrónicos o informáticos y telemáticos, para su organización, funcionamiento y relación con las personas. Cada órgano y ente de la Administración Pública deberá establecer y mantener una página en internet, que contendrá entre otra, la información que se considere relevante, los datos correspondientes a su misión, organización, procedimiento, normativa que lo regula, servicios que presta, documentos de

¹ G.O. Extraordinaria 6.147 del 17 de noviembre de 2014.

interés para las personas, ubicación de sus dependencias e información de contactos.

Asimismo, el artículo 152 de la LOAP (2014) establece la posibilidad que tienen los órganos y entes administrativos de utilizar nuevas tecnologías, lo cual expresa de la siguiente forma:

Artículo 152: Los órganos y entes de la Administración Pública podrán incorporar tecnologías y emplear cualquier medio electrónico, informático, óptico o telemático para el cumplimiento de sus fines. Los documentos reproducidos por los citados medios gozarán de la misma validez y eficacia del documento original, siempre que se cumplan los requisitos exigidos por ley y se garantice la autenticidad, integridad e inalterabilidad de la información.

Sobre la implementación de estas herramientas tecnológicas la Sala Político Administrativa tuvo oportunidad de pronunciarse con ocasión de las notificaciones electrónicas realizadas por la Comisión de Administración de Divisas (CADIVI) y el cumplimiento de los requisitos previstos en los artículos 73 y 74 de la Ley Orgánica de Procedimientos Administrativos². A tal efecto, dispuso la referida Sala del Tribunal Supremo de Justicia³, lo siguiente:

(...) la normativa que regula el uso de estos 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 deben 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, lo que permite deducir a esta Sala que no todos los mensajes de datos que envía la Administración por medios electrónicos deben necesariamente contener los requisitos de forma y de fondo de los actos administrativos, pues estas herramientas se desarrollan y sirven de apoyo para mejorar los servicios ofrecidos a los ciudadanos, simplificando los trámites y formalidades de la actividad administrativa, y para que los interesados tengan acceso a la información sobre la gestión pública.

Conforme al criterio jurisprudencial antes citado, la normativa que rige el uso de los medios electrónicos no pretende sustituir el cumplimiento de los requisitos y formalidades que deben reunir ciertos actos administrativos para producir efectos jurídicos, sino regular los nuevos mecanismos tecnológicos para aumentar la eficiencia de la gestión pública.

Asimismo, en aquella oportunidad dispuso la Sala que los mensajes de datos obtenidos por correo electrónico, como resultado de la consulta efectuada a través del Sistema Automatizado de la Comisión de Administración de Divisas

² GO. 2.818 del 1º de julio de 1981.

³ *Vid.* sentencias SPA números 1.011 del 8 de julio de 2009, 1.437 del 8 de octubre de 2009 y 100 del 3 de febrero de 2010 y 403 del 15 de abril de 2015.

(CADIVI), no debían contener a la luz de la normativa aplicable, los requisitos de forma y de fondo de los actos administrativos, por lo que la legalidad de dichos mensajes de datos no podían impugnarse bajo el argumento de no reunir las aludidas exigencias.

De la misma manera, la Sala Político Administrativa dejó sentado en sentencia N° 1.358 del 15 de octubre de 2014 que el artículo 3 de la Providencia N° 055 emanada de la Comisión de Administración de Divisas (CADIVI) establecía un régimen especial que sometía a los usuarios a los requisitos, controles y trámites para la administración de divisas destinadas al pago de gastos de actividades académicas en el exterior, al consagrar que

los estudiantes deberán inscribirse en el Registro de Usuarios del Sistema de Administración de Divisas (RUSAD), por una sola vez y junto con la primera solicitud (...) presentaran ante el operador cambiario autorizado, la planilla obtenida por medios electrónicos...”. Por lo tanto, estimó la mencionada Sala “que el usuario debe adecuarse al mecanismo tecnológico creado por dicho órgano en la Internet, esto es el Sistema Automatizado de la Comisión de Administración de Divisas (CADIVI), a través de su página WEB “www.cadivi.gob.ve”, para realizar los trámites correspondientes a sus solicitudes de autorización de adquisición de divisas,

y, en consecuencia, concluyó el fallo en referencia que la oportunidad para pedir la nulidad de tales actos corría desde el momento que CADIVI envió el correo electrónico indicándole al interesado sobre la negativa de su solicitud de adquisición de divisas.

Tales normas no son los únicos ejemplos de nuestra legislación, ni reflejan o agotan el tema sobre la experiencia adelantada en sede administrativa⁴.

De hecho resulta pertinente destacar que Venezuela para el año 2004 ocupaba el tercer lugar en América Latina de países adelantados en el acceso global a la información. El primer puesto pertenecía a Costa Rica, mientras que en la segunda posición se situaban Argentina y México⁵.

No obstante, la experiencia registrada en sede Administrativa si bien resulta orientadora respecto a los avances que aún están por alcanzarse en los procesos judiciales, lo cierto es que ello no constituye el verdadero tema de estudio de este ensayo⁶.

⁴ El artículo 125 del Código Orgánico Tributario también refiere y autoriza la implementación de los medios electrónicos por parte de la Administración Pública.

⁵ Tales datos fueron tomados del estudio realizado por BUSQUETS, J. (2007) *Análisis Comparado del Poder Judicial Electrónico en América Latina*. Disponible en <http://www.file:///C:/users> (consultado en fecha 03 de octubre de 2016), p. 118

⁶ Para profundizar sobre los avances en sede administrativa se sugiere la lectura de AMONI, G. (2010). *Memorias. XIV Congreso Iberoamericano de Derecho e Informática*. Monterrey, Nueva León, México; así como RIVERA, M. (2014). *Revista de Derecho y Tecnología N° 15*. “El acto administrativo electrónico en Venezuela”. Universidad Católica del Táchira. San Cristóbal – Venezuela.

En efecto, las presentes líneas estarán dedicadas al análisis del uso de la tecnología en los procesos que se siguen ante la jurisdicción contencioso administrativa y al respecto debemos advertir que en este espacio no hemos tenido la misma proyección que en otras áreas del Derecho, mucho más aventajadas.

Lo expuesto quizás obedezca a la dificultad que le suma a estos procesos el cumplimiento de las prerrogativas concedidas a ciertos entes públicos, tal como explicaremos más adelante.

Habida cuenta de ello, los operadores de justicia estamos llamados a detenernos en estos planteamientos, aunque ello tenga por norte la identificación de las debilidades o dificultades, ya que en definitiva su hallazgo nos permitirá idear soluciones a corto, mediano y largo plazo.

Bajo esta dirección, conviene advertir que el desarrollo de las nuevas tecnologías en la gestión judicial en palabras del procesalista ORTELLS, M. (2002)⁷ puede abordarse bajo dos perspectivas, a saber:

- a. Las nuevas tecnologías como medio o instrumento para la realización de la actividad procesal, tanto del tribunal y de sus auxiliares, como de las partes;
- b. Las tecnologías como generadoras de otras realidades sociales y consecuentemente jurídicas, lo que supone la existencia de materias litigiosas novedosas, sobre las que versará la actividad procesal.

De tales visiones nos interesa concentrarnos en lo descrito en el literal «a», referido al empleo de las tecnologías como medio o instrumento para la realización de la actividad procesal del tribunal, sus auxiliares y las partes, todo ello en el marco de los procesos que se siguen ante la jurisdicción contencioso administrativa.

Así, encontramos que el estudio será estructurado en tres secciones que tratarán el uso de las tecnologías en ciertas fases o respecto a algunas actuaciones procesales, a saber, lo atinente a las citaciones, notificaciones y demás emplazamientos; lo concerniente a la celebración de las audiencias preliminares y por último, todo lo relativo a la práctica y evacuación de las diligencias probatorias.

Queremos advertir que el enfoque de este ensayo es meramente descriptivo, por cuanto únicamente pretendemos mostrar al lector la experiencia práctica en la atención de estos asuntos, aludiendo, en ocasiones, a casos concretos y la forma como han sido resueltos.

⁷ Citado por BUSQUETS, J. (2007) *ob. cit.* Disponible en <http://www.file:///C:/users> (consultado en fecha 03 de octubre de 2016), p. 116

II. Uso de la tecnología respecto a las citaciones, notificaciones y demás emplazamientos

1. Planteamiento general

La Ley Orgánica de la Jurisdicción Contencioso Administrativa fue aprobada en el año 2010⁸ y puso fin a una larga transitoriedad de la derogada Ley Orgánica de la Corte Suprema de Justicia, seguida por la posterior Ley Orgánica del Tribunal Supremo de Justicia (2004)⁹.

Más allá de las críticas que se han formulado al mencionado texto legal (LOJCA) -algunas justificadas y otras producto de la natural resistencia al cambio- lo que nadie puede negar es que esta regulación procedimental tuvo una nueva visión o cambio trascendental.

En este contexto, pueden resaltarse como características generales de este esquema procedimental, las siguientes notas: 1. Creación de procedimientos tipos para la tramitación de las diferentes pretensiones, lo cual propicia una sana simplificación; 2. Incorporación de audiencias en diferentes fases de los procesos, situación que facilita la realización de principios como el de oralidad e inmediación; 3. Ampliación de las facultades oficiosas de los jueces; 4. Flexibilización de los lapsos procesales; 5. Inclusión de nuevas y mayores oportunidades para promover pruebas; 6. Posibilidad de ejercer un despacho de saneamiento; 7. Incorporación de mecanismos de participación popular y, por último, 8. Una indiscutible tendencia a fomentar los medios electrónicos para la realización de algunas actuaciones procesales.

De tales aspectos, nos concentraremos en esta oportunidad en lo descrito en el numeral 8, para lo cual hay que acotar que el artículo 38 de la Ley Orgánica de la Jurisdicción Contencioso Administrativa autoriza el uso de notificaciones y citaciones electrónicas cuando prevé: *“el Tribunal podrá practicar las citaciones y notificaciones por medios electrónicos”*, advirtiendo que en tales casos las certificaciones se harán conforme al Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas, debiendo el Secretario dejar la respectiva constancia en el expediente, a los fines de que comiencen a computarse los lapsos procesales.

Por su parte, el numeral 3 del artículo 91 de la Ley Orgánica del Tribunal Supremo de Justicia (2010) consagra que de no ser posible la notificación personal, ésta podrá practicarse, entre otros medios, por

...boleta que sea enviada a través de sistemas de comunicación telegráficos, facsimilares, electrónicos y similares, en cuyo caso el Secretario o Secretaria dejará constancia en el expediente de haberla practicado. A tal efecto las partes indicarán su dirección de correo electrónico o número de fax cuando

⁹ G.O. 37.942 del 20 de mayo de 2004

⁸ G.O. 39.451 del 22 de junio de 2010

se incorporen al proceso. Al momento de librarse la boleta se ordenará su publicación en el portal electrónico del Tribunal Supremo de Justicia...

Asimismo precisa el artículo 92 de la mencionada Ley Orgánica que este tipo de notificaciones surtirán efectos “...*al quinto día de despacho siguiente a cuando su práctica conste en autos y su publicación en el portal electrónico del Tribunal Supremo de Justicia...*”.

Nótese que ambas normas (artículo 38 de la Ley Orgánica de la Jurisdicción Contencioso Administrativa y 92 de la Ley Orgánica del Tribunal Supremo de Justicia) tienen un sentido diferente, toda vez que, entre otros aspectos, la Ley Orgánica de la Jurisdicción Contencioso Administrativa no concede un lapso para entender practicada la citación o notificación, sino que declara que el cómputo correspondiente se hará inmediatamente a la constancia dejada por el secretario en el expediente. Tampoco se contempla en la Ley Orgánica de la Jurisdicción Contencioso Administrativa la necesidad de publicar la boleta en la página *web* y a diferencia de lo que ocurre con el artículo 91 de la Ley Orgánica del Tribunal Supremo de Justicia esta forma de notificaciones o citaciones no son supletorias, es decir, para el caso que no se logre la personal.

Empero, siendo que la Ley Orgánica de la Jurisdicción Contencioso Administrativa es la ley especial en la materia, debe dársele aplicación preferente, lo cual no es óbice para que en la práctica se publiquen tales boletas en la página *web* del Tribunal Supremo de Justicia, como complemento que redunde en mayores garantías para los justiciables¹⁰.

Lo anterior encuentra sustento en lo previsto en el artículo 31 de la Ley Orgánica de la Jurisdicción Contencioso Administrativa, cuando declara que las demandas tramitadas ante esta Jurisdicción se sustanciarán conforme a lo previsto en dicha Ley y “...*supletoriamente se aplicarán las normas de procedimiento de la Ley Orgánica del Tribunal Supremo de Justicia y del Código de Procedimiento Civil...*”.

Adicionalmente, no podemos dejar de lado que en el ámbito concreto del contencioso administrativo existen diferentes tipos de notificaciones, emplazamientos y llamados a juicios, algunos de los cuales se encuentran regulados en normativas especiales, que incorporan el cumplimiento de un conjunto de formalidades para considerar válidas estas actuaciones procesales.

De ahí que el estudio de estos temas debe atender a la normativa especial, a fin de determinar la compatibilidad entre las normas generales que regulan las notificaciones y citaciones electrónicas y las prerrogativas que se conceden a ciertos entes públicos para entenderlos válidamente notificados.

¹⁰ Actualmente, estas boletas son cargadas en un link de la página del TSJ identificado como “boletas” disponible en <http://www.tsj.gob.ve>.

2. Tipos de emplazamientos y notificaciones producidas en los juicios contencioso administrativos

La Ley Orgánica de la Jurisdicción Contencioso Administrativa prevé una serie de procedimientos tipos para tramitar las diferentes pretensiones que se ventilan ante esta jurisdicción. Dependiendo del procedimiento empleado, los emplazamientos varían y tienen distinta significación.

Detengámonos en la regulación de las demandas de contenido patrimonial, cuyas normas son supletorias al resto de los procedimientos.

En tales acciones una vez admitida la demanda el juez ordenará los diferentes emplazamientos para que los interesados comparezcan a la audiencia preliminar. Dicha audiencia se fija cumplidas las notificaciones y citaciones ordenadas en el auto de admisión.

Frecuentemente, estos llamados implican la citación de la parte demandada, la notificación de la Procuraduría General de la República o, si fuere el caso, del Procurador del Estado o del Síndico Procurador Municipal. También el juez puede emplazar a los consejos comunales, entes, asociaciones y demás personas vinculadas con la controversia, para que opinen sobre el juicio¹¹. Entonces, encontramos que en estos procesos se producen formas diferentes de emplazamientos, a saber:

- a. La citación de la parte demandada
- b. La notificación de la PGR o Procurador del Estado o Síndico Procurador Municipal
- c. El llamado que puede realizar el juez a los consejos comunales y demás personas vinculadas a la controversia
- d. Otros emplazamientos

Analicemos cada una de estas modalidades por separado a objeto de evaluar la compatibilidad de los regímenes especiales con lo alusivo a las citaciones y notificaciones electrónicas, previsto tanto en la Ley Orgánica del Tribunal Supremo de Justicia (2010) como en la Ley Orgánica de la Jurisdicción Contencioso Administrativa (2010).

2.1. La citación de la parte demandada

En cuanto a este aspecto, es menester indicar que la forma de llevar a cabo la citación varía según se trate de un ente público con las prerrogativas de la República o un particular. Por ello, dividiremos esta sección en dos partes, la atinente a aquellos demandados que tienen las mismas prerrogativas de la República y la de los restantes que en contraposición no las poseen.

¹¹ *Vid.* art. 58 de la LOJCA

2.1.1. Demandados con las prerrogativas procesales de la República

A partir de la sentencia N° 727 del 12.07.2010, relacionada con el recurso de revisión ejercido por el Instituto Venezolano de los Seguros Sociales (IVSS) contra la decisión de la Sala Político Administrativa del Tribunal Supremo de Justicia N° 1.082 del 21.07.2009, la Sala Constitucional dejó sentado respecto a las citaciones de los entes públicos que poseen las mismas prerrogativas de la República, lo siguiente:

[T]odos los órganos jurisdiccionales deben velar por la fiel aplicación de estas prerrogativas [procesales], en el sentido de aplicarlas preferentemente a las normas procesales ordinarias, ello en virtud de que persiguen resguardar los intereses patrimoniales de la República y de todos aquellos entes públicos sobre los que aquella tenga derechos, no con el objetivo de evitar la responsabilidad del Estado, sino de impedir afectaciones en el cumplimiento de sus fines fundamentales establecidos en el ordenamiento jurídico, mediante el equilibrio entre los derechos de las personas y las potestades y obligaciones de la República. (Vid. 902/2004 caso: C.V.G. Bauxilum C.A.).

Ahora bien, respecto a los privilegios procesales de los entes descentralizados funcionalmente, en especial los institutos autónomos, el artículo 97 de la Ley Orgánica de la Administración Pública (publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 37.305 del 17 de octubre de 2001, vigente para el momento de la interposición de la demanda), disponía que *“Los Institutos Autónomos gozarán de los privilegios y prerrogativas que la ley nacional acuerde a la República, los estados, los distritos metropolitanos o municipios”*. A lo que vale agregar, que actualmente, bajo el vigente Decreto con rango y fuerza de Ley Orgánica de la Administración Pública (publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 5.890 Extraordinario, del 31 de julio de 2008), los institutos autónomos continúan gozando de los mismos privilegios y prerrogativas de la República, conforme lo prevé el artículo 98 de dicha ley.

De manera, que estos entes públicos gozan de los privilegios procesales otorgados a la República (...).

En este contexto, observa la Sala, que el artículo 81 del Decreto con Rango, Valor y Fuerza de Ley de Reforma Parcial del Decreto con Fuerza de Ley Orgánica de la Procuraduría General de la República, dispone que las *“Las citaciones al Procurador o Procuradora General de la República para la contestación de la demanda deben ser practicadas por oficio, acompañado del libelo y de los recaudos producidos por el actor. El oficio debe ser entregado personalmente al Procurador o Procuradora General de la República, o a quien esté facultado por delegación”*.

Conforme a dicha norma, surge la obligación para todos los órganos jurisdiccionales, que cuando se haya intentado una demanda contra la República o cualquier otro ente público -que por remisión expresa de la ley goce de los privilegios procesales otorgados a la República- de notificar mediante oficio.

En otras palabras, tales citaciones se efectuarán conforme a las previsiones del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Procuraduría General de la República (2016), cuyo artículo 93 dispone que estas actuaciones “...*deben ser practicadas por oficio, acompañado del libelo y de los recaudos producidos por el actor...*”. También advierte la norma que estos oficios se entregaran personalmente al Procurador o Procuradora General de la República o a quien esté facultado para recibirlo.

Con relación a esto último la Sala Político Administrativa hizo una importante precisión en sentencia N°1.205 del 5 de octubre de 2011, al establecer que a falta de estos funcionarios podía aceptarse la recepción de los documentos por la persona que se desempeñe como su asistente, adjunto, o secretaria. Textualmente, destacó la referida Sala lo que a continuación se transcribe:

Finalmente, resulta oportuna la presente decisión para puntualizar que cuando las citaciones y notificaciones relacionadas con las acciones o recursos previstos en la Ley Orgánica de la Jurisdicción Contencioso Administrativa, estén dirigidas a los funcionarios responsables de los órganos superiores de dirección de la Administración Pública Central (Presidente o Presidenta de la República, Vicepresidente Ejecutivo o Vicepresidenta Ejecutiva, Ministros o Ministras y Viceministros o Viceministras), así como a las máximas autoridades de los demás órganos de rango constitucional, o a los Gobernadores y a los Alcaldes, éstas se entenderán practicadas (sean citaciones o notificaciones) no sólo cuando hayan sido entregadas personalmente al funcionario citado, sino también cuando hayan sido recibidas por la persona que se desempeñe como el o la asistente, el adjunto o la adjunta o la secretaria o secretario de dichos funcionarios, en la oficina del Despacho de los mismos, el cual deberá ser identificado debidamente por el Alguacil, con su nombre y apellido, número de cédula de identidad y cargo que ocupa, así como el lugar, fecha y hora de la citación.

Esto se justifica dado el conocimiento que posee este Máximo Tribunal de la dificultad a la que cotidianamente se enfrentan sus Alguaciles para obtener acceso a los Despachos de los altos funcionarios del Estado, dadas las altas responsabilidades y funciones que éstos cumplen, lo cual muchas veces imposibilita la práctica de sus citaciones personales¹².

Por lo tanto, la implementación de las citaciones electrónicas cuando el demandado es un ente público con las prerrogativas de la República debe incorporar el cumplimiento de todas y cada una de las formalidades descritas, a

¹² Vid. Sentencia de la SPA N° 1.205 del 5 de octubre de 2011 disponible en <http://www.tsj.gob.ve>

saber: remisión electrónica de los recaudos presentados por el actor y certificación de su recepción por parte de los funcionarios autorizados.

En la actualidad los medios electrónicos no han sido implementados para el supuesto descrito (citaciones de entes públicos con las prerrogativas procesales de la República), por las razones siguientes:

- Falta de digitalización de los expedientes, lo cual dificulta la remisión de los recaudos que deben acompañarse a los oficios correspondientes.
- Ausencia del certificado de firma electrónica que permita dar certeza tanto al remitente como a su destinatario y
- El volumen de información que sería enviada a la dirección electrónica correspondiente. La cantidad de recaudos que deben acompañarse a estos emplazamientos, tornaría ineficaz e inapropiado el uso del sistema común de correos electrónicos. En efecto los emails soportan un tráfico de información de aproximadamente 5 megas, lo cual es claramente insuficiente e inseguro. Para solucionarlo habría que crear un sistema especial que permita superar estos obstáculos. De hecho en España se adoptó un sistema conocido con el nombre de *Lexnet* que permite compartir y tolerar este tráfico de información con bastante confiabilidad¹³.

También podría evaluarse la experiencia del Tribunal Fiscal mexicano el cual a partir del 07 de agosto de 2011 comenzó un plan piloto conocido con el nombre de “Sistema del Juicio en Línea”¹⁴.

En este contexto, autores como LILLO, R. (2010)¹⁵ describen la experiencia de Inglaterra en el uso de los juicios electrónicos, de la siguiente manera:

Ejemplos de aplicaciones que permiten la tramitación automática vía Web de procesos es posible encontrar en Inglaterra. A través del llamado sistema County Court Bulk Centre, las grandes empresas de crédito tramitan las causas de ejecución de deudas monetarias, transfiriéndolas de los tribunales locales a una oficina en Northhampton encargada de procesar todos estos casos de manera automática mediante una aplicación computacional. Producto de esa buena experiencia, se implementó un sistema de Demanda Monetaria en Línea o MCOL por su sigla en inglés (Money Claim on-Line), el cual permite a los consumidores y comerciantes, demandante y demandados interponer sus demandas de cobro de dinero bajo un proceso completamente basado en tecnología Web.

¹³ Se sugiere la consulta de CABALLERO DE LA TORRE, M. (2004) “Lexnet un sistema de información para la notificación telemática y la cooperación”. Consultado en fecha 04 de octubre de 2016 y disponible en la dirección electrónica: http://www.csi.map.es/csi/tecniimap/tecniimap_2004/comunicaciones/tema_04/4_021.pdf, p. 21.

¹⁴ Para mayor información se sugiere ingresar a la página <http://www.tfja.mex>

¹⁵ Consultado en www.ijusticia.org/docs/LOBOS.pdf en fecha 04 de octubre de 2016

Habida cuenta de ello y mientras se encuentra el sistema más conveniente para nuestro país, lo cierto es que en la actualidad no contamos con la tecnología para implementar estas herramientas, lo cual no significa que en un futuro cercano estas limitaciones no puedan ser superadas. Es decir, que bajo ningún concepto tenemos que renunciar a la idea de emplear los medios electrónicos para estos casos, sólo que su implementación y funcionamiento requiere además de la iniciativa del legislador, de la disponibilidad presupuestaria y voluntad de los operadores jurídicos.

En respaldo de la urgencia e importancia de invertir y dedicar tiempo a estos temas, debemos señalar que dentro de la jurisdicción contencioso administrativa es común la presencia de tribunales cuyas circunscripciones judiciales abarcan todo el territorio nacional o regiones del mismo¹⁶, lo cual obliga con frecuencia al otorgamiento de comisiones a tribunales de otros ámbitos competenciales para practicar notificaciones, citaciones o cualesquiera otras diligencias probatorias, todo lo cual redundará en un mayor retraso en la sustanciación de estos juicios. Máxime cuando los comisionados en muchos casos no están familiarizados con las formalidades y especificidades de este tipo de actuaciones.

De manera que, la implementación de un sistema electrónico permitiría llegar a todas las regiones sin necesidad de acudir a las comisiones judiciales que –como se explicó antes– recargan de trabajo y desvían la atención de tribunales de otros ámbitos competenciales.

2.1.2. Demandados sin las prerrogativas de la República

Ciertamente en estos casos se reducen buena parte de los obstáculos para el uso de los medios electrónicos, pero actualmente también enfrentamos limitaciones que han impedido el empleo de estos mecanismos en dichos supuestos. Veamos algunas de ellas:

En primer lugar, conviene plantearse cuál sería la vía más idónea para obtener una fuente segura de los correos electrónicos de los sujetos intervinientes en el proceso. Especialmente, este tema cobra relevancia cuando nos referimos a la citación del demandado, ya que en este escenario resulta importante tener certeza sobre la confiabilidad de la dirección electrónica.

A tal efecto, cabe destacar que la legislación vigente en materia contencioso administrativa no despeja la interrogante, ya que si bien el numeral 3 del artículo 91 de la Ley Orgánica del Tribunal Supremo de Justicia (norma de aplicación supletoria a los juicios que se siguen ante este ámbito competencial) declarará que para el uso de los medios electrónicos “*las partes indicarán su dirección de correo electrónico o número de fax, cuando se incorporen al proceso...*”,

¹⁶ Este asunto fue corregido en parte por la LOJCA, la cual modificó la competencia territorial de la mayoría de estos tribunales, propiciando un mayor acercamiento de la justicia a los administrados.

no deja de ser menos cierto que la lectura integral de la norma puede llevarnos a la conclusión de que el supuesto descrito se refiere sólo a las notificaciones excluyendo de su *ratio* a la citación del demandado.

No obstante, aun en el caso que se admitiera una interpretación amplia de la norma, basada en una equiparación entre los términos notificación y citación, lo cierto es que según la redacción del artículo en referencia (num. 3 del art. 91 LOTSJ), los medios electrónicos sólo podrían usarse cuando no sea posible gestionarla de forma personal, tal como se desprende del encabezado de la disposición *in comento* que precisa “[l]as notificaciones de las partes, interesados o interesadas deberán ser practicadas en principio de forma personal...”

Por otro lado, se observa que si decidiéramos acudir a la aparente amplitud que ofrece el artículo 38 de la Ley Orgánica de la Jurisdicción Contencioso Administrativa, el cual en su texto alude tanto a notificaciones como a citaciones y al mismo tiempo no las supedita al agotamiento de la forma personal, lo cierto es que la disposición en comento advierte que tales diligencias “...se harán de conformidad con lo establecido en el Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas...”.

Ahora bien, cuando verificamos el Texto normativo mencionado en el señalado artículo 38, apreciamos que el mismo contiene algunas reglas para la determinación de la recepción de un mensaje de datos que merecen ser destacadas. Específicamente, conviene citar el artículo 11 del Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas:

Artículo 11. Salvo acuerdo en contrario entre el Emisor y el Destinatario, el momento de recepción de un Mensaje de Datos se determinará conforme a las siguientes reglas:

1. Si el Destinatario ha designado un sistema de información para la recepción de Mensajes de Datos, la recepción tendrá lugar cuando el Mensaje de Datos ingrese al sistema de información designado.
2. Si el Destinatario no ha designado un sistema de información, la recepción tendrá lugar, salvo prueba en contrario, al ingresar el Mensaje de Datos en un sistema de información utilizado regularmente por el Destinatario.

Según la norma transcrita la recepción del mensaje de datos se determina de dos maneras que varían en atención a si el destinatario ha designado o no un sistema de información para la recepción. Así, tenemos que para el primer caso (cuando el sistema ha sido designado) la recepción tiene lugar a partir del ingreso del mensaje al sistema de información; mientras que en el segundo escenario (no hay designación) dicho mensaje se entiende recibido al ingresar a un sistema de información utilizado regularmente por el destinatario.

En la mayoría de los casos los jueces no tienen para el momento de practicar la citación del demandado, e incluso posteriormente, los elementos necesarios

para establecer si el receptor ha escogido o no ese sistema de información o incluso si se trata de uno usado regularmente.

No obstante, el artículo 13 del Decreto en comento, ofrece una solución interesante, al precisar lo que a continuación se transcribe:

Artículo 13. El Emisor de un Mensaje de Datos podrá condicionar los efectos de dicho mensaje a la recepción de un acuse de recibo emitido por el Destinatario.

Las partes podrán determinar un plazo para la recepción del acuse de recibo. La no recepción de dicho acuse de recibo dentro del plazo convenido, dará lugar a que se tenga el Mensaje de Datos como no emitido.

Cuando las partes no establezcan un plazo para la recepción del acuse de recibo, el Mensaje de Datos se tendrá por no emitido si el Destinatario no envía su acuse de recibo en un plazo de veinticuatro (24) horas a partir de su emisión. Cuando el Emisor reciba el acuse de recibo del Destinatario conforme a lo establecido en el presente artículo, el Mensaje de Datos surtirá todos sus efectos.

Basándonos en lo previsto en la norma supra transcrita podríamos concluir que el juez puede supeditar la recepción del mensaje a la acreditación de un acuse de recibo emitido por el destinatario; sin embargo, en la mayoría de los casos las personas que son citadas en juicio no realizan, ni están obligadas a hacerlo, este tipo de conductas de manera voluntaria. De ahí que la efectividad de tales mecanismos no debería quedar condicionada a la buena voluntad del citado, sino que al efecto es pertinente idear los mecanismos para que el sistema emita la certificación de la recepción con las suficientes garantías.

Aún así tendríamos el inconveniente de establecer cuál sería la fuente oficial para obtener la dirección electrónica del citado. Sobre el particular conviene destacar que en la actualidad cuando no se cuenta con el domicilio del demandado bien sea porque el actor lo desconoce o debido a que la dirección suministrada por éste al Alguacil está desactualizada, resulta inexacta o incompleta, la práctica que viene implementando el Juzgado de Sustanciación de la Sala Político Administrativa consiste en oficiar a determinados organismos del Estado para que remitan los datos que al efecto aparecen en sus archivos¹⁷.

Dicha práctica si bien genera retrasos que se ven con bastante frecuencia en las demandas de nulidad que involucran la presencia de un denunciante, lo cierto es que sería una alternativa para obtener el correo oficial del demandado.

Por lo tanto, debe insistirse en la búsqueda de mecanismos que permitan optimizar el intercambio de esta información, ya que a pesar de la entrada en vigencia 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 (2012), aún no se ha explotado en toda su potencialidad las herramientas que dicho cuerpo normativo consagra.

17 Normalmente se acude al SENIAT, IVSS, RNC, CNE y CADIVI

En efecto, el texto legal bajo estudio define como objeto de esa ley el establecimiento de “...las bases y principios que regulan el acceso e intercambio electrónico de datos, información y documentos entre los órganos y entes del Estado, con el fin de garantizar la implementación de un estándar de interoperabilidad...”.

Por su parte, el artículo 4 del cuerpo normativo en referencia define la interoperabilidad como la “[c]apacidad de los órganos y entes del Estado de intercambiar por medios electrónicos datos, información y documentos de acceso público”.

De manera que, a través del operador de la interoperabilidad se podría acceder a la Plataforma Nacional de Servicios de Información Interoperables de manera más efectiva y rápida, sin que ello implique un trámite formal de envío de oficios, tal como se sigue hoy día.

Empero, mientras se avanza en la eficaz herramienta que está prevista en el indicado cuerpo normativo, el Juzgado de Sustanciación de la Sala Político Administrativa viene incorporando en los oficios dirigidos al CNE, SENIAT, IVSS, RNC, entre otros, la dirección de correo electrónico oficial del mencionado órgano jurisdiccional¹⁸, a los fines de la remisión *on line* de la información, si así lo estiman pertinente los entes requeridos.

Por lo tanto, la falta de una plataforma tecnológica acorde ha sido el único impedimento para que las normas mencionadas alcancen su plena efectividad. De hecho en la práctica el mencionado Juzgado de Sustanciación de la Sala Político Administrativa se vio en la obligación de negar una solicitud de citación electrónica, por la ausencia de elementos tecnológicos que permitieran garantizar el cumplimiento de su finalidad¹⁹.

Habida cuenta de lo anterior, confiamos que en un futuro cercano estas dificultades puedan ser superadas, ya que la experiencia alcanzada en sede administrativa –como indicamos al inicio de este estudio– resulta orientadora y alentadora para llevar a cabo esa tarea en el ámbito judicial.

A pesar de lo descrito, el aludido Juzgado de Sustanciación viene incorporando algunas medidas tendientes a la progresiva inclusión de estos mecanismos.

Muestra de ello es que en la actualidad los expedientes llevados por dicho órgano jurisdiccional tienen una carátula en cuya contraportada se identifican las partes y demás intervinientes, con la finalidad de que aquellos litigantes que deseen colocar sus datos (correo electrónico y fax) reciban, a través de éstos, las boletas que se libran a lo largo del juicio.

Cabe acotar, que el envío de estos documentos no sustituye ni exime al tribunal del deber de aplicar los sistemas tradicionales de notificación, pero

¹⁸ spad.juzsu@tsj.gob.ve

¹⁹ Se sugiere la consulta de la decisión del Juzgado de Sustanciación de la Sala Político Administrativa N° 136 del 17 de abril de 2013, disponible en la página web del Tribunal Supremo de Justicia.

constituye una medida complementaria que va generando la cultura para el empleo a futuro de estos medios.

También debemos indicar que esta iniciativa ha sido recibida con beneplácito y cada vez son más los litigantes que se suman a la idea de suministrar sus correos electrónicos. Incluso en algunos casos los incorporan a sus escritos.

2.2. De las notificaciones dirigidas al Procurador General de la República, Procuradores de Estados y Síndicos Procuradores Municipales

En cuanto a este punto damos por reproducidas muchas de las consideraciones realizadas al momento de analizar las citaciones de entes públicos con las prerrogativas procesales de la República.

En efecto, las notificaciones extendidas a la Procuraduría General de la República, Procuradores Generales de los Estados y Síndicos Procuradores Municipales, están revestidas del cumplimiento de una serie de formalidades que hacen en el estadio actual de las cosas incompatible el régimen de notificaciones electrónicas con el previsto tanto en la Ley Orgánica de Jurisdicción Contencioso Administrativa como en la Ley Orgánica del Tribunal Supremo de Justicia.

Prueba de ello es que el artículo 38 de la Ley Orgánica de la Jurisdicción Contencioso Administrativa dispone que las notificaciones electrónicas surten efecto desde la constancia dejada en el expediente por el Secretario, situación que no toma en cuenta los lapsos de suspensión o plazos concedidos por la Ley Orgánica de la Procuraduría General de la República para entender notificado a dicho funcionario.

Similar situación ocurre con el artículo 92 de la Ley Orgánica del Tribunal Supremo de Justicia, el cual consagra que estos tipos de notificaciones (electrónicas) surtirán efecto a partir del quinto día de despacho siguiente a haberse practicado, aspecto que –como se destacó líneas atrás– contradice las prerrogativas procesales de la República consagradas en la LOPGR.

Por lo tanto, aun cuando puedan superarse los obstáculos para tramitar estas notificaciones a través de los medios electrónicos, lo cierto es que la manera de computar los lapsos no puede ser la descrita en los artículos 38 de la Ley Orgánica de la Jurisdicción Contencioso Administrativa ni en el mencionado artículo 92 de la Ley Orgánica del Tribunal Supremo de Justicia, razón por la cual la implementación de estos sistemas de notificaciones debe aparejar una regulación acorde con la normativa especial en la materia o en su defecto corresponderá a la jurisprudencia ocuparse de estos temas, a través de una interpretación que permita conciliar las prerrogativas del Estado con las normas que disponen las reglas para el inicio de los lapsos procesales cuando la diligencia ha sido practicada electrónicamente.

A la fecha no se han emitido pronunciamientos en ese sentido, lo cual resulta lógico debido a la falta de implementación de los medios electrónicos para estas formas de notificaciones; sin embargo, superadas las dificultades estudiadas en las líneas que anteceden, estos temas con seguridad serán materia de estudio.

2.3. De los emplazamientos dirigidos a los representantes del poder popular y demás asociaciones que hacen vida en la comunidad

En el esquema de democracia participativa consagrado en la Constitución de la República Bolivariana de Venezuela el pueblo no se limita a elegir representantes, sino que actúa activamente en el ejercicio del Poder Público.

De esta manera, encontramos que los distintos textos legales contemplan – como parte de un desarrollo constitucional– diferentes formas de participación popular.

Evidentemente, que la jurisdicción contencioso administrativa no escapa a ello, más aún cuando los asuntos que se atienden en este ámbito competencial tienen que ver con la actividad del Estado en todas sus expresiones, lo cual incide en la esfera jurídica de los ciudadanos.

Así, tenemos que la ley que rige dicha jurisdicción desde el año 2010, establece diversos procedimientos tipos para enmarcar las diferentes pretensiones o peticiones que se dirigen, en primera instancia, ante los tribunales.

En este contexto, pueden identificarse tres grandes grupos o categorías de procedimientos, a saber:

1. El de las **demandas de contenido patrimonial** (artículos 56 y siguientes), utilizado para exigir una condenatoria de tipo pecuniario, por lo que resulta común su empleo, aunque no exclusivamente, en materia de indemnización por daños y perjuicios y en el ámbito contractual.
2. El **procedimiento breve** (artículos 65 y siguientes) empleado para reclamar por la deficiente prestación de un servicio público, las llamadas vías de hecho y las abstenciones. Este procedimiento, debido a su carácter sumario no puede involucrar pretensiones de contenido patrimonial.
3. Por último, el **procedimiento de las demandas de nulidad, interpretación y controversias administrativas** (artículos 76 y siguientes).

Cada uno de estos procedimientos tienen normas rectoras encargadas de propender la participación popular dentro de los procesos contenciosos administrativos.

Muestra de ello lo constituye el artículo 58 de la LOJCA, situado en el capítulo concerniente al procedimiento de demandas de contenido patrimonial. Dicha norma prevé textualmente lo siguiente:

El Juez o Jueza podrá, de oficio o a petición de parte, convocar para su participación en la audiencia preliminar a las personas, entes, consejos comunales, colectivos o cualquier otra manifestación del poder popular de planificación, control y ejecución de políticas y servicios públicos, cuyo ámbito de actuación se encuentre vinculado con el objeto de la controversia, para que opinen sobre el asunto debatido.

De ser procedente su participación se les notificará, de conformidad con lo dispuesto en el artículo 37 de esta Ley, fijándose la audiencia cuando conste en autos la notificación respectiva.

Las personas y entes antes señalados, no requerirán representación ni asistencia de abogado. El Juez o Jueza facilitará su comparecencia y deberá informarles sobre los aspectos relevantes de la controversia.

Igualmente, el numeral 3 del artículo 68 de la LOJCA, contempla esta forma de participación dentro de los procedimientos breves y, más específicamente en el marco de las acciones por reclamación de servicios públicos al disponer, lo siguiente:

Artículo 68. En el caso previsto en el numeral 1 del artículo 65 de esta Ley [reclamos por la omisión, demora o deficiente prestación de los servicios públicos], deberá notificarse a: (...) 3. Cualquier otra persona o ente público, privado o del Poder Popular relacionado con el asunto, a solicitud de parte o a juicio del Tribunal.

Asimismo, el numeral 3 del artículo 78 *eiusdem*, también permite insertar la referida intervención dentro de las demandas de nulidad, interpretación y controversias administrativas, cuando dispone que el juez o jueza puede notificar a cualquier otra persona, órgano o ente que deba ser llamado a la causa por exigencia legal o a criterio del Tribunal, dentro de cuya categoría cabe incluir a los representantes del poder popular.

Ahora bien, dependiendo del procedimiento de que se trate pudiera pensarse que la participación popular es diferente, ya que para el caso de las demandas de contenido patrimonial el referido artículo 58 dispone que el llamado será a la audiencia preliminar y la notificación se efectuará conforme al artículo 37 de la LOJCA, es decir de manera personal.

En cambio respecto las acciones por omisión, demora o deficiente prestación de un servicio público, la ley (art. 68.3 LOJCA) sólo impone el deber de llamarlos

cuando sea necesario, pero no precisa a qué fines y bajo cuáles formalidades deberá hacerse el emplazamiento.

Por último, cuando se trate de la demandas de nulidad, controversias administrativas y recursos de interpretación, cabe acotar que el último aparte del artículo 78 de la LOJCA sí contempla la forma como deberán practicarse estas notificaciones, esto es, “...*mediante oficio que será entregado por el o la Alguacil en la oficina receptora de correspondencia de que se trate...*”, precisando además, que en estos casos dicho funcionario “...*dejará constancia, inmediatamente, de haberlo notificado y de los datos de identificación de la persona que recibió el oficio...*”.

Ahora bien, al margen de las diferencias que podrían plantearse respecto a la forma de hacer efectiva este tipo de participación, dependiendo del procedimiento en cuestión, conviene precisar que en todos los escenarios la intervención de los representantes del Poder Popular puede plantear problemas prácticos de envergadura.

Algunos de ellos ya han sido atendidos por el Juzgado de Sustanciación de la Sala Político Administrativa. Específicamente me referiré a la decisión N° 53 dictada el 19 de febrero de 2014, donde se estableció que la notificación personal de todos y cada uno de los consejos comunales que hacían vida en una localidad podía acarrear, de cara a circunstancias concretas, violaciones al derecho a la tutela judicial efectiva de los accionantes, razón por la cual los jueces estaban llamados a ponderar en cada caso las situaciones específicas que lo rodean, a fin de conciliar el derecho a la participación ciudadana con el referido derecho a la tutela judicial efectiva.

En todo caso, la búsqueda de tales soluciones genera a su vez interrogantes que se vinculan con el uso y acceso a los medios electrónicos. Dichos planteamientos se relacionan, entre otros, con los siguientes puntos:

- a. ¿A quién solicitar información a fin de conocer cuáles son las instancias del Poder Popular que operan en un determinado Municipio?
- b. ¿Podrían los consejos comunales emitir su opinión vía electrónica en lugar de apersonarse a las audiencias y demás actuaciones del proceso?

Sobre el particular es menester destacar que en un intento por recoger la información a nivel nacional de los consejos comunales que hacen vida en cada una de las comunidades, el Tribunal Supremo de Justicia conjuntamente con el Ministerio del Poder Popular para la Comunas y los Movimientos Sociales creó una plataforma de consulta por parte de los jueces, a los fines de conocer los consejos comunales registrados.

De este modo, tales funcionarios pueden solicitar la asignación de un usuario y clave que permite consultar los consejos comunales registrados en un determinado sector; sin embargo, la data sólo incluye el teléfono de sus voceros,

siendo que la mayoría no tienen una sede física, es decir, se les conoce como itinerantes.

Ahora bien, la elección de los voceros dura dos años, por lo que la información en referencia se desactualiza con facilidad. Asimismo, hemos tenido casos concretos donde la localidad relacionada con la controversia involucra más de 283 consejos comunales registrados²⁰, lo cual hace inviable su ubicación vía telefónica y la debida acreditación en el expediente del cumplimiento de la referida diligencia.

A lo anterior debemos sumar la dificultad que representa el traslado a Caracas para personas de escasos recursos, a los fines de presenciar e intervenir en una audiencia que se llevará a cabo en el Juzgado de Sustanciación de la Sala Político Administrativa o directamente ante la mencionada Sala cuando se trata de las audiencias de juicio.

De ahí que el aludido Juzgado ha implementado mecanismos para darle efectividad a estos llamados y al mismo tiempo facilitar a los voceros su participación dentro de los procesos contencioso administrativo. Tales prácticas han aparejado la necesidad de acudir a nuevas tecnologías.

Así, encontramos que el emplazamiento de los consejos comunales se viene haciendo a través de los Consejos Locales de Planificación Pública, por ser los órganos de enlace entre las instancias de Poder Público y las comunidades, en cuya conformación se incluyen a representantes del Poder Popular. En este contexto, se les solicita a los aludidos Consejos de Planificación que informen y difunda entre los representantes del Poder Popular la dirección electrónica del Juzgado de Sustanciación, a fin de que aquellos ciudadanos interesados en el objeto de la controversia puedan emitir su opinión *on line*²¹.

La alternativa descrita otorga una herramienta electrónica que propende el derecho de rango constitucional referido a la participación ciudadana en los asuntos públicos.

También hemos requerido la colaboración del Ministerio del Poder Popular para las Comunas y los Movimientos Sociales, a fin de que carguen en su página *web* la boletas dirigidas a los consejos comunales, a objeto de que estos se informen sobre las controversias seguidas ante la Sala y de ser el caso emitan su opinión vía *on line* o personalmente a través de su comparecencia en juicio.

²⁰ Vid. decisión del Juzgado de Sustanciación de la SPA N° 53 del 19.02.2014

²¹ Un ejemplo de lo descrito fue la experiencia tenida en un caso que involucraba un asunto relacionado con el Archipiélago Los Roques donde se utilizó al Jefe de Oficina Insular como enlace para la ubicación del consejo comunal que hace vida en el lugar. Vid. Oficio N° 908 de 29.09.2016, librado por el Juzgado de Sustanciación de la SPA en el expediente N° 2016-0466. Actualmente, todos los oficios librados a los Consejos Locales de Planificación Pública con la finalidad de que éstos emplacen a los consejos comunales incluyen una coetilla en la que se les solicita informen a los voceros la dirección electrónica del Juzgado de Sustanciación de la Sala, para que, de estimarlo pertinente, emitan su opinión vía *on line*.

Tales mecanismos nos han permitido llegar con mayor eficacia a las comunidades y al mismo tiempo le ha brindado a los ciudadanos una herramienta sencilla a través de la cual pueden hacer valer su postura en juicio, todo lo que redundará en un efectivo cumplimiento de la democracia participativa consagrada constitucionalmente.

2.4. Otros emplazamientos

Por último, no podemos dejar de lado los llamados y notificaciones que se extienden a los peritos y demás auxiliares de justicia. Con toda seguridad podemos afirmar que en este ámbito específico se han podido implementar con mejores resultados los medios electrónicos.

Corroboramos lo expuesto el hecho que el Juzgado de Sustanciación de la Sala Político Administrativa viene practicando las notificaciones de los defensores *ad-litem*, intérpretes públicos, peritos y demás auxiliares de justicia designados, vía electrónica.

Muestra de ello lo constituyen las decisiones 383 y 108 del 1º de diciembre de 2015 y 31 de marzo de 2016, respectivamente, en las cuales el referido órgano jurisdiccional ordenó estas notificaciones a través de los correos electrónicos aportados por los auxiliares de justicia al momento de su designación o juramentación²². De hecho en la última de las mencionadas decisiones la notificación fue extendida con la finalidad de que tales expertos aclararan el informe pericial consignado en el expediente, razón por la cual se dejó sentado que una vez que la Secretaria estampara la respectiva nota de haberse cumplido con el envío de las boletas, así como sus publicaciones en el portal electrónico del Tribunal Supremo de Justicia, comenzaría a discurrir un lapso de cinco (5) días de despacho, a objeto de que estos auxiliares de justicia aclararan el informe pericial consignado.

Similar situación se produjo con ocasión de la notificación extendida a un defensor *ad-litem*, la cual fue ordenada vía electrónica, tal como se desprende del auto del Juzgado de Sustanciación de la Sala Político Administrativa N° 133 del 21 de abril de 2016.

Cabe destacar que el Juzgado de Sustanciación también ha recibido cartas de aceptación de los diferentes expertos y demás auxiliares de justicia, a través de los medios electrónicos. Concretamente, vía fax o correo electrónico, supuestos en los cuales la Secretaria del órgano jurisdiccional estampa una nota en el expediente y consigna los recaudos que acreditan su cumplimiento.

²² En el acta de juramentación de experto de fecha 6.10.2016 levantada en el Exp. 2014-1285 (nomenclatura de la SPA), relacionada con el Caso: C.E. Minerales de Venezuela S.A vs. Ministerio del Poder Popular para el Proceso Social del Trabajo, el auxiliar de justicia suministró en ese acto su correo electrónico a los efectos de cualquier notificación.

De manera que en cuanto a este particular se ha avanzado sin problema en el uso de estos mecanismos. El éxito pudiera responder a la naturaleza y finalidad de estas notificaciones que, generalmente, involucran una participación sobre la designación de un cargo. En consecuencia, no es de extrañar que si el auxiliar de justicia tiene interés en desempeñar la función encomendada, facilite los medios para que fluya su emplazamiento.

Habida cuenta de ello, confiamos que esta experiencia puede ser el inicio de las situaciones que se susciten en el futuro con relación a los demás intervinientes en el juicio.

III. Uso de la tecnología en las audiencias

Específicamente al Juzgado de Sustanciación le compete atender las denominadas audiencias preliminares reguladas en el marco de las demandas de contenido patrimonial.

Tales audiencias son grabadas y agregadas al expediente en versión disco compacto, todo lo cual permite su reproducción ante el juez de mérito.

Con frecuencia, las partes consignan un CD a fin de que se proceda a la reproducción de la audiencia, lo cual es acordado a través de un auto de similar redacción a aquellos que ordenan la expedición de copias certificadas.

Sin embargo, se presenta la inquietud referida a si las partes pueden solicitar la transcripción del contenido del audio. Tal asunto fue abordado por el mencionado Juzgado en el expediente 2014-0901 con motivo del cual se otorgaron copias mecanográficas de la respectiva audiencia.

Para proveer sobre la solicitud descrita se utilizó como fundamento lo establecido en el segundo aparte del artículo 189 del Código de Procedimiento Civil, según el cual a petición de parte u orden del juez se puede realizar la versión escrita del contenido de una grabación, a través del Secretario o algún amanuense bajo la dirección de aquél, o por alguna otra persona natural o jurídica, bajo juramento de cumplir fielmente su contenido. De ahí que en el caso concreto se ordenó a la Secretaría del Juzgado la transcripción de la misma.

Otro tema que preocupa, relacionado con la incorporación de estos sistemas de grabación, es la preservación del CD y más aún de la calidad del audio que ellos contienen.

Para garantizar estos aspectos tanto el entonces Presidente de la Sala Político Administrativa (2015), como la actual Presidenta ordenaron, a través del Departamento de Informática del Tribunal Supremo de Justicia, la elaboración de un respaldo informático de estos audios, lo cual permite solventar cualquier contingencia que pudiera plantearse relacionada con la destrucción, deterioro o extravío de los CD.

Asimismo, se observa que la incorporación de estas y otras tecnologías plantea nuevos retos que deberán ser resueltos por los operadores jurídicos. En

este contexto, se presenta como interesante el estudio sobre la posibilidad de llevar a cabo estas audiencias a través de video conferencia.

Sobre el particular, debemos acotar que a la fecha el Juzgado de Sustanciación de la Sala Político Administrativa no ha tenido oportunidad de atender este planteamiento, por lo que no existe una experiencia práctica que ofrecer en ese sentido.

Sin embargo, lo que sí ha sucedido es que algunos participantes de las audiencias solicitan permiso para reproducir videos durante su desarrollo, así como también piden el apoyo audiovisual para mostrar presentaciones que permitan ilustrar sus exposiciones, lo cual ha sido permitido, tomando en cuenta –entre otras razones - que tales herramientas redundan en un mayor ejercicio del derecho a la defensa de las partes.

Lo descrito ha sido experimentado en otras latitudes y así lo refiere LILLO, R. (2010)²³, cuando destaca lo siguiente:

Ejemplos de utilización de TIC en audiencia como herramientas para la información entregada en audiencia encontramos en Singapur. En primer lugar, se establecieron varias Technology Courts (Cortes Tecnológicas) para facilitar la presentación de evidencia y promover mayores niveles de eficiencia en las audiencias, para lo cual se mantienen 5 tribunales, de diversos tamaños, para ser usados en casos con necesidades tecnológicas específicas, en los cuales las partes tienen acceso a tecnología audiovisual de punta. En segundo lugar, se dispone del Mobile Info-Tech Trolley Services, consistente en un carro móvil para complementar el uso de computadores portátiles y otros asistentes personales digitales. Este Trolley o carro, incluye un proyector, pantalla para proyectar, visualizador, grabador de video cassette (VCR), de DVD o de VCD y una televisión. Esto ayuda a que la instalación tecnológica pueda ser movida entre las distintas salas de la cortes y promueve a que los abogados utilicen presentaciones multimedia y Power Point, incluso cuando las audiencias no son llevadas a cabo ante las Cortes Tecnológicas.

Actualmente, si bien no contamos con unos equipos fijos instalados en el auditorio donde se llevan a cabo las audiencias preliminares que atiende el Juzgado de Sustanciación de la Sala Político Administrativa, no deja de ser menos cierto que estos se encuentran disponibles en el Tribunal Supremo de Justicia, a través de la solicitud que debe canalizarse por vía del Departamento de Informática, así como la Gerencia General. En todo caso, las partes que quieran servirse de estos equipos deben manifestarlo con anterioridad al Tribunal, a objeto de realizar los trámites concernientes a su uso.

Asimismo, el auditorio de Sala Plena ubicado en la PB del Tribunal Supremo de Justicia cuenta con una pantalla y demás herramientas que permiten la realización de video conferencias, las cuales pueden ser empleadas, una vez

23 *Ob cit*, p. 128

obtenidas las autorizaciones correspondientes, tal como ocurrió en el marco de la evacuación de una prueba testimonial, cuya realización detallaremos en el título siguiente.

IV. Empleo de la tecnología en las diligencias probatorias

Este tema puede abordarse bajo varias perspectivas, a saber el uso de la tecnología como medios de pruebas y el empleo de ésta para la evacuación de algunos medios de prueba.

En esta ocasión sólo me referiré al segundo de los planteamientos, relacionado con la incorporación de los avances tecnológicos en la evacuación de algunos medios de prueba.

Sobre el particular conviene describir la experiencia del Juzgado de Sustanciación de la Sala Político Administrativa con motivo de la evacuación de una prueba testimonial, la cual había sido admitida sin citación, fijándose la oportunidad para que tuviera lugar la deposición del testigo, de conformidad con lo dispuesto en el artículo 483 del Código de Procedimiento Civil; sin embargo, el abogado promovente de la prueba y el testigo comparecieron al Tribunal, días antes de la realización del aludido acto, a objeto de manifestar y acreditar que el testigo en cuestión tenía programado un viaje al exterior y no regresaría al país hasta dentro de seis (6) meses, razón por la cual pidió, en primer lugar, que se adelantara la fecha establecida para su deposición, o, en su defecto, se tomara la misma por los medios electrónicos. Tales solicitudes fueron atendidas por el mencionado órgano jurisdiccional mediante auto N° 190 del 30 de junio de 2016²⁴, en el que expresamente se estableció, lo siguiente:

Al respecto, importa poner de relieve que la fijación de la oportunidad para el examen de los testigos promovidos en un proceso, es un mandato legal contemplado en el artículo 483 del Código de Procedimiento Civil, que en modo alguno puede ser considerado “*un formalismo*”. En efecto, la razón de ser de dicho precepto obedece a la necesidad de garantizar que la parte contra quien pretende hacerse valer la prueba testimonial de que se trate, conozca la oportunidad en que podrá -de estimarlo- ejercer el control de la prueba, como manifestación plena del derecho a la defensa, de expreso rango constitucional.

De modo que, adelantar la oportunidad de la declaración de un testigo, a través de la figura de la habilitación, sin que la contraparte pueda tener conocimiento oportuno de tal circunstancia, atenta contra el ejercicio del control de la prueba, que en el caso de la prueba testimonial se traduce en la institución de la repregunta de los testigos, la cual forzosamente debe llevarse a cabo en la oportunidad en que tenga lugar la celebración del acto, a tenor de lo previsto en el artículo 485 del Código de Procedimiento Civil.

Con fundamento en lo expuesto, esta Juzgadora NIEGA, por improcedente, la solicitud formulada en esta misma fecha por la representación judicial de los

24 Disponible en <http://www.tsj.gob.ve>

recusantes, de habilitar “*el tiempo necesario el día de hoy*” para que el testigo Julio Natalio Carrazana Lazarovic rinda su declaración en la articulación probatoria de autos. Así se declara.

No obstante lo anterior, se advierte que el abogado Julio Carrazana Gallo pidió que “*en caso de considerar pertinente este Tribunal (...) evacuar el testigo, pudiese realizarlo a través de medios informáticos*”, a cuyo objeto indicó una dirección de correo electrónico. Asimismo, cabe destacar que la parte recusante acompañó a su diligencia copia de “*Recibo de boleto electrónico*” con el fin de acreditar la circunstancia alegada, a saber, el inminente viaje del testigo Julio Natalio Carrazana Lazarovic pautado para el 6 de julio de 2016 y cuyo regreso se extiende hasta el mes de marzo de 2017.

Atendiendo al referido pedimento, vista la consignación en autos del boleto *in commento*, así como el tiempo durante el cual el prenombrado ciudadano se encontrará fuera de la República Bolivariana de Venezuela, este Juzgado de Sustanciación, procediendo con el fin de garantizar la tutela judicial efectiva y el derecho de las partes a traer al proceso las pruebas que juzguen pertinentes, acuerda realizar el examen del testigo Julio Natalio Carrazana Lazarovic a través de video-conferencia. Así se establece.

Dicho acto se llevará a cabo en el día y hora fijados en la citada decisión N° 189 del 29 de junio de 2016, en el Auditorio Anexo al de la Sala Plena, ubicado en la Planta Baja de este Tribunal Supremo de Justicia; y para su realización, será enviado el enlace correspondiente al correo electrónico aportado por el solicitante (...)

Cabe destacar que dicha prueba fue finalmente evacuada y a los fines de dejar constancia del testimonio en el expediente se ordenó la transcripción de la grabación, de conformidad con lo establecido en el artículo 189 del Código de Procedimiento Civil, el cual en su extracto pertinente contempla:

Las declaraciones de las partes, las posiciones juradas, las declaraciones de testigos y cualesquiera otras diligencias del Tribunal que deban hacerse constar en acta, podrán ser tomadas mediante el uso de algún medio técnico de reproducción o grabación del acto, por disposición del Tribunal o por solicitud de alguna de las partes. En estos casos, la grabación se mantendrá bajo la custodia del juez, el cual ordenará realizar la versión escrita de su contenido por el Secretario o algún amanuense bajo la dirección de aquél, o por alguna otra persona natural o jurídica, bajo juramento de cumplir fielmente su contenido. En todo caso, el Secretario, dentro de un plazo de cinco días agregará al expediente la versión escrita del contenido de la grabación, firmada por el Juez y por el Secretario. Si ninguna de las partes hiciere objeción al acta, señalando expresamente alguna inexactitud, la misma se considerará admitida, pasados que sean cuatro días de su consignación en los autos. En caso de objeciones, el Juez fijará día y hora para la revisión del acta con los interesados, oyendo nuevamente la grabación. De lo resuelto por el Juez en ese acto, no habrá recurso alguno.

De lo anterior se desprende que el juez cuenta con cinco días de despacho para consignar en el expediente la aludida transcripción, la cual de no ser impugnada dentro de los cuatro días de despacho siguientes, conduce a que se le considere admitida en todas sus partes.

Igualmente, importa destacar que la utilización de estos medios es posible siempre que la persona que debe rendir declaración cuente con un equipo dotado de la cámara y micrófono necesarios para poder establecer el contacto, a través del enlace que previamente le es enviado a su correo electrónico.

Por otro lado, se debe tener en cuenta que el auditorio que posee los equipos para llevar a cabo estas video conferencias está ubicado en la PB del Tribunal Supremo de Justicia, razón por la cual, tales solicitudes deben canalizarse con tiempo a objeto de que se gestionen las autorizaciones pertinentes.

Adicionalmente, conviene precisar que el uso de las nuevas tecnologías plantea, también, otras realidades, a las cuales los operadores jurídicos deben dar respuesta. Una de ellas sería, ¿cómo podría comprobarse la identidad del testigo que declarará a través de video conferencia?

En el caso mencionado, la anterior inquietud fue despejada, debido a que el testigo compareció al Tribunal días antes de emprender su viaje y en compañía del abogado promovente solicitó, en primer lugar, que se adelantara la evacuación de la prueba o, en su defecto, que ésta se tomara por los medios electrónicos, todo lo cual permitió identificarlo con las debidas garantías.

Sin embargo, pensemos en el caso de que la prueba de testigos sea promovida para ser evacuada a través de video conferencia. ¿Debe el promovente indicar el correo electrónico del testigo?, ¿cómo tenemos la certeza de que la cuenta electrónica suministrada es la oficial?, ¿bajo qué parámetros el tribunal puede establecer la identidad del testigo?, ¿debido a la diferencia de horarios, la prueba podría evacuarse fuera de las horas de despacho del Tribunal?

Estas y otras interrogantes deberán ser atendidas, según las circunstancias concretas que se presenten. En todo caso, el objetivo de este ensayo no es desviar la atención a esos temas, aunque obligatoriamente ellos vienen a la mente, en la medida que se avanza en la progresiva incorporación de los medios electrónicos en las diferentes fases de los procesos judiciales.

Otro aspecto vinculado con las diligencias probatorias en el cual se ha introducido el uso de los medios electrónicos es el atinente a la evacuación de los informes requeridos a Instituciones y Oficinas Públicas. En tales casos, se suministra la dirección de correo oficial del Juzgado de Sustanciación de la Sala, para que la información sea remitida vía *on line*, de estimarlo necesario el órgano o ente requerido.

De manera que, tales mecanismos son algunos ejemplos de la implementación de los medios electrónicos por parte del Juzgado de Sustanciación, los cuales han encontrado cabida en diferentes fases o etapas procesales, según ha sido expuesto en las líneas que anteceden.

V. Conclusiones

Las nuevas tecnologías están y deben seguir utilizándose en toda la gestión pública, ya que ello permite mejorar la prestación del servicio y en el caso concreto del Poder Judicial optimiza la tramitación de los procesos judiciales.

La jurisdicción contencioso administrativa aun cuando ha avanzado en la aprobación de Textos Legales que incorporan los medios electrónicos, en la práctica sigue enfrentado dificultades para su utilización, las cuales tienen que ser identificadas a objeto de idear soluciones a corto, mediano y largo plazo.

Conviene destacar que Venezuela para el año 2004 ocupaba la tercera posición en América Latina de países adelantados en el uso de las tecnologías para la gestión pública. De hecho, en sede administrativa hemos obtenido importantes avances, mencionados en la parte introductoria de este ensayo.

En el campo específico de la gestión judicial, se advierte que en la última década se han llevado a cabo esfuerzos que merecen ser reconocidos y comentados.

Prueba de ello es que antes del año 2000 no era posible consultar en línea las decisiones del Alto Tribunal de Justicia, así como otras actuaciones que actualmente son publicadas en la página *web*.

En paralelo se aprecia que la mayoría de la legislación aprobada en la última década se suma a la tendencia de incorporar estas herramientas electrónicas en el desenvolvimiento de la Administración de justicia.

Sin embargo, la potencialidad de los mecanismos previstos en estos textos legales no ha sido explotada en toda su dimensión, por razones de diversa índole, las cuales deben ser analizadas y superadas a objeto de evitar que esta regulación normativa sea lo que comúnmente se le denomina letra muerta.

La identificación de las posibles debilidades no debe sumergirnos en el pesimismo, ni desalentarnos respecto al uso de estos mecanismos, por el contrario, los operadores jurídicos estamos llamados a compartir estas experiencias para conjugar esfuerzos que nos orienten hacia la solución.

El Juzgado de Sustanciación de la Sala Político Administrativa del Tribunal Supremo de Justicia ha tomado partido por la progresiva incorporación de estos medios. Prueba de ello, son las notificaciones dirigidas a los auxiliares de justicia, las cuales se vienen practicando de forma electrónica.

Igualmente, se han atendido planteamientos jurídicos propios del empleo de las tecnologías, y al mismo tiempo se ha hecho uso de estas herramientas electrónicas para la evacuación de ciertos medios probatorios.

Por otro lado, conviene destacar que las nuevas tecnologías han jugado un papel protagónico al momento de hacer efectiva en juicio la participación del Poder Popular, pues en aras de cumplir con el mandato constitucional relativo a acercar la justicia a los administrados se han brindado soluciones tecnológicas para que los consejos comunales emitan su opinión sobre una determinada controversia.

En similar sentido se ha hecho uso de esa tecnología para llevar a cabo la obtención de los domicilios de alguno de los sujetos procesales cuando sus direcciones son inexactas, se han desactualizado o se desconocen. En estos escenarios se oficia a ciertos organismos públicos para que remitan los datos que aparecen en sus registros. Para facilitar la obtención de esta información se ha puesto a la orden la dirección electrónica del órgano jurisdiccional.

Sabemos que tales medidas no son la solución definitiva a estos temas pero en el estadio actual mejoran su desenvolvimiento.

No obstante, confiamos que en un futuro cercano las herramientas contempladas 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 (2012) puedan emplearse en toda su potencialidad.

Sin embargo, mientras se producen los cambios necesarios es indispensable el aprovechamiento de los recursos y medios existentes.

Tampoco podemos perder de vista que el estudio de estos asuntos está llamado a ser una constante no sólo por la manera vertiginosa como avanza la tecnología, sino por el hecho de que el empleo de estas herramientas soluciona ciertos problemas, pero al mismo tiempo apareja la necesidad de resolver otros que se generan como consecuencia de su implementación.

Por lo tanto, las reflexiones que ofrecemos no agotan el tema, por el contrario, dan inicio a otros estudios, nuevos planteamientos y futuras investigaciones.

Posiblemente, a algunos le parezca utópica la idea de un proceso digital, pero aun asumiendo que ello sea cierto, lo cual dudo, ya que en algunos países hay experiencias al respecto, tal como ha sido mencionado en este ensayo, debemos tener presente que en palabras de DESCARTES “[d]os cosas contribuyen a avanzar: ir más de prisa que los otros o ir por el buen camino”²⁵. En mi opinión, vamos por buen camino.

25 DESCARTES, R. (1596-1650) Filósofo y matemático francés.

Domicilio fiscal electrónico obligatorio para la notificación de comunicaciones o actos administrativos emanadas de la Administración Tributaria venezolana

Mariana del V. Buitrago Rodríguez*

SUMARIO: I. Introducción. II. Tipos de domicilios a los efectos fiscales establecidos en el Código Orgánico Tributario del año 2014. 1. Domicilio de las personas naturales. 1.1. Reglas generales. 1.2. Domicilio en Venezuela de las personas naturales, para la práctica de las actuaciones de la Administración Tributaria. 2. Domicilio de las personas jurídicas y demás entes colectivos. 2.1 Regla general. 2.2. Domicilio en Venezuela de las personas jurídicas y demás entes colectivos, para la práctica de las actuaciones de la Administración Tributaria. 3. Práctica de las actuaciones administrativas tributarias, en personas domiciliadas en el extranjero. III. El domicilio fiscal electrónico obligatorio para la notificación de comunicaciones o actos administrativos. 1. Notificación de comunicaciones o actos administrativos tributarios. 1.1. Notificación. 1.2. Notificaciones tributarias. 1.3. Comunicaciones y actos administrativos tributarios. 1.3.1. Comunicaciones tributarias. 1.3.2. Actos administrativos tributarios. 2. Domicilio fiscal electrónico obligatorio. 2.1. Generalidades. 2.2. Definición del domicilio fiscal electrónico obligatorio. 2.3. Fallas del domicilio fiscal electrónico obligatorio que atentan contra el derecho a la defensa del administrado. IV. Consideraciones finales.

Resumen

Este artículo comprende el estudio del domicilio fiscal electrónico obligatorio dispuesto en el Código Orgánico Tributario vigente; tal figura jurídica-fiscal, se

Recibido: 28/1/2017 • Aceptado: 5/3/2017

* Abogada egresada de la Universidad Católica del Táchira. Especialista en Derecho Mercantil opción Tributos Empresariales, Universidad de los Andes (Venezuela). Profesora asociada de la Universidad de Los Andes. Email: buitragomariana@gmail.com

distingue por ser un mecanismo utilizado para imponer al administrado, notificaciones de comunicaciones y actos administrativos emanados de la Administración Tributaria. Para ello, se planteó enumerar los tipos de domicilios establecidos en el Código Orgánico Tributario; describir el domicilio fiscal electrónico obligatorio previsto en el Código Orgánico Tributario vigente así como los tipos de comunicaciones y actos administrativos que pueden notificarse con este tipo de domicilio; y finalmente, identificar los vacíos jurídicos del artículo 34 del Código Orgánico Tributario vigente. El método de estudio fue una investigación documental, con metodología de carácter descriptivo. Se llegó a la conclusión que la figura del domicilio fiscal bajo estudio crea inseguridad jurídica, que atenta contra el derecho a la defensa del administrado.

Palabras claves: Domicilio fiscal. Notificaciones tributarias. Comunicaciones tributarias. Actos administrativos tributarios. Domicilio fiscal electrónico obligatorio.

Abstract

This article includes the study of the compulsory electronic tax domicile, established in the current Organic Tax Code; Such legal-fiscal figure, is distinguished by being a mechanism, used to impose on the administered, notifications of communications and administrative acts emanating from the Tax Administration. For this, it was proposed to list the types of domiciles established in the Tax Code; Describe the compulsory electronic tax domicile provided for in the current Organic Tax Code as well as the types of communications and administrative acts that can be notified with this type of address; And finally, identify the legal gaps of Article 34 of the current Tax Code. The method of study was a documentary research, with descriptive methodology. It was concluded that the figure of the tax domicile under study creates legal insecurity, which undermines the right to defend the administration.

Keywords: Tax address. Tax notifications. Tax communications. Tax administrative acts. Mandatory electronic tax address.

I. Introducción

La gestión de la Administración Pública a nivel mundial ha virado gracias a la irrupción de las Tecnologías de la Información y las Comunicaciones; ello para mitigar el exceso de trámites burocráticos, así como, procedimientos lentos y dispendiosos, dentro de las actividades de gobernanza, en los diferentes niveles básicos de la Administración.

Así pues, la mayoría de los países del orbe, dentro de su organización territorial de la Administración Pública, en sus distintos niveles (nacional, estatal y municipal), y en sus diversos órganos de actuación, incluyen en las actividades

de gestión de gobierno y la modernización en su hacer, a través de la implementación y uso de las Tecnologías de la Información y las Comunicaciones.

Ello brinda al ciudadano una mejora en los servicios públicos y la consecuencial eficacia en la gobernanza, gracias al gobierno electrónico o, el *e-government*, que:

...incluye todas aquellas actividades basadas en las modernas tecnologías informáticas, en particular Internet, que el Estado desarrolla para aumentar la eficiencia de la gestión pública, mejorar los servicios ofrecidos a los ciudadanos y proveer a las acciones del gobierno de un marco mucho más transparente que el actual¹.

Bajo esta orientación, el gobierno electrónico en Venezuela, encuentra en la Constitución de la República² su mejor aliada; al considerar de interés público, la ciencia, la tecnología, la innovación y sus aplicaciones; y los apunta, como instrumentos fundamentales, para el desarrollo social, político y económico del país; por ello, las innovaciones implementadas por el Estado venezolano, al servicio de los ciudadanos a través del uso de las Tecnologías de la Información y las Comunicaciones, optimizan las gestiones públicas, acercando a los administrados a la Administración Pública.

Dentro de las actividades de gestión pública, la Administración Nacional, contempla entre sus competencias: la creación, organización, recaudación, administración y control de una serie de impuestos de carácter nacional³; gestiones que lleva a cabo a través de la Administración Tributaria Nacional, la cual debe ceñirse a las consideraciones establecidas en el apartado del sistema tributario⁴ del texto constitucional vigente.

En Venezuela, gracias al mandato constitucional previsto el Artículo 110 *ejusdem*, la Administración Tributaria Nacional y los dispositivos legales vigentes que la rigen, deben incorporar el uso de las Tecnologías de la Información y las Comunicaciones para facilitar las operaciones y actividades de la gestión de gobierno. En tal sentido, el Código Orgánico Tributario⁵ dispone⁶ en la Sección

1 CASTOLDI, Pablo: "El gobierno electrónico como un nuevo paradigma de la Administración". *Prudentia Iuris*, N° 55. Buenos Aires. Universidad Católica Argentina, 2002, pp. 112-117, especialmente p. 112.

2 Véase art. 110 Constitución de la República Bolivariana de Venezuela (1999). Con la enmienda N° 1 de fecha 15 de febrero de 2009. Gaceta Oficial de la República Bolivariana de Venezuela N° 5.908 Extraordinario, del 19 de febrero de 2009.

3 Véase art. 156 numeral 14 Constitución de la República Bolivariana de Venezuela (1999). Con enmienda ...*op. cit.*

4 Véase el arts. 316 y 317, Constitución de la República Bolivariana de Venezuela (1999). Con enmienda ...*op. cit.*

5 Código Orgánico Tributario (2014). Gaceta Oficial de la República Bolivariana de Venezuela N° 6152, Extraordinario, del 18 de noviembre de 2014.

6 Artículo 34 Código Orgánico Tributario (2014)... *op. cit.* "La Administración Tributaria podrá establecer un domicilio fiscal electrónico obligatorio para la notificación de comunicaciones

IV, Capítulo III, Título II, la facultad que tiene la Administración Tributaria, de establecer un domicilio fiscal electrónico obligatorio, con preferencia a los demás domicilios establecidos en el referido instrumento legal.

Con base en lo anterior, el presente trabajo plantea que el alcance de dicha discrecionalidad por parte de la Administración Tributaria, al establecer un domicilio fiscal electrónico obligatorio, se convierte en una situación problemática. En efecto, según el artículo 110 del Código Orgánico Tributario, la facultad concedida a la Administración Tributaria, para establecer un domicilio fiscal electrónico, tanto para la notificación de comunicaciones o actos administrativos a los sujetos pasivos, tiene un carácter obligatorio; considerándose que esa facultad discrecional raya en la arbitrariedad, y ensombrece la gestión de gobernanza electrónica que debe llevar a cabo la Administración Tributaria.

II. Tipos de domicilio a los efectos fiscales establecidos en el Código Orgánico Tributario del año 2014

En su *stricto sensu*, el domicilio según la RAE⁷ es concebido como el “*lugar en que legalmente se considera establecido alguien para el cumplimiento de sus obligaciones y el ejercicio de sus derechos*”. En tal sentido, el domicilio, debe ser considerado como el lugar o asiento en el que puede ser ubicada legalmente tanto una persona natural, como una persona jurídica.

La doctrina extranjera, define al domicilio fiscal, como: *el lugar de localización del obligado tributario en sus relaciones con la Administración, siendo fijado en la normativa tributaria por importantes razones de seguridad y de eficacia en la aplicación de los tributos*⁸.

De allí que en la esfera jurídico-tributaria, el domicilio fiscal otorga seguridad jurídica para localizar a los obligados o sujetos pasivos de la relación jurídica tributaria; es decir, el domicilio fiscal, debe ser concebido como el ámbito espacial, a los efectos tributarios y de la práctica de las actuaciones de la Administración Tributaria.

En virtud de lo anterior, es menester señalar que el Código Orgánico Tributario, dispone desde el artículo 30 al artículo 33 *ejusdem*, las generalidades de la figura del domicilio fiscal, así como los tipos de domicilios fiscales que a efectos de actuaciones de la Administración Tributaria establece la ley; es decir,

o actos administrativos, que requiera hacerle a los sujetos pasivos. Dicho domicilio electrónico tendrá preferencia respecto de los previstos en los artículos 31, 32 y 33 de este código. Sin perjuicio de lo previsto en los artículos 31, 32 y 33 de este Código, la Administración Tributaria Nacional, a los únicos efectos de los tributos nacionales, podrá establecer un domicilio especial para determinados grupos de contribuyentes o responsables de similares características, cuando razones de eficiencia y costo operativo así lo justifiquen”.

⁷ Disponible en: <http://dle.rae.es/?id=E6cyAL3> [Consulta: 2017, enero 15].

⁸ Francisco Manuel MELLADO BENAVENTE: *Todo procedimiento fiscal 2006-2007*, S.A. CISS, 2007, p. 123.

el domicilio fiscal de persona natural en Venezuela; el domicilio fiscal de personas jurídicas y demás entes colectivos en Venezuela; así como el domicilio en persona domiciliada en el extranjero.

No obstante, el artículo 34 del Código Orgánico Tributario, dispone la potestad de la Administración Tributaria de establecer un domicilio fiscal electrónico obligatorio. Dicho domicilio, debe considerarse una variante para determinar el lugar o espacio no físico del sujeto pasivo u obligado de la relación jurídica tributaria, a través de notificaciones de comunicaciones o actos administrativos, realizadas por medio del uso de las Tecnologías de la Información y las Comunicaciones.

1. Domicilio de las personas naturales a los efectos fiscales

1.1. Reglas generales

Para considerar a una persona natural domiciliada en Venezuela, a los efectos tributarios, se requiere, según lo establecido en el Código Orgánico Tributario⁹, verificar el cumplimiento de ciertas reglas generales, que se reducen a: un tiempo establecido en ley, y la permanencia dentro del territorio nacional.

La persona natural, debe tener una estancia dentro del territorio nacional, no inferior a ciento ochenta y tres (183) días continuos o, discontinuos en un año calendario o, en el año inmediatamente anterior al del ejercicio al cual corresponda determinar el tributo.

Además, se considera igualmente domiciliada una persona natural, a los efectos tributarios, que ha establecido su residencia o lugar de habitación en Venezuela. Exceptuando, aquellas personas naturales, que en el año calendario permanezcan en otro país, por un período continuo o discontinuo de más de ciento ochenta y tres (183) días, y den testimonio en documento fehaciente de autoridad competente del Estado del cual acrediten, haber adquirido la residencia, para efectos fiscales en ese otro país.

De la misma manera, los venezolanos que desempeñen en el exterior servicios, funciones, representaciones diplomáticas, oficinas consulares, representaciones permanentes y las misiones temporales, o cargos oficiales de la República, de los estados, de los municipios o de las entidades funcionalmente descentralizadas, y que perciban remuneración de cualquiera de estos entes públicos.

⁹ Véase artículo 30 del Código Orgánico Tributario (2014) ... (*op. cit.*)

1.2. Domicilio en Venezuela de las personas naturales, para la práctica de las actuaciones de la Administración Tributaria

A los efectos tributarios y para la práctica de las actuaciones de la Administración Tributaria venezolana, en personas naturales, se tendrá como domicilio:

a. El lugar donde desarrollen sus actividades civiles o comerciales; esta máxima, responde a la orientación del domicilio en materia civil¹⁰. En efecto, si la persona natural, tiene más de un sitio en el que realice actividades civiles o comerciales, se tendrá como domicilio el lugar donde desarrolle su actividad principal.

b. El lugar de su residencia; regla que “*somete toda la materia imponible a la ley del lugar donde reside el sujeto*”¹¹. En este sentido, se debe respetar lo dispuesto en el artículo 31 del Código Civil¹², siempre que, la persona desarrolle tareas bajo relación de dependencia; vale decir, no tenga actividad comercial, o, civil como independiente. Por el contrario, si el obligado tributario tiene una actividad comercial o civil y actúa como independiente, y no fuere conocido el lugar donde esta actividad se desarrolle, la Administración Tributaria, entiende como domicilio su residencia.

c. El lugar donde ocurra el hecho imponible; siempre que sea imposible aplicar los criterios *supra* señalados, referidos a la territorialidad o la residencia.

d. El lugar que elija la Administración Tributaria; siempre que exista más de un domicilio, según lo dispuesto en las reglas antes mencionadas y soportadas en el Artículo 31 del Código Orgánico Tributario, o sea imposible determinarlo en función de los criterios referidos en el artículo bajo estudio.

2. Domicilio de las personas jurídicas y demás entes colectivos

2.1. Regla general

El criterio general para considerar a una persona jurídica *verbigratia* sociedad de personas (sociedad en nombre colectivo, sociedad en comandita); o sociedad de capitales (sociedad anónima, sociedad de responsabilidad limitada); y demás entes colectivos (asociaciones, fundaciones entre otros),

¹⁰ Artículo 27 del Código Civil (1982). Gaceta Oficial de la República Bolivariana de Venezuela N° 2.990 Extraordinaria, del 26 de julio de 1982: “El domicilio de una persona se halla en el lugar donde tiene el asiento principal de sus negocios e intereses”.

¹¹ Luis O. FERNÁNDEZ: Criterio de la Territorialidad y de la Residencia, un análisis crítico <http://www.estudio-contable-fd.com.ar/articulos-impuestos/impuesto-ganancias/criterios-territorialidad-residencia> [Consulta: 2017, enero 23].

¹² Artículo 31 del Código Civil (1982)... *op. cit.*: “La mera residencia hace las veces de domicilio respecto de las personas que no lo tienen conocido en otra parte”.

domiciliados en Venezuela según la ley adjetiva tributaria vigente¹³, es constituir en el país el tipo social a través del cumplimiento de las formalidades legales¹⁴; sin embargo, si el ente, está constituido en el extranjero, la norma establece que se hayan domiciliado en la República, conforme a la ley.

2.1. Domicilio en Venezuela de las personas jurídicas y demás entes colectivos, para la práctica de las actuaciones de la Administración Tributaria

A los efectos tributarios y para la práctica de las actuaciones de la Administración Tributaria venezolana, en personas jurídicas y demás entes colectivos, se tendrá como domicilio según el artículo 32 del Código Orgánico Tributario:

a. El lugar donde esté la dirección o administración efectiva de la persona jurídica, o demás entes colectivos; siendo éste, *“la sede o reciento en que ejerce la dirección y gestión de la actividad”*¹⁵. Ello, concurda con la primera parte del artículo 28 del Código Civil venezolano, sin que se deba considerar la salvedad dispuesta en el referido artículo.

b. El lugar donde se halle el centro principal de su actividad; presupuesto que aplica, cuando haya sido imposible ubicar la dirección o administración efectiva de la persona jurídica o ente colectivo.

c. El lugar donde ocurra el hecho imponible; siempre que sea imposible aplicar los criterios *supra* señalados; por lo que se tomará en cuenta, el lugar de acaecimiento de las circunstancias materiales del presupuesto establecido en la ley tributaria y que origina el nacimiento de la obligación tributaria.

d. En caso de existir más de un domicilio, o, cuando sea imposible determinarlo, la Administración Tributaria, tiene la potestad de elegir un domicilio.

3. Práctica de las actuaciones administrativas tributarias, en personas domiciliadas en el extranjero

La Administración Tributaria, practicará sus actuaciones en personas sean naturales o jurídicas, domiciliadas en el extranjero, tomando en cuenta las siguientes consideraciones previstas en el artículo 33 del Código Orgánico Tributario:

¹³ Artículo 30.5. del Código Orgánico Tributario (2014)... *op. cit.*: “Se consideran domiciliados en la República Bolivariana de Venezuela para los efectos tributarios: 5. Las personas jurídicas constituidas en el país, o que se hayan domiciliado en él, conforme a la Ley”.

¹⁴ Véase el artículo 19 del Código Civil (1982)... *op. cit*

¹⁵ <https://edukavital.blogspot.com.ar/2015/07/significado-de-domicilio-fiscal.html> [Consulta: 2017, enero 24].

a. El domicilio de su representante en el país; en este sentido, debe entenderse que, el representante o apoderado (persona natural o jurídica) en el país, actúa bajo un mandato o representación, es decir, por cuenta de otra persona que está domiciliada en el extranjero. En otras palabras, *“esa persona está autorizada legalmente a través de un poder, para representar y en su caso obligar a otra persona”*¹⁶ no domiciliada en Venezuela.

En consecuencia, en el caso de una persona domiciliada en el extranjero, debe tomarse en cuenta, el domicilio de su representante en el país, siguiendo las reglas establecidas en los apartados del domicilio de persona natural y del domicilio de persona jurídica y demás entes colectivos en Venezuela para poder practicar las actuaciones administrativas.

b. El lugar situado en Venezuela en el que se desarrolle su actividad, negocio o explotación, o el lugar donde se encuentre ubicado su establecimiento permanente o de base fija; siempre y cuando, la persona domiciliada en el extranjero no tenga representante en el país y consecuentemente, no pueda aplicarse la regla dispuesta en el literal “a” de esta sección.

c. El lugar donde ocurra el hecho imponible; siempre que no se pueda aplicar las reglas dispuestas en los literales “a” y “b” de esta sección. Por ello, el lugar donde ocurra el hecho imponible, debe considerarse, como el elemento espacial, con descripción legal en el supuesto de hecho establecido en la norma tributaria, y que al ser materializado, indica el lugar en el cual el sujeto obligado por la norma jurídica, realiza el hecho que está señalado en la misma.

III. El domicilio fiscal electrónico obligatorio para la notificación de comunicaciones o actos administrativos tributarios

1. Notificación de comunicaciones o actos administrativos tributarios

1.1. Notificaciones

Se entiende por la palabra notificar *“2. tr. Comunicar formalmente a su destinatario una resolución administrativa o judicial”*¹⁷; por ello, debe entenderse que la notificación, es un proceso por el cual, se informa a alguien, de una determinada disposición emanada del Estado, a través de sus órganos administrativos o judiciales. De allí que la notificación:

¹⁶ Servicio Nacional de Administración Aduanera y Tributaria: Glosario Tributos Internos-apoderado. <http://www.lisandroferreira.com.ve/documents/GLOSARIOTRIBUTOSINTERNOS.pdf> [Consulta: 2017, enero, 25].

¹⁷ Disponible en: <http://dle.rae.es/srv/search?m=30&w=notificar> [Consulta: 2017, enero 26].

... es un acto consecuencia de otro acto, con el que mantiene una relación accesoria, por lo que se afirma, que la notificación no tiene un contenido propio y se presume que es un medio para dar a conocer el contenido de otro acto¹⁸.

1.2. Notificaciones tributarias

La notificación tributarias, son consideradas como *“instrumento [s] de difusión que maneja las administraciones tributarias(...) y se presume que es un medio para dar a conocer el contenido de otro acto, que con acierto viene a ser una declaración unilateral que surge de una función administrativa”*¹⁹.

La notificación tributaria, por tanto, es el medio de difusión que utiliza la Administración Tributaria, para hacer la comunicación formal del acto administrativo tributario. En este sentido, la notificación tributaria tiene por finalidad comunicar otro acto de carácter administrativo tributario, que puede versar en: diligencias, actas, inspecciones, multas, sanciones entre otros.

Estas notificaciones, según el artículo 172 del Código Orgánico Tributario pueden realizarse de manera personal, entregándola contra el recibo al contribuyente; por constancia escrita entregada por funcionario de la administración Tributaria en el domicilio del contribuyente o responsable; o por correspondencia postal efectuada por correo público o privado, por sistemas de comunicación telegráficos o electrónicos, siempre que se deje constancia en el expediente de su recepción.

Sin embargo, en caso de no haber podido determinarse el domicilio del contribuyente, según lo dispuesto en los apartados anteriores de este trabajo, o cuando fuere imposible practicar la notificación por cualquiera de los medios señalados en el párrafo anterior, la notificación se practicará mediante publicación de un aviso en los diarios de mayor circulación de la República, o de la ciudad sede de la Administración Tributaria que haya emitido el acto; el aviso contendrá los extremos del artículo 176 del Código Orgánico Tributario.

1.3. Comunicaciones y actos administrativos tributarios

1.3.1. Comunicaciones tributarias

Las comunicaciones tributarias, se pueden definir como *“cualquiera de las actividades que, con carácter perceptivo, son llevadas a cabo en el campo de la información tributaria, por parte tanto de la Administración tributaria*

¹⁸ Alex D. Hernández Domínguez: *La información como erradicación del delito fiscal* http://gredos.usal.es/jspui/bitstream/10366/128354/1/DDAFP_Hern%C3%A1ndezDom%C3%ADnguezAD_Informaci%C3%B3ninstrumento.pdf. [Consulta: 2017, enero 20].

¹⁹ Alex D. Hernández Domínguez: *La información como erradicación...op. cit.*

como de los ciudadanos o de otras Administraciones Públicas”²⁰; es decir las comunicaciones tributarias, en su *lato sensu* tiene por función primordial, informar.

La información emitida a través de una comunicación tributaria, debe ser vista como un mecanismo de información jurídica formal así como un mecanismo de servicio de índole tributario. El objeto de la comunicación tributaria, es obtener y transmitir información dependiendo del sujeto emisor de la misma; vale decir, información emitida de la Administración Tributaria a los ciudadanos (sujetos pasivos de la relación jurídica tributaria o no) y viceversa, en otras palabras de los ciudadanos (sujetos pasivos de la relación jurídica tributaria) a la Administración Tributaria (como sujeto activo de la relación jurídica tributaria), además del flujo de información a otros órganos de la Administración Pública.

1.3.2. Actos administrativos tributarios

El acto administrativo en Venezuela está definido en el artículo 7 de la Ley Orgánica de Procedimientos Administrativos²¹, como “*toda declaración de carácter general o particular emitida de acuerdo a las formalidades y requisitos establecidos en la Ley, por los órganos de la administración pública*”. De allí que, el acto administrativo en su sentido general, es considerado como, la manifestación de voluntad de algún órgano de la Administración Pública, la cual debe ceñirse a las formalidades y requisitos previstos en la Ley, y cuyo destinatario puede ser de carácter particular o por el contrario un destinatario general.

Ramón Parada²², define el acto administrativo, bajo la concepción del ejercicio de potestad administrativa al señalar:

...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 Contenciosa-administrativa.

El acto administrativo, debe provenir entonces, de algún órgano de la Administración Pública, en función de su actuación y potestad administrativa; “*sin ser relevante quien dicta el acto, por lo que en Venezuela se acoge el criterio funcional*”²³.

20 Jordi Jové i Vitalta: http://diposit.ub.edu/dspace/bitstream/2445/65194/1/JJiV_TESIS.pdf. *Aspectos generales de la comunicación tributaria* [Consulta: 2017, enero 26]

21 Ley Orgánica de Procedimientos Administrativos (2008). Gaceta Oficial de la República de Venezuela N° 5.890 Extraordinaria, del 15 de julio de 2008.

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

23 Mónica RIVERA CAJAS: “El acto administrativo electrónico en Venezuela”. *Revista Derecho y Tecnología*, N°15. San Cristóbal. Universidad Católica del Táchira, 2015, pp. 85-104

Ahora bien, es menester aclarar que el acto administrativo tributario, no ha sido definido como tal, dentro de la ley adjetiva tributaria vigente. De allí que, sea necesario considerar las definiciones *supra* mencionadas, para dar un aproximación a la definición de acto administrativo tributario.

En tal sentido, el acto administrativo tributario, debe entenderse como la declaración de voluntad de Administración Tributaria, quien actuando bajo su potestad administrativa tributaria, y de acuerdo a las formalidades y requisitos de ley, impone su voluntad de imperio, sobre los derechos, libertades o interés de un sujeto pasivo de la relación jurídica tributaria bien en calidad de contribuyente o responsable. Para que el acto administrativo tributario tenga efectos, es necesario que el mismo sea notificado tal como lo dispone el Artículo 171 del Código Orgánico Tributario.

El acto administrativo tributario está bajo el control de la misma Administración Tributaria, a través de la revisión de oficio. Este procedimiento administrativo tributario, dispone que la Administración Tributaria, se reserva en todo momento, la posibilidad de corregir sus actos, para así subsanar todos los vicios de que adolezca el acto; salvo aquellos actos administrativos tributarios que estén viciados de nulidad absoluta, *verbi gratia* un acto administrativo tributario de ejecución ilegal como la aplicación de una sanción distinta a la dispuesta en la ley.

Además el acto administrativo tributario de efectos particulares, está bajo la posibilidad de impugnación por parte del sujeto pasivo de la relación jurídica tributaria (contribuyente o responsable), a través del recurso jerárquico, dispuesto en el artículo 252 del Código Orgánico Tributario. Este recurso debe intentarse por ante la oficina de la que emanó el acto administrativo, y en el lapso de 25 días hábiles contados a partir de la fecha en que se notificó el acto administrativo impugnado.

Sin embargo, el acto administrativo tributario firme puede ser objeto de impugnación a través del recurso de revisión, el cual podrá intentarse dentro de los tres (3) meses siguientes a la fecha de la sentencia, ante los funcionarios competentes para conocer el recurso jerárquico, siempre que se evidencie alguno de los extremos previstos en el artículo 263 del Código Orgánico Tributario²⁴.

Asimismo, el acto administrativo tributario puede ser objeto de control de la jurisdicción contenciosa, a través del recurso contencioso tributario, el cual procede bajo los extremos establecidos en el artículo 266 del Código Orgánico

24 Artículo 263 del Código Orgánico Tributario (2014)... *op. cit.*: “El Recurso de Revisión contra actos administrativos firmes podrá intentarse ante los funcionarios competentes para conocer del recurso jerárquico en los siguientes casos: Cuando hubiere aparecido de pruebas esenciales para la resolución del asunto, no disponibles para el momento de su tramitación; Cuando en la resolución hubieren influido en forma decisiva documentos o testimonios declarados falsos, por sentencia judicial firme; Cuando la resolución hubiere sido adoptado por cohecho, violencia, soborno u otra manifestación fraudulenta, y ello hubiere quedado establecido en sentencia judicial firme”.

Tributario, y ante el tribunal competente, o por ante un juez con competencia territorial en el domicilio fiscal del recurrente, o ante la oficina de la Administración Tributaria de la cual emanó el acto, por lo que este recurso judicial, puede ejercerse subsidiariamente con el recurso jerárquico.

2. Domicilio fiscal electrónico obligatorio

2.1. Generalidades

El ordenamiento jurídico venezolano, desde la entrada en vigencia de la Constitución de la República en el año 1999, ha avanzado e incorporado las Tecnologías de la Información y la Comunicación, creando la necesidad de incluir, dentro de los diversos organismos de Administración Pública, el uso de los medios electrónicos. Así pues, la Carta magna establece en el artículo 110, el interés público, por parte del Estado venezolano, del uso de la ciencia, la tecnología, la innovación y sus aplicaciones; anunciando el constitucionalista, que la Ley determinará, los modos y medios para dar cumplimiento a esta garantía.

Una manera de poner en práctica la garantía constitucional antes referida, es la inclusión de la tecnología, la innovación y sus aplicaciones dentro de la Administración Pública; lo que permite encajar, a los diversos órganos de la Administración Pública, al talante del siglo XXI, a través del gobierno electrónico o *e-government*.

En el año 2001 y dentro del desarrollo de la garantía prevista en el artículo 110 de la Constitución de la República, se incorpora en materia tributaria y dentro de las normas adjetivas (Código Orgánico Tributario), la figura del domicilio electrónico, como uno de cimientos a la apertura de la electrificación y el gobierno electrónico en materia tributaria.

Esta figura estaba dispuesta en el artículo 34 del Código Orgánico Tributario²⁵ del año 2001; en este se disponía la posibilidad de convenir, que tenían tanto la Administración Tributaria y los contribuyentes o responsables, en un domicilio electrónico. El mismo consistía, en un mecanismo tecnológico seguro, que servía de buzón de envío de actos administrativos, condicionando por tanto esta figura al correo electrónico convenido entre ambas partes de la relación jurídica tributaria.

Con la entrada en vigencia del Código Orgánico Tributario del año 2014, se modifica la figura de domicilio electrónico *supra* mencionada. La misma pasa a ser, una figura tributaria discrecional de la Administración Tributaria,

²⁵ Artículo 34 Código Orgánico Tributario (2001) Gaceta Oficial de la República de Venezuela N° 37.305, del 17 de octubre de 2001: “La Administración Tributaria y los contribuyentes o responsables, podrán convenir adicionalmente la definición de un domicilio electrónico, entendiéndose como tal a un mecanismo tecnológico seguro que sirva de buzón de envío de actos administrativos...”

denominada domicilio fiscal electrónico obligatorio, la cual aparece dispuesta en el artículo 34 *ejusdem*.

2.2. Definición del domicilio fiscal electrónico obligatorio

La figura del domicilio fiscal electrónico obligatorio, prevista en la ley adjetiva tributaria del año 2014, no es definida, por legislación tributaria nacional, ni por la doctrina. Sin embargo, a tenor de determinar un concepto de domicilio fiscal electrónico obligatorio, vale la pena, presentar la definición de domicilio fiscal electrónico de Lucas Bustos²⁶ quien señala que: “*El domicilio fiscal electrónico es el sitio informático seguro, personalizado, válido y optativo registrado por los contribuyentes y responsables para el cumplimiento de sus obligaciones fiscales y para la entrega o recepción de comunicaciones de cualquier naturaleza*”.

De este contexto conceptual, se desprende que el domicilio fiscal electrónico, es un sitio informático, en el que se hacen posible el tratamiento automático de entrega o recepción de comunicaciones tributarias, a través de la información llevada a cabo por medio de computadoras, el cual es válido, y ofrece una confianza, para quien como contribuyente o responsable, registra de manera personal y optativa esta figura de domicilio fiscal electrónico.

Ahora, del concepto de domicilio fiscal electrónico referido, emerge una particularidad de tratamiento de registro optativo válido por parte de los contribuyentes y responsables, el cual encuadraba dentro de los extremos establecidos en el Código Orgánico Tributario del año 2001; ya que, este domicilio a tenor del Artículo 34 *ejusdem*, debía ser aceptado por la Administración Tributaria, para encajar como válido, y el mismo tenía un carácter adicional, lo cual se suma a los domicilios fiscales existentes dispuestos en la ley adjetiva tributaria.

Sin embargo, lo anteriormente expuesto difiere del sentido dispuesto en el artículo 34 del Código Orgánico Tributario venezolano vigente. En efecto, del referido artículo, se deja leer entre líneas, que es la Administración Tributaria, quien tiene la potestad, de establecer un domicilio fiscal electrónico, que deja de ser opcional para convertirse en obligatorio, sin que medie la opinión del contribuyente o responsable; todo ello, para notificar comunicaciones o actos administrativos de carácter tributario.

La figura de domicilio fiscal electrónico obligatorio, dispuesta en el Código Orgánico Tributario vigente, no identifica, para este tipo de domicilio fiscal, la existencia de seguridad (dispuesta en el Código Orgánico Tributario derogado), como requisito *sine qua non*, para todas las actuaciones llevadas a cabo por

²⁶ Lucas Bustos: *Domicilio Fiscal, su conceptualización y las diferencias con otros tipos de domicilios* <http://www.dameleconsultores.com.ar/domicilio-fiscal-su-conceptualizacion-y-las-diferencias-con-otros-tipos-de-domicilios/> [Consulta: 2017, enero 11]

medios electrónicos e informáticos. Así como tampoco, dispone el Código Orgánico Tributario vigente en el artículo 34, el mecanismo tecnológico a utilizar, en el envío de notificaciones de comunicaciones y actos administrativos tributarios.

De la misma manera, el domicilio fiscal electrónico obligatorio es, según se infiere del artículo 34 del Código Orgánico Tributario vigente, preferente frente a las reglas de los domicilios fiscales de las personas naturales y jurídicas domiciliadas en Venezuela o el extranjero.

Tomando en consideración lo antes expuesto, se puede definir el domicilio fiscal electrónico obligatorio como, el sitio informático seguro y válido, dispuesto por la Administración Tributaria, en función de la gobernanza electrónica y en su potestad discrecional, para notificar de comunicaciones y actos administrativos tributarios, a los contribuyentes y responsables como sujetos pasivos de la relación jurídica tributaria; este domicilio fiscal electrónico obligatorio, tendrá preferencia de aplicación, respecto a los domicilios dispuestos en él a partir del artículo 30 al Artículo 33 ambos inclusive del Código Orgánico Tributario vigente.

2.3. Fallas del domicilio fiscal electrónico obligatorio que atentan contra el derecho a la defensa del administrado

De la redacción del artículo 34 del Código Orgánico Tributario vigente, se desprende una serie de faltas, que pudieran considerarse como una redacción desafortunada de la norma, la cual gira en torno al funcionamiento del domicilio fiscal electrónico obligatorio; que trae como consecuencia la vulneración al derecho a la defensa del administrado, quien es impuesto de este tipo de domicilio.

Al efecto, la redacción del artículo 34 *ejusdem*, no indica el mecanismo a utilizar para establecer el domicilio fiscal electrónico obligatorio, tal como lo disponía la redacción del artículo 34 del Código Orgánico Tributario del año 2001, cuando señalaba el derogado artículo “*mecanismo tecnológico seguro que sirva de buzón de envío de actos administrativo*”.

Vale decir, en la norma vigente, no se puntualiza, el medio tecnológico, ni mucho menos, el medio procedimental para la imposición de este tipo de domicilio. En este sentido, pudiera inferirse que en referencia al medio tecnológico, para la práctica de este domicilio fiscal electrónico obligatorio, queda al *arbitrium* y discrecionalidad de la Administración Tributaria, la escogencia del mismo, por el simple hecho de no existir reglado en la norma, aclarando que este vacío legislativo, pudiese ser, para evitar obsolescencias legislativas, en cuanto al mismo.

Empero, en lo que concierne al medio procedimental del domicilio electrónico fiscal obligatorio, debe señalarse que no se establece alguna consideración referente a este apartado, dentro de la ley adjetiva tributaria. Por ello, y en aplicación del principio de analogía admisible para colmar vacíos legales, dispuesto

en el artículo 6 del Código Orgánico Tributario²⁷, aunado al numeral 5 del artículo 2 *ejusdem*, que estipula como fuente del derecho tributario, “*Las reglamentaciones y demás disposiciones de carácter general establecidas por los órganos administrativos facultados al efecto*”, es por lo que, debe aplicarse cualquier norma análoga como por ejemplo, alguna providencia administrativa o resolución emanada de la Administración Tributaria, que aclare la duda que surge por el vacío legal del artículo 34 del Código Orgánico Tributario.

Al efecto, la Providencia Administrativa número 48 del año 2013²⁸, la cual dispone, en el artículo 1, el deber de inscripción en el Registro Único de Información Fiscal, y según lo ordena el artículo 3 de la referida Providencia Administrativa, “*conforme a los requisitos y especificaciones técnicas establecidas en el Portal Fiscal*”, debe ser admisible como fuente del derecho tributario, para interpretar y colmar el vacío de ley que se desprende del artículo 34 del Código Orgánico Tributario.

En tal sentido, según se infiere de lo antes expuesto, el funcionamiento del domicilio fiscal electrónico obligatorio, debe ser especificado, tanto en requisitos y especificaciones técnicas, en el Servicio Nacional de Administración Aduanera y Tributaria, a través del Portal Fiscal (página *web* <http://www.seniat.gob.ve>) o, cualquiera otro que sea creado por el Servicio Nacional Integrado de Administración Aduanera y Tributaria para sustituirlo.

Sin embargo, dentro del portal fiscal en el enlace trámites electrónicos, para clave y usuario persona natural así como en el enlace clave y usuario para persona jurídica se desprende un PDF contentivo de una guía fácil clave y usuario tanto para persona natural²⁹, así como una guía fácil clave y usuario

27 Artículo 6 del Código Orgánico Tributario (2014)... *op. cit.*: “La analogía es admisible para colmar vacíos de legales, pero en virtud de ella no pueden crearse tributos, exenciones, exoneraciones ni otros beneficios, tampoco tipificar ilícitos ni establecer sanciones”.

28 Artículo 1 de la Providencia Administrativa N° 48 que regula el Registro único de Información Fiscal (2013). Gaceta Oficial de la República Bolivariana de Venezuela N° 40.214, del 25 de julio de 2013 “Las personas naturales, las personas jurídicas y las entidades sin personalidad jurídica que sean sujetos pasivos de tributos administrados por el Servicio Nacional Integrado de Administración Aduanera y Tributaria (SENIAT) o que deban efectuar trámites ante cualquier Ente u Órgano de la Administración Pública, deberán inscribirse en el Registro Único de Información Fiscal (RIF), conforme a lo establecido en esta Providencia Administrativa.

Igualmente deberán inscribirse en el Registro Único de Información Fiscal (RIF), los sujetos o entidades no residentes o no domiciliadas en la República Bolivariana de Venezuela, que no posean establecimiento permanente o base fija cuando realicen actividades económicas en el país o posean bienes susceptibles de ser gravados en el mismo”.

29 Servicio Nacional de Administración Aduanera y Tributaria: Guía Fácil y Usuario Persona Natural http://declaraciones.seniat.gob.ve/portal/page/portal/MANEJADOR_CONTENIDO_SENIAT/05MENU_HORIZONTAL/5.1ASISTENCIA_CONTRIBUYENTE/5.1.2ORIENTACION_GENERA/5.1.2.1TRAMITES_ELECTRONI/CUPN.pdf

para las personas jurídicas³⁰, las cuales disponen, preguntas esenciales para poder registrarse en el portal Servicio Nacional de Administración Aduanera y Tributaria.

Como primer requisito, se exige, tanto a la persona natural, como a la persona jurídica, poseer una cuenta de correo válida. Al registrarse como nuevo usuario, e ingresar los datos exigidos en los campos requeridos, se solicita una dirección de correo electrónico principal. En este campo, se deja leer, que *“la dirección de correo electrónico principal, será considerada como domicilio electrónico, para realizar la notificación de los actos administrativos, de acuerdo con lo establecido en el COT, art. 34”*. De allí que, esta dirección de correo electrónico, según el manual o guía fácil de trámites electrónicos, publicada por el Servicio Nacional de Administración Aduanera y Tributaria, se establece por tanto, como el domicilio electrónico.

Sin embargo, surgen las preguntas: ¿la leyenda debajo del campo requerido de correo electrónico principal, se convierte en norma?, ¿este texto escrito *“la dirección de correo electrónico principal, será considerada como domicilio electrónico, para realizar la notificación de los actos administrativos, de acuerdo con lo establecido en el COT, art. 34”*, que acompaña al campo requerido de correo principal solicitado, de trámite electrónico de clave y usuario para persona natural y persona jurídica, debe entenderse por interpretación analógica una disposición de carácter general, emanada por los órganos administrativos facultados al efecto?

De ser sí, la respuesta en ambas interrogantes formuladas anteriormente, el sujeto pasivo de la relación jurídica tributaria, pudiera alegar, inseguridad jurídica, por falta de previsión legal del funcionamiento del domicilio fiscal electrónico obligatorio, en norma legal de carácter tributario.

Para aclarar la inferencia anterior, debe señalarse que no existen disquisiciones académicas, ni mucho menos explicaciones doctrinales que entren a exponer, la explicación de la vía procedimental para que la Administración Tributaria, pueda establecer el domicilio fiscal electrónico obligatorio. Tampoco puede considerarse como norma procedimental, la guía PDF dispuesta en el portal fiscal en el enlace trámites electrónicos (para clave y usuario persona natural, ni para clave usuario persona jurídica); amén de que el domicilio al que hace referencia la guía mencionada, es el domicilio electrónico y no el domicilio dispuesto el artículo 34 del Código Orgánico Tributario vigente.

De manera que, la Administración Tributaria, al notificar por domicilio fiscal electrónico obligatorio, comunicaciones y actos administrativos tributarios, está actuando arbitrariamente, al no indicar en la norma jurídica, los trámites necesarios para establecer o imponer la figura bajo estudio.

³⁰ Servicio Nacional de Administración Aduanera y Tributaria: Guía Fácil y Usuario Persona Jurídica http://declaraciones.seniat.gob.ve/portal/page/portal/MANEJADOR_CONTENTIDO_SENIAT/05MENU_HORIZONTAL/5.1ASISTENCIA_CONTRIBUYENTE/5.1.2ORIENTACION_GEÑERA/5.1.2.1TRAMITES_ELECTRONI/CUPJ.pdf

Otro punto criticable al artículo 34 del Código Orgánico Tributario (2014), es la no inclusión de la relación recíproca y bidireccional, entre el administrado sujeto pasivo de la relación jurídica tributaria (contribuyente, responsable) y, la Administración tributaria.

Es decir, el administrado que desee formalizar, por medio de pedimento, alguno de los recursos contra acto administrativo individual y de carácter tributario, no podrá interponer por vía electrónica, a través del domicilio fiscal electrónico obligatorio, en la dirección de la cual emanó el acto a recurrir, su petición.

De manera que, puede considerarse como una vulneración al derecho de la defensa del administrado; pues, para recurrir de los actos administrativos de efectos particulares (en vía administrativa), el administrado, debe intentar de manera física, el recurso administrativo en la oficina de la cual emanó el acto, por lo que vale preguntarse ¿acaso, no podría el administrado, interponer el recurso administrativo tributario, por medios electrónicos, a la dirección electrónica de la cual emanó tal comunicación?

Finalmente, el artículo 34 de la norma adjetiva vigente, establece que el domicilio fiscal electrónico obligatorio *“tendrá preferencia respecto a los previstos en los Artículos: 31, 32, 33 de este Código (sic)”*, constituyendo por tanto esta precisión legislativa, una alteración de las normas básicas del domicilio de las personas naturales y jurídicas dispuestas en la legislación venezolana, alterando por tanto, el derecho a la defensa del administrado, quien a los efectos tributarios, y para la práctica de notificaciones de comunicaciones y actos administrativos tributarios, ha precisado un domicilio físico, siguiendo el orden de prelación y las normas establecidas en los artículos 31, 32, y 33 del Código Orgánico Tributario.

IV. Consideraciones finales

El domicilio fiscal electrónico obligatorio, dispuesto en el Código Orgánico Tributario vigente, debe considerarse teóricamente, un avance de la gobernanza electrónica en materia de Administración Tributaria en Venezuela. Esta figura jurídica, como acto, debe ser considerado independiente de la comunicación y el acto administrativo tributario; lo cual significa que, el domicilio fiscal electrónico obligatorio, es la vía utilizada, con carácter de preferencial por la Administración Tributaria frente a los demás domicilios dispuestos en la norma adjetiva tributaria, para hacer saber, un acto comunicacional o, un acto administrativo emanado de la Administración Tributaria.

Las implicaciones de esta figura jurídica tributaria para el administrado (contribuyente o responsable), giran en función a los vacíos de ley, que vulnera la garantía constitucional de seguridad jurídica y, consecuentemente, el derecho a la defensa del administrado.

Esto se puede notar en, la falta del procedimiento legal tributario, que establezca la actuación por trámite administrativo tributario, en el que la Administración Tributaria, exija el cumplimiento de ciertos pasos y diligencias al administrado, para imponer el domicilio fiscal electrónico obligatorio. En este orden de ideas, la inseguridad jurídica vulnera el derecho a la defensa del administrado, al no incluir dentro de las normas jurídicas (adjetivas y sustantivas tributarias) ni las reglamentaciones y demás disposiciones de carácter general establecidas por los órganos administrativos facultados al efecto, el procedimiento para que la Administración Tributaria pueda imponer o establecer un domicilio fiscal electrónico obligatorio.

Como si fuera poco, el uso del domicilio fiscal electrónico obligatorio, debe entenderse según se infiere de la ley, como una carga u obligación para el administrado, quien solo estará atento a ese tipo de domicilio, para ser notificado de comunicaciones y actos administrativos tributarios. Dado que, el administrado no podrá interponer en vía administrativa, recurso administrativo tributario y dispuesto en ley, contra el acto administrativo tributario notificado por medio electrónico, a través del uso del domicilio electrónico fiscal obligatorio presentando el recurso en documento electrónico, como respuesta, en la cuenta electrónica de la que emanó dicha notificación, atentando ello a la garantía de derecho a la defensa.

Finalmente, si la Administración Tributaria, incorporara normas instruccionales de carácter obligatorio, a través de providencias administrativas emanadas por el Servicio Nacional de Administración Aduanera y Tributaria, que permitan: a) dar certeza, en la forma en que debe registrarse el administrado para poseer domicilio fiscal electrónico obligatorio; b) disponer el efectivo uso del referido domicilio fiscal, que incluya la posibilidad de dirigir peticiones o interponer los recursos administrativos tributarios previsto en el Código Orgánico Tributario); se estaría garantizando el efectivo derecho a la defensa del administrado.

Todo ello mejoraría la gestión pública y la prestación de servicios de la Administración Tributaria; dando por tanto, fiel cumplimiento al principio de interés prioritario del Estado, en la ciencia, la tecnología, la información y sus aplicaciones, dispuesta en la Constitución de la República, con lo que se lograría el uso obligatorio de las Tecnologías de la Información y las Comunicaciones.

CONFERENCIAS

XX Congreso Iberoamericano de Derecho e Informática
Federación Iberoamericana de Asociaciones de Derecho e Informática.
Salamanca, octubre, 2016

Derechos humanos en la protección ética de los menores en las redes sociales. Caso Colombia y Perú

Jefferson Stewart Espinosa Vera*

SUMARIO: I. Los derechos humanos en el ciberespacio. II. La problemática del chat en los menores-*grooming* y educación parental en las nuevas tecnologías. III. Comportamientos psicológicos y sociales de las víctimas (menores de edad). IV. La legislación colombiana. V. Ética en las redes sociales o infoética, riesgos y vulnerabilidades en la web. VI. Análisis crítico del artículo 5° de la Ley N° 30096. “La violación a la indemnidad y libertad sexual a través de la tecnología”. VII. El bien jurídico tutelado. VIII. El *iter criminis*. IX. El camino y desarrollo del supuesto contemplado en el Art 5° de la Ley N° 30096. X. Conclusiones.

Resumen

En el presente trabajo se analizan las incidencias de las tecnologías de la información y las comunicaciones en la esfera de las libertades partiendo de los cambios sociales contemporáneos. Se estudia la problemática del chat y los menores en el ambiente de la educación parental en las nuevas tecnologías, así como la importancia del esfuerzo de la legislación al tratar de proteger a los niños, jóvenes y adolescentes que pueden ser atacados por cibernautas criminales que buscan engañar a este tipo de población tan vulnerable protegida constitucional y penalmente.

• Aceptado por el Comité Académico para ser presentado en el XX Congreso Iberoamericano de Derecho e Informática celebrado en Salamanca, España durante el mes de octubre, 2016. Aprobado por la Junta Directiva FIADI para ser publicado en la *Revista Derecho y Tecnología*, el 16 de noviembre de 2016.

* Abogado (Colombia), Universidad Autónoma Latinoamericana (Colombia), Maestrando en Derecho Procesal. Universidad Nacional de Rosario (Argentina), Diplomado en Docencia Universitaria. Pedagogía Currículo y Didácticas. Universidad Pontificia Bolivariana (UPB-Colombia), Diplomado en Derechos Humanos y Control de Convencionalidad – ACDPC (Colombia) y Universidad de Bologna (Italia).. Ponencia elaborada en Co –autoría en idioma castellano con el Dr. Miguel Ángel Vidalón Choque- Abogado (Perú) - Universidad Nacional Hermilio Valdizán de Huánuco.

Palabras clave: Derechos humanos. Menores. Redes sociales. Protección jurídico

Abstract

In this paper the effects of information and communication technologies in the sphere of the freedoms, starting from the contemporary social changes are analyzed. The issues associated with chat and children in the field of parental education in new technologies are studied, as well as the importance of the legislation's efforts to protect children, and young people that may be attacked by cybernauts who seek to deceive this type of vulnerable population, protected both under constitutional and criminal law.

Keywords: Human rights. Minors. Social Networks. Legal Protection

I. Los derechos humanos en el ciberespacio

La incidencia de las Tecnologías de la Información y comunicaciones y las Nuevas Tecnologías en la esfera de las libertades, ha configurado una nueva generación de derechos humanos. Éstos nuevos derechos, demuestran que el catálogo de las libertades nunca será una obra cerrada y acabada. Una sociedad libre, pluralista y democrática deberá mostrarse siempre sensible y abierta a la aparición de nuevas necesidades que fundamenten nuevos derechos. Mientras estos no hayan sido reconocidos por el ordenamiento jurídico nacional y/o internacional, actuarán como categorías reivindicativas, pre- normativas y axiológicas, pero los derechos humanos no son meros postulados de “deber ser”. La teoría de los derechos humanos no puede ser insensible a la urgencia de tomar en serio la tarea de construir una teoría de las libertades abierta y responsablemente comprometida con la respuesta a las nuevas necesidades y exigencias de los seres humanos que viven en la era de las nuevas tecnologías. En nuestro tiempo, que se distingue por la omnipresencia de las Nuevas Tecnologías en todos los aspectos de la vida individual y colectiva, se ha ampliado decisivamente la incidencia de las TIC en amplios sectores de la experiencia jurídica y política. Los Derechos Humanos como terminología, es un concepto relativamente nuevo, se puede decir que incluso es de uso más regular a partir del primer cuarto del siglo XX, y especialmente desde mediados de ese siglo, con la aprobación de la Declaración Universal de los Derechos Humanos, el 10 de diciembre de 1948. Ya en 1945, la Carta de la Organización de las Naciones Unidas había acuñado ese término, en la que expresaba, como uno de sus propósitos, *“Realizar la cooperación internacional en la solución de problemas internacionales de carácter económico, social, cultural o humanitario, y en el desarrollo y estímulo del respeto a los derechos*

*humanos y a las libertades fundamentales de todos, sin hacer distinción por motivos de raza, sexo, idioma o religión...*¹ (El subrayado no es del original). En este contexto, las Nuevas Tecnologías, han propiciado nuevas formas de ejercicio de los derechos y, de hecho, pueden contribuir a un reforzamiento del tejido participativo de las sociedades democráticas. Así, la ciberciudadanía y la teledemocracia constituyen un nuevo horizonte de los derechos. La sociedad en que vivimos, no es la misma en la que se aprobaron la Declaración Universal de Derechos Humanos (aprobada en 1948, justo después de la II Guerra Mundial), los Pactos Internacionales de Derechos Humanos (aprobados en 1966, en plena guerra fría) y el resto de instrumentos internacionales de protección de los derechos humanos. En este contexto, uno de los aspectos a tener en cuenta, sin duda, es el avance tecnológico que ha habido desde entonces. En estos últimos años –ya desde los años 60, pero sobre todo en los últimos veinte años- se ha caracterizado por el gran desarrollo de la tecnología y, en concreto, de lo que hoy se denominan las Tecnologías de la Información y la Comunicación (TIC). La DUDHE hace referencia a las TIC a lo largo de su articulado, como por ejemplo en el artículo 5. Este desarrollo tecnológico ha supuesto la emergencia de nuevos derechos, muchas veces en respuesta a nuevas agresiones. Un ejemplo es el derecho a la protección de datos personales –reconocido también a la DUDHE, artículo 5.9-, que surgió ante la necesidad de proteger al individuo frente a los peligros que podía suponer la informática. Por otro lado, hoy por hoy, el consumo y uso de estas tecnologías de forma desenfrenada y sin control está suponiendo graves violaciones de derechos humanos en todo el ciclo de vida de los aparatos electrónicos, los cuales tienen relación directa con la libertad, integridad, formación e indemnidad e intangibilidad de los niños, niñas y adolescentes.

II. La problemática del chat en los menores - *grooming* y educación parental en las nuevas tecnologías

Uno de los servicios más utilizados por usuarios de Internet en general y muy especialmente por los menores como medio de comunicación, es sin dudas el de los *chats*. Aquí es donde ellos pueden ser fácilmente engañados por terceros para conseguir datos personales y bancarios, como sus números de cuentas, de tarjetas de crédito, *passwords*, etc.; pertenecientes a sus progenitores a fines de cometer luego estafas. A esta práctica se le ha denominado como *grooming*. Los pedófilos y pederastas buscan, como una de las tácticas más comunes, entrar en contacto por este medio electrónico aprovechándose de las características del mismo, haciéndose pasar por otro menor, intercambiándose en la mayoría de los casos imágenes comprometedoras. Una vez en posesión de ellas, el acosador extorsiona al menor en cuestión diciéndole que enviará las

¹ Carta de la Organización de las Naciones Unidas, artículo 1.

imágenes a sus familiares y/o amigos, cuyas direcciones de correo electrónico ya están en posesión del adulto previamente, al entrar en esa primera fase de confianza.

- Las TIC al servicio de la educación en los menores de edad

Las Nuevas Tecnologías están tomando mucho protagonismo en la sociedad, pero a la vez en la educación, el papel que juegan las Tecnologías de la Información y la Comunicación (TIC) en un mundo cada vez más digitalizado, es muy importante para el mejoramiento de la calidad educativa, los beneficios que aporta el modelo educativo implementado desde las TIC son innumerables, lo cual plantea algunos retos a tener en cuenta si se quiere mejorar verdaderamente el nivel educacional que permita a las nuevas generaciones (niños), ser competitivos en el mundo digitalizado.

El ilustre filósofo y lingüista norteamericano NOAM CHOMSKY² ha reflexionado sobre este apartado, el del impacto de las nuevas tecnologías en la educación, él cree que para hacer un buen uso de ellas, lo primero que debe tener el alumno es un buen marco de referencia, en el cual debe moverse, buscar de manera adecuada y saber diferenciar la información veraz y correcta. Para ello necesita alguien que le enseñe todo esto, y quién mejor que su profesor. Dice que al haber en Internet tanta cantidad de información lo único que le puede suceder al alumno si no sigue los pasos anteriormente mencionados es perjudicarlo, ya que puede almacenar datos objetivos de distintas páginas pero que a la vez estén totalmente fuera de la realidad.

- Patria potestad y educación en las modernas tecnologías. Especial referencia a Internet

A lo largo de la historia, los niños han ocupado diversos estatus en las sociedades en las que se desarrollaban. Es bien conocido que hasta mediados del siglo XVIII existieron sistemas de crianza y prácticas educativas que tenían como común denominador la proyección de la agresión del adulto sobre el niño,

2 (...) “En cuanto a la tecnología en la educación, debe decirse que la tecnología es algo neutro. (...) Por ejemplo: Internet es extremadamente valiosa si se sabe lo que se está buscando; yo la uso todo el tiempo en mi investigación. Si se sabe lo que se está buscando, si se tiene una especie de marco de referencia, que nos dirige a temas particulares y nos permite dejar al margen muchos otros, entonces puede ser una herramienta muy valiosa. Por supuesto, uno debe estar siempre dispuesto a preguntarse si el marco de referencia es el correcto: Tal vez algo que encontremos cuestionará la forma en que vemos las cosas. No se puede perseguir ningún tipo de investigación sin un marco de referencia relativamente claro que dirija la búsqueda y que ayude a seleccionar lo que es significativo y lo que no lo es, lo que hay de que dejar de lado, a lo que hay que darle seguimiento, lo que merece ser cuestionado o desarrollado” NOAM CHOMSKY (Texto- El objetivo de la Educación: La Deseducación). CONCEPTO DE TECNOLOGÍA Y EDUCACIÓN- NOAM CHOMSKY.

considerándolo sólo como un objeto de derecho y no, como lo es en la actualidad, un sujeto de derecho. Es en razón de esta irrupción que se ha producido la necesidad de que los padres deben educar a sus hijos en el correcto uso de estas tecnologías, al abrigo de la autoridad que les otorga el ejercicio de la responsabilidad parental. En este contexto es necesario que se establezca entre padres e hijos un fluido diálogo para el logro de tal fin.

- Educación parental, filtros y TICS

La conducta del hombre en sociedad tiene muchas características y muchas formas. En la actualidad con el avance de las tecnologías de la información y la comunicación (TIC) el comportamiento del hombre ha explorado nuevos horizontes y nuevos caminos; uno de ellos es el mundo virtual y en especial el de las redes sociales³. El *grooming* es una práctica de acoso y abuso sexual en contra de niños y jóvenes que, en la mayoría de los casos, sucede a través de las redes sociales. A continuación, y a modo ejemplificativo, se pueden citar algunas pautas mínimas que los padres deberían implementar para inculcar a sus hijos un manejo responsable de la red:

- a) Establecer acuerdos y normas razonables en el uso de la Internet y los dispositivos digitales a utilizar por parte de los hijos (por ejemplo; estableciendo tiempos límites, espacios y condiciones de uso)
- b) Tomar medidas de privacidad ya que el menor podría ser víctima de un experto en técnicas para el engaño, y se necesita prevenir.
- c) Los padres deben conocer las redes sociales para saber su funcionamiento, para poder anticipar las potenciales situaciones de riesgo.
- d) Observar los estados de ánimo del menor. Cuando un menor es víctima de abuso, violencia o chantaje, presenta actitudes anormales.
- e) Los adultos y padres deben ser un ejemplo de usuarios ya que los niños aprenden a través del modelaje de sus padres, así que se debe asumir un rol responsable.

Hay varios sistemas de filtrados, entre los que podemos mencionar los siguientes:

- 1) El sistema llamado de “listas negras” o “listas de sitios a bloquear;
 - 2) El sistema de bloqueo mediante la búsqueda a través de palabras claves;
- y

³ Forma de interacción social definida como servicio en línea enfocado a comunidades de personas que comparten intereses y actividades, o que están interesados en explorar los intereses y las actividades de otros, y que requiere el uso de software.

- 3) El sistema denominado PICs (*Platform for Internet Content Selection*), el cual se fundamenta en una clasificación previa y el etiquetamiento de los contenidos de las páginas web utilizando para ello verdaderos “códigos de barras” electrónicos invisibles que son leídos por el *software* que posee el usuario.

III. Comportamientos psicológicos y sociales de las víctimas (menores de edad)

Es importante reconocer que los niños, niñas y adolescentes víctimas de algún tipo de modalidad de delito informático, tienden a presentar cambios en su comportamiento.

- Presentan una agresividad continua con los compañeros, maestros, amigos, familiares o mascotas.
- A pesar de haber mostrado entusiasmo por Internet, de un momento a otro pierde el interés por permanecer en el ciberespacio.
- Se convierten en personas tímidas y poco sociables, que no comentan lo que les sucede, demostrando estrés, llanto o pesadillas.
- Indiscutiblemente este fenómeno interfiere en el rendimiento escolar de los niños, niñas y adolescentes, demostrado en bajas calificaciones sin justificación.
- Evita mostrarle a los padres o hablar de sus amigos de las redes sociales.

A continuación, se analizará dicha situación tanto en el caso colombiano y peruano, respectivamente:

IV. La legislación colombiana

En las últimas décadas el proceso de globalización presentado a nivel mundial, ha permitido avances tecnológicos, sociales y culturales a gran escala, dejando entrever un aumento en la utilización de los delitos informáticos como un modo de actuación delincuencial en contra de los niños, niñas y adolescentes, como población más vulnerable dentro del ciberespacio. Por esta razón se ve la necesidad de incluir en la legislación nacional colombiana, mediante la Ley 1273 del 2009 que realiza modificaciones al Código Penal Colombiano donde se tipifican los delitos informáticos como “*aquellas conductas que recaen sobre herramientas informáticas, llámense programas, ordenadores, etc.; como aquellas que valiéndose de estos medios lesionan otros intereses jurídicamente tutelados como son la intimidad, el patrimonio económico, la fe pública, etc.*”¹ Es así como se genera preocupación por parte de las instituciones encargadas de la Protección de la Infancia y Adolescencia por la utilización de este *modus operandi*, como la herramienta que facilita el acoso

sexual, la pornografía con menores de edad y prostitución infantil. Dentro de esta modalidad es importante destacar las formas que se utilizan para victimizar a los niños, niñas y adolescentes, como el *ciberacoso* o *cyberbullying* que es el uso de información electrónica y medios de comunicación que está contenida en el correo electrónico, redes sociales, blogs, mensajería instantánea, mensajes de texto, teléfonos móviles y *websites*, para acosar, intimidar o amedrentar a una persona con comentarios difamatorios, degradantes y agresivos. Igualmente está el *grooming* y el *sexting*. Este último que es mostrarse a través de fotos insinuantes en la Red.

- **Caso colombiano. Jurisprudencia:**

Respecto al caso colombiano, es importante destacar la sentencia; proferida por la Honorable Corte Suprema de Justicia de la República de Colombia (Sala de Casación Penal), el día 29 de Julio de 2015- SP 9792- 2015- Radicado: 42307- (Aprobado Acta 259)- Magistrada Ponente: Dra Patricia Salazar Cuéllar-Bogotá D.C- Colombia que entre otros temas fundamentales analiza el derecho a la intimidad, la protección de los menores de edad en las redes sociales.(Ley de infancia y adolescencia de Colombia – Ley 1098 de 2006- Ley 679 de 2001 por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución de Colombia y se regula entre otros aspectos el uso de redes globales de información en relación con menores).El fallo de la Corte Suprema de Justicia de la República de Colombia, autorizó mediante un fallo en el que se indica que los padres de familia podrán tener acceso a las claves de redes sociales y correos de sus hijos, sin que esto sea una violación del derecho a la intimidad.

De esta forma los padres quedan autorizados “para asistir, orientar y controlar las comunicaciones de sus hijos menores de edad”, según la sentencia del alto tribunal, ahora los Padres de familia, tienen la facultad de acceder a la información con el objetivo de proteger a los menores en casos en que puedan estar en riesgo. Esta decisión fue tomada por los magistrados de la Corte Suprema de Justicia colombiana, luego de que a sus despachos llegaran los correos de una menor de edad inspeccionados por su madre. En ese caso se había denunciado una violación a la intimidad. La Corte Constitucional colombiana se ha pronunciado mediante fallo de tutela de Junio de 2016, con respecto a las medidas que deben adoptar las diferentes instituciones educativas, con respecto a la violencia de género o *ciberbullying* que se está generando a través de las redes sociales y que están marcando de forma infame a los menores de edad, inclusive llevando al suicidio a una estudiante colegiada, razón por la cual se ha pedido control inmediato en estas dependencias. La Corte estudió el caso de una menor de edad de quien sus compañeros habían subido una foto desnuda a una página web destinada exclusivamente al matoneo de sus compañeros de clase. Para la

Corte la publicación de estas fotografías íntimas es un ejemplo de la violencia de género a través de las redes sociales, dado a que no existe un control en los centros educativos.

V. Ética en las redes sociales o infoética, riesgos y vulnerabilidades en la web

Las redes sociales, al ser un sistema informático como cualquier otro, cuentan con peligrosas vulnerabilidades debidas principalmente a sus mismos usuarios. Son ellos quienes están expuestos a diferentes amenazas y su falta de conocimiento muchas veces puede llevarlos a revelar información personal, probablemente recolectada por quienes con seguridad no tienen las mejores intenciones. Las redes sociales son, por lo tanto, un escenario propicio para quienes pretendan atentar contra la seguridad de la información de muchísimas personas; adicionalmente los usuarios, en la mayoría de casos, no son conscientes del riesgo incurrido al divulgar abiertamente información de amplio interés para los delincuentes, situación que ha ayudado a proliferar dichas prácticas. Las vulnerabilidades pueden tener origen en alguno de los siguientes aspectos:

- a) Espacios o elementos físicos: áreas de trabajo de los usuarios, ubicación de servidores, cableado, entre otros.
- b) Los usuarios: las personas podrán revelar información importante muchas veces sin saberlo, incluso después de ser advertidas.
- c) Claves de acceso: la complejidad de dichas combinaciones es esencial, si hay obvia y poco cambio, este elemento de seguridad se convertirá en una vulnerabilidad.
- d) Mala programación: en algunos casos los desarrolladores no se enfocan en equipar su software de buena seguridad, esto crea huecos fácilmente aprovechables por personas malintencionadas.
- e) Mala infraestructura: algunas redes no cuentan con equipos adecuados para evitar posibles ataques.
- f) Integridad de datos: falta de copia o redundancia que puede causar pérdidas.

- La ética en las redes sociales - infoética.

Una discusión filosófica planteada desde hace tantos años pueda salirse del alcance de una investigación informática; así tenga un especial enfoque en las leyes relacionadas con dichos temas. Sin embargo, es necesario tener en cuenta algunas consideraciones pertinentes para quienes cuenten con conocimientos diferentes a los del común.

Son precisamente las habilidades de muchos desarrolladores de software-tema que la mayoría de las personas no domina-, aquellas a las que es necesario

prestar especial atención debido a los muchos comportamientos legalmente válidos, pero desde un punto de vista ético bastante reprochables. El desarrollo de aplicaciones para las más populares redes sociales es un aspecto que no escapa de esa discusión donde se plantea el cumplimiento de la ley así la actitud sea éticamente incorrecta. No son las redes sociales una herramienta creada para violar la ley y cometer toda clase de delitos, al contrario, son una útil y poderosa interfaz de interacción y entretenimiento que lamentablemente algunos de sus usuarios han ido convirtiendo en un espacio donde es necesario ser cauteloso con datos personales. Luego de éstas consideraciones, analizaremos en un caso en concreto, el tema del *grooming* en la legislación peruana de una manera muy crítica ya habiendo analizado la situación colombiana y que puede ser aplicable a varias legislaciones de una manera muy general en algunos aspectos.

República de Colombia
Corte Suprema de Justicia
Sala de Casación Penal Magistrada Ponente:
Dra. Patricia Salazar Cuéllar
SP 9792-2015
Rad.: 42307
(Aprobado Acta 259)
Bogotá D.C.- Colombia, Julio 29 de 2015

República de Colombia
Corte Suprema de Justicia
Sala de Casación Penal Magistrada Ponente:
Dra. Patricia Salazar Cuéllar
SP 9792-2015
Rad.: 42307
(Aprobado Acta 259)
Bogotá D.C.- Colombia, Julio 29 de 2015

VI. Análisis crítico del artículo 5º de la Ley N° 30096. “La violación a la indemnidad y libertad sexual a través de la tecnología”

Como consecuencia de la globalización y el avance tecnológico, la sociedad es receptora, en principio, de un progresivo avance y evolución de códigos que hacen de la vida del hombre una actividad moderna y práctica⁴. Sin embargo,

⁴ Al respecto: Art. Luis Gracia Martín: LOS ÁMBITOS Y LAS MANIFESTACIONES DEL DERECHO PENAL MODERNO.- “La doctrina penal incluye en el actual “Derecho Penal Moderno” a una pluralidad de nuevos tipos penales que amplían la intervención penal a ámbitos que, como por ejemplo el de la actividad económica, habían permanecido tradicionalmente y en

tal avance tecnológico también ha despertado una sensación de inseguridad en la clase política, de tal forma que ha concebido el avance tecnológico como un canal mediante el cual viaja una amenazante fuente de peligros para un sector vulnerable de la población, de manera que se ha optado por entender que tales medios tecnológicos ponen en peligro, la concreta vigencia de ciertos bienes jurídicos. El legislador ha relacionado la vulnerabilidad de cierto sector indefenso de la población con el avance tecnológico, atendiendo a la poca capacidad que tienen éstos para discernir y disuadir, respecto y sobre, las actividades peligrosas [acciones] que dirigen otras personas para lesionar su derecho [bien jurídico] a la indemnidad y libertad sexual en el caso peruano o de los delitos contra la libertad, integridad y formación sexuales en el caso colombiano. A saber de tal situación, debemos afirmar que una vez más el legislador recurre al derecho penal para justificar una forma de criminalización estatal que se orienta y justifica en la protección de la indemnidad, la libertad sexual de niños, niñas y adolescentes que en el interactuar tecnológico, son aprehendidos para fines sexuales⁵. Tal situación, sin ánimo de oscurecer la buena voluntad y preocupación con la que debió contar el legislador al momento de diseñar la ley N° 30096, representa –no obstante– una manifestación expansiva negativa del *ius puniendi* en la lucha contra la criminalidad, con la única finalidad de darle prestigio y presencia al Estado, el mismo que actúa indudablemente sugerido por las demandas de los medios de comunicación. Frente a tal escenario, el Estado a través del derecho penal ha recurrido una vez más a la criminalización [prevención general] y punición [prevención especial] de la lesión a la indemnidad y libertad sexual de menores de edad, figura que por demás está decir, es tutelado ya por los artículos 173°; 175°; y, 183° - A del Código Penal Peruano.

VII. El bien jurídico tutelado

Para entender y justificar la existencia de la ley penal como única manifestación de prevención y represión con la que cuenta el Estado para punir conductas⁶, debe hacerse la pregunta de qué es lo que se pretende salvaguardar con ella, o lo que equivale a decir lo mismo, cuál es su objeto de tutela, de

mayor o menor medida fuera de su alcance...” En “DERECHO PENAL ECONÓMICO Y DE LA EMPRESA” Coordinadores: Francisco R. Heydegger/ Atahumán P. Jhuliana. Idemsa, primera edición marzo del 2013. P. 13-75.

⁵ Ver artículo 5° de la Ley N° 30096.

⁶ Cfr. Jorge Rendón Vásquez. En “EL DERECHO COMO NORMA Y RELACIÓN SOCIAL” – Sección I – Fuentes de creación del Derecho – Lima agosto 1984. P. 172. // Luis Jiménez de Asúa. En “LA LEY Y EL DELITO”- La Ley Penal y su Exclusivismo – Buenos Aires – Argentina; segunda edición – marzo de 1954. P. 92. // Claude Du Pasquier. En “INTRODUCCION AL DERECHO”, traducción del francés y notas por Julio Ayasta Gonzalez. Lima – Perú tercera edición 1983. P. 34. // Eugenio Raúl Zaffaroni. En “MANUAL DE DERECHO PENAL PARTE GENERAL – TOMO I” Ediciones jurídicas 1986. P. 389. // Felipe Villavicencio Terreros. En “DERECHO PENAL PARTE GENERAL” Cuarta reimpresión, enero del 2013. P.

manera que deberá establecerse que con ella se busca la protección efectiva de ciertos valores elevados a la categoría de bienes jurídicos. El artículo 1° de la ley N° 30096 [en adelante la ley] acotando el objeto que tiene la ley, ha establecido que la misma tiene por objeto la prevención y sanción de conductas que afecten los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidos mediante la utilización de tecnologías de la información o de la comunicación con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

VIII. El *iter criminis*⁷

Cuando el artículo 5° de la ley hace una descripción típica, lo hace también respecto de una descripción cronológica de sucesos que han de verificarse en la realidad, en ese sentido, debe ajustarse el análisis típico y cronológico que aquí se pretende hacer, en función al siguiente tenor: “*el que a través de las tecnologías de información o de la comunicación, contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él*”. Recalcando siempre, que la sola puesta en peligro de tales bienes jurídicos es lo que se tutela, mas no su efectiva lesión⁸.

- La fase subjetiva-psíquica del sujeto [ideación y preparación]

Todo delito doloso precisa también de la verificación de actos previos a los comúnmente conocidos actos de ejecución y consumación, estos actos han sido estudiados para ilustrar el camino psicológico del delito en cuanto se entiende que la piedra angular o sustantivo del delito será siempre la conducta humana. Un ejemplo más familiar resultaría al imaginar si para que A matase a B [ideación] A compra el arma [preparación] y finalmente empuña el arma y dispara a B [ejecución]; nótese que de la verificación de los ejemplos antes propuestos, podemos asignar características a los actos de preparación que los diferencian de aquellos actos de ejecución, atendiendo al tiempo y forma en la que estos aparecen en la realidad. En ese sentido, los actos de preparación importan un canal⁹ que busca conectar siempre el aspecto subjetivo-natural [ideación] con el aspecto objetivo-material [ejecución], de tal suerte que la

94. // Francisco Muñoz Conde. En “DERECHO PENAL PARTE GENERAL”- 4ta edición, setiembre del 2000. P. 64.

7 Ob. Cit. Raúl Peña Cabrera. P. 295. *CAPITULO XIII – 1).- ITER CRIMINIS*.

8 Al respecto, el Dr. Jorge Luis Salas Arenas. En “INDEMNIDAD SEXUAL – TRATAMIENTO JURÍDICO DE LAS RELACIONES SEXUALES CON MENORES DE 14 A 18 AÑOS”. Primera edición. Lima – Perú, agosto del 2013. P. 38.

9 Ob. Cit. Felipe Villavicencio Terreros. P. 418.

preparación crea las *condiciones periféricas*¹⁰ exigidas por la idea delictiva del agente para poner en marcha la acción ejecutiva, la misma que tiene una conexión directa con la consumación del hecho ideado.

- La fase objetiva-material del delito [ejecución y consumación]

Con base a lo expuesto en el apartado anterior, corresponden al aspecto material del delito, los actos de ejecución y consumación del hecho¹¹.

IX. El camino y desarrollo del supuesto contemplado en el Art. 5° de la Ley N° 30096

El capítulo III de la Ley hace referencia a los delitos informáticos contra la indemnidad y la libertad sexual, por tal aseveración, podríamos llegar a una primera conclusión, y es que el objeto o bien jurídico a tutelar con el tipo penal en comento sería *–la indemnidad y la libertad sexual–*. Tal idea pareciera alejarse de la realidad cuando al echar un vistazo por el artículo 5°, se evidencia que lo realmente sancionable es la proposición con fines sexuales, por medios tecnológicos, a niños, niñas y adolescentes. Es decir, cuando el artículo en comento exige como primer acontecimiento el “contactar” a una víctima «para» preparar las condiciones de lesión a su indemnidad o libertad sexual, podemos entender que tal descripción, busca sancionar las “propuestas” con fines sexuales a niños, niñas y adolescentes a través de la tecnología.

- La fase subjetiva-psicológica [fase interna del delito]

En ese sentido, lo que pretendemos establecer es, cuál es la “idea criminal” del agente, atendiendo al artículo 5° de la ley. Si bien es cierto que el tenor del artículo se circunscribe a una *“proposición hecha por parte del agente, con fines sexuales por medios tecnológicos a niños, niñas y adolescentes”*, no podemos concebir tal idea, como el objetivo final deseado por el agente. Más razonable sería consensuar y dar por zanjado el asunto, y afirmar que la idea criminal aquí es la de obtener material pornográfico y/o sostener una actividad sexual con la víctima, ya sea ésta niño, niña o adolescente.

¹⁰ Ob Cit. Raúl Eugenio Zaffaroni. P. 343. Al respecto el profesor Zaffaroni ha preferido llamarlos “resultados concomitantes”.

¹¹ Ob. Cit. Luis Bramont Arias Torres. P. 344. – Fase Externa.

- La fase objetiva-material [fase externa del delito]

Si se entiende que lo descrito en el artículo 5° de la ley hace referencia a los actos previos, tales como ideación y preparación, los actos de ejecución y consumación son los que claramente pueden desprenderse del artículo 173° del código penal, el mismo que sanciona los actos ejecutivos sin necesidad de esperar la consumación del objeto ideado en la fase psicológica. En ese sentido, consideramos que el alcance punitivo que describe el artículo 5° de la ley carece de técnica legislativa en el sentido de que intenta sancionar con una pena actos que no corresponden a la fase objetiva-material.

X. Conclusiones

- Es vital que a la luz de las normas de Colombia y Perú, se traten temas tan álgidos y a la vez de suma importancia, como son las nuevas tecnologías que están en su máximo esplendor en los últimos veinte años, y que debido a la celeridad de los sistemas informáticos, la Legislación de cada País debe prevenir los riesgos que esto acarrea en ambas naciones, como lo son los abusos de cibernautas o delincuentes informáticos que aprovechan estas altas tecnologías para constreñir a menores de edad y a adultos en sus cuentas bancarias y personales; violando así el derecho a la intimidad entre otros, consagrado constitucional y penalmente en los ordenamientos jurídicos respectivos.

- La problemática se basa es en la facultad que tienen los padres para con sus hijos; toda vez que es de suma importancia la enseñanza desde temprana edad en el uso responsable de este tipo de redes sociales.

-Si bien es cierto que la patria potestad es de los padres; también es garante el Estado de Derecho; toda vez que es el encargado de legislar para proteger a sus hijos (los tributarios). Educando desde las escuelas a los menores de edad con el fin de prevenirlos sobre el alcance tecnológico, que puede ser para bien o para mal; dependiendo obviamente del uso que se le dé a estas herramientas informáticas.

- Los avances tecnológicos están ampliando su campo de acción y las amenazas son cada día más latentes, sin embargo la solución no sería prescindir del uso de las nuevas tecnologías de la información y comunicación, lo realmente importante es establecer reglas claras en el núcleo familiar para evitar posibles problemas con los niños, niñas y adolescentes, tomando medidas con las cuales se puede evitar que sean víctimas de este tipo de delitos. Respecto a los mecanismos de filtrado en los medios tecnológicos, no es solamente la protección que traiga el equipo en sí; sino el filtro mental que se le haga al menor debido a su comportamiento habitual o deshabitual que nos merezca especial atención en determinado momento, evitando así un colapso emocional o hasta el suicidio del menor. El mejor filtro es el padre atento.

- Los riesgos informáticos siempre existirán y hasta lo podríamos comparar con la actividad peligrosa de conducir un vehículo automotor, es bien sabido que como manejas y controlas tu vida, entre ellas la información personal, podrás ser atropellado por un delincuente informático y fácilmente vulnerar tu seguridad informática por falta de previsibilidad.
- La existencia de la ley penal en Colombia y Perú, atienden siempre a un objeto de Tutela, de manera que con ella se busca la protección efectiva de ciertos valores elevados a la categoría de bienes jurídicos. Ello como una condición de límite operacional impuesto por el propio Estado en su pretendida intromisión en el ámbito de las libertades individuales.
- El objeto que se pretende proteger con la ley 1273 de 2009(enero 05) de Colombia y el artículo 5° de la Ley 30096 de Perú, carece de buena técnica legislativa. Por el contrario, a tales supuestos, resulta más adecuado aplicar los artículos 173°, 175°, y 183–A. La era del Ciberespacio, trae aspectos innovadores en el campo de la informática, sin embargo crea nuevas conductas penales, las cuales afectan a la población vulnerable (menores de edad), ante debe de existir una regulación legal para prevenir ello.
- El *grooming*, que es una nueva modalidad del accionar de los pederastas y pedófilos, los Estados democráticos deben de concientizar de manera rápida y organizada a los menores y adolescentes, a fin de que sepan el nuevo actuar de los delincuentes.

Regulación de la protección de datos personales en Chile a la luz de los estándares internacionales. Deficiencias y Desafíos.

Patricia Reyes Olmedo*

SUMARIO: 1. La protección de datos personales en Chile. 2. Regulación vigente en Chile. 3. Estándares internacionales para la protección de datos personales. 4. Deficiencias y desafíos de la regulación chilena a la luz de los estándares internacionales.

Resumen

La aproximación actual al derecho a la protección de datos personales nos obliga a tener presente el nuevo escenario configurado por la Sociedad Red y el Gobierno de la Información que ha impulsado la incorporación masiva de la tecnología en la vida cotidiana de las personas y que ha originado un cambio de paradigma en la protección de este derecho. Si bien Chile fue uno de los países pioneros de la región latinoamericana en dictar normas de protección de datos personales, actualmente su legislación, contenida en la Ley N° 19.628, de 1999, es notablemente frágil. Este artículo describe y analiza críticamente los contenidos principales de la normativa chilena, revisa los estándares internacionales vigentes en materia de control, manejo y seguridad de la información personal, con el objeto de identificar las deficiencias y desafíos que enfrenta el país para proteger adecuadamente a sus ciudadanos, bajo el prisma de que se trata de un derecho humano fundamental.

Palabras clave: Sociedad Red y el Gobierno de la Información. Protección de datos personales.

• Aceptado por el Comité Académico para ser presentado en el XX Congreso Iberoamericano de Derecho e Informática celebrado en Salamanca, España durante el mes de octubre, 2016. Aprobado por la Junta Directiva FIADI para ser publicado en la *Revista Derecho y Tecnología*, el 16 de noviembre de 2016.

* Doctora en Comunicación, Derecho a la Información y Ética de la Universidad Complutense de Madrid. Magíster en Gestión de Organizaciones de la Universidad de Valparaíso. Abogada de la Universidad de Chile. Profesora Escuela de Derecho de la Universidad de Valparaíso. Correo electrónico: patricia.reyes@uv.cl.

Abstract

The current approach to the right to the protection of personal data forces us to take in count the new scenario configured by the Network Society and the Government of Information that has promoted the massive incorporation of technology in the daily life of people. That has originated a paradigm shift in the protection of this right. Although Chile was one of the pioneer countries in the Latin American region to dictate personal data protection rules, its legislation, contained in Ley N° 19.628, de 1999, is now remarkably fragile. This article critically describes and analyzes the main contents of the Chilean regulations, reviews the current international standards in terms of control, management and security of personal information, in order to identify the deficiencies and challenges facing the country to adequately protect its Citizens, under a view that it is a fundamental human right.

Keywords: Network Society. Information Governance. Personal data protection.

1. La protección de datos personales en Chile

El derecho a la protección de datos personales no se encuentra reconocido constitucionalmente de forma autónoma en Chile, aunque diversas iniciativas legales han sido presentadas con este objeto¹. No obstante lo anterior, se ha entendido que la Constitución Chilena², aprobada en 1980 y reformada sustancialmente en 2005, lo hace indirectamente en los artículos 19 N° 4 y 19 N°12.

Concretamente el artículo 19 N° 4 garantiza a toda persona el respeto y protección a su vida privada, a su honra, a la de su familia y a la libertad de información y el artículo 19 N° 12 consagra la libertad de emitir opinión y de informar sin censura previa, sin que pueda interpretarse que ella implique la posibilidad de acceder o dar acceso a datos personales.

En base a los preceptos constitucionales mencionados, los órganos jurisdiccionales competentes han aceptado la interposición de acciones de protección para proteger los derechos afectados por el tratamiento de datos personales. También se ha manifestado en este sentido el Tribunal Constitucional, órgano garante de la supremacía constitucional en el país, a propósito del pronunciamiento sobre publicación de las remuneraciones de altos ejecutivos

1 Actualmente en tramitación el proyecto de ley boletín N° 9384-07. Ver texto en https://www.camara.cl/pley/pley_detalle.aspx?prmID=9798&prmBoletin=9384-07

2 Constitución Política de la República de Chile. Texto completo actualizado en línea: <http://www.leychile.cl/Navegar?idNorma=242302> [Fecha de consulta: mayo de 2016]

del canal de televisión pública³, al establecer que “*la protección de la vida privada de las personas guarda una estrecha relación con la protección de los datos personales, configurando lo que la doctrina llama derecho a la autodeterminación informativa*” (considerando 25°).

En materia legal, en 1999 y tras 6 años de tramitación, Chile aprobó la Ley 19.628⁴, que rige hasta hoy en día y que se constituyó así en una de las primeras leyes sobre la materia publicada en la región. Sin embargo, debemos consignar que ella obedeció a la presión empresarial de la época de legalizar el tratamiento de datos personales, teniendo como modelo regulatorio la LORTAD española⁵ que fue derogada el mismo año de la dictación de la ley en Chile, en virtud de los cambios sustantivos que estaban ocurriendo en Europa en la manera de conceptualizar y proteger este derecho.

La ley 19.628 ha tenido sólo 4 modificaciones⁶ durante los más de 16 años de vigencia, pese a que producto de sus múltiples debilidades y falencias que describimos más adelante, se han presentado más de 50 proyectos de ley⁷ para modificarla. Al respecto, en los últimos años, se ha insistido reiteradamente, desde distintos ámbitos, en la necesidad de otorgar una regulación adecuada para la protección de datos personales en Chile. De hecho, la temática se encuentra incluida en la Agenda para la Transparencia y Probidad en los Negocios y la Política del actual gobierno, pues como se ha dicho es un compromiso pendiente con la OECD y porque resulta clave para ser declarado país seguro y adecuado por la Comunidad Económica Europea. Con este objetivo, el 2015 el gobierno preparó un anteproyecto de ley destinado a cambiar integralmente el régimen de protección de datos personales en Chile que fue sometido a consulta y a discusión técnica en una mesa público-privada. Sin embargo, hasta la fecha el proyecto no se ha presentado y más aún se ha señalado que habría un nuevo texto en preparación a punto de ser ingresado.

2. Regulación vigente en Chile

A continuación, se describen y analizan los principales contenidos de la ley 19.628.

3 STC roles acumulados N°1732-10 y 1800-10 de fecha 21 de junio de 2011. Ver texto completo en línea: <http://www.tribunalconstitucional.cl/wp/ver.php?id=1985> [Fecha de consulta: mayo de 2016]

4 Ley N° 19.628 sobre Protección de la Vida Privada. Texto completo actualizado en línea: <http://www.leychile.cl/Navegar?idNorma=141599> [Fecha de consulta: mayo de 2016].

5 Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

6 Ley 20.575 (2012), Ley 20.521 (2011), Ley 20.463 (2010) y Ley 19.812 (2002)

7 Ver proyectos modificatorios: <http://www.leychile.cl/Navegar?idNorma=1037366>

1. Ámbito de aplicación

Según el artículo 1° de la ley 19.628, ésta se aplica al tratamiento de los datos de carácter personal realizado en registros o bancos de datos, por organismos públicos o por particulares.

Como se observa, la aplicación de la ley alcanza tanto a los organismos públicos, entendiendo como tales al conjunto de órganos que forman parte de la administración del Estado, como asimismo a los entes privados que realizan tratamiento de datos personales, no obstante inexplicablemente éstos últimos quedan fuera de la obligación de registro.

2. Sujetos

La ley 19.628 distingue los siguientes tipos de sujetos intervinientes:

- a) Titular de los datos. Es el legitimado activo y se encuentra definido como la persona natural a la que se refieren los datos de carácter personal, y a quien se le confieren los derechos de acceso, modificación, cancelación y bloqueo que analizamos más adelante.
- b) Responsable del registro o banco de datos. Es el legitimado pasivo identificado como la persona natural o jurídica privada, o al respectivo organismo público, a quien competen las decisiones de tratamiento de los datos de carácter personal y reconocido como responsable del tratamiento en el derecho comparado. La imprecisión terminológica hace que se confunda al responsable del tratamiento con el responsable del fichero lo que afecta la protección.
- c) Terceros. A su respecto la ley 19.628 los reconoce como destinatarios de la transferencia o comunicación de los datos personales.

3. Tipología de los datos personales

En atención a la protección otorgada podemos reconocer las siguientes categorías:

- a) Datos de acceso público. Son aquellos que constan en fuentes accesibles al público, esto es registros o recopilaciones de acceso no restringido o reservado. Es un concepto muy controversial, pues la ambigüedad en su determinación permite que estos datos queden exceptuados de la mayoría de los resguardos establecidos en la propia ley,
- b) Datos sensibles. Son aquellos que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad. Presenta muchos reparos, pues la ejemplificación profundiza en una categorización errónea al incluir datos que no tienen tal carácter, lo que dificulta su correcta interpretación.

- c) Datos económicos, financieros, bancarios o comerciales. Si bien la ley no los define, se refiere a ellos como los provenientes de obligaciones de esta naturaleza y le dedica un título con una regulación separada.

4. Principios del tratamiento de datos personales

Si bien es cierto la ley 19.628 no contiene una conceptualización sistemática, podemos señalar que informan el tratamiento de datos los siguientes principios:

- a) Legalidad o licitud, según el cual el tratamiento de los datos personales sólo puede efectuarse cuando la propia ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello.
- b) Finalidad, que exige que los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, sin embargo, incorrectamente la ley excepciona de este resguardo el tratamiento de los datos que provengan o se hayan recolectado de fuentes accesibles al público. Ante esta debilidad, pero sólo en lo que dice relación con tratamiento de datos personales de carácter económico, financiero, bancario o comercial, la modificación introducida por la ley 20.575⁸ vino a establecer expresamente el principio de finalidad en el tratamiento de estos datos, restringiendo el tratamiento a la evaluación de riesgo comercial y para el proceso de crédito y prohibiendo expresamente la exigencia de esta información en los procesos de selección personal, admisión pre-escolar, escolar o de educación superior, atención médica de urgencia o postulación a un cargo público.
- c) Consentimiento, que dispone que será legítimo el tratamiento cuando concurra la voluntad del titular, el cual deberá ser adecuadamente informado de las consecuencias de su autorización u oposición al tratamiento. Es consentimiento debe ser informado, expreso y por escrito, y revocable. No obstante, la misma ley establece excepciones a la obtención de este consentimiento, las que en la práctica socavan el principio de finalidad pues permiten legitimar la mayoría de los tratamientos de datos personales.
- d) Transparencia, recogido parcialmente respecto de los organismos públicos, a quienes se exige el deber de notificación y registro de los bancos de datos que administran.

⁸ Ley 20.575 que establece el principio de finalidad en el tratamiento de datos personales. Texto completo en línea <http://www.leychile.cl/Navegar?idNorma=1037366> [Fecha de consulta: mayo de 2016].

- e) Calidad, que dispone el derecho a modificación, cancelación o bloqueo en el caso de datos caducos, erróneos, inexactos, equívocos o incompletos.
- f) Seguridad de los datos, en la exigencia de cuidado con diligencia, responsabilidad por los daños; y obligación de confidencialidad de las personas que trabajan en el tratamiento.
- g) Temporalidad del tratamiento, que forma parte de la configuración de lo que a nivel internacional se denomina como “derecho al olvido”, y que se reconoce sólo respecto de los datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial y respecto de algunas sanciones administrativas o penales.

5. Tutela del derecho

La ley reconoce, en su título II, los derechos ARCO⁹ a los titulares de datos, bajo la denominación de Acceso, Modificación, Cancelación y Bloqueo. Con respecto a las acciones, la ley 19.628 establece un amparo o habeas data y una acción indemnizatoria.

6. Organismo de control

Es una de las mayores debilidades del sistema y un obstáculo para que Chile sea considerado un país con un adecuado y/o seguro. El Servicio de Registro Civil e Identificación tiene a su cargo la mantención de los registros de los bancos de datos de los organismos públicos; pero sin facultades sancionatorias; y según la ley 20.285¹⁰, el Consejo para la Transparencia debe velar por cumplimiento de la ley 19.628 por los órganos de la Administración del Estado.

3. Estándares internacionales para la protección de datos personales

En el escenario internacional existe hoy consenso generalizado que hay derechos fundamentales y no fundamentales, más allá de la privacidad y/o intimidad, que se ven afectados por el tratamiento de datos personales, por lo que su protección debe ser garantizada.

La legislación, jurisprudencia y la propia doctrina han ido configurando las bases de la protección de este nuevo derecho, que en definitiva se sustenta sobre tres ejes fundamentales:

- a) El reconocimiento de que las personas a que se refieren o conciernen los datos personales son sus “titulares” o “dueños” y por ende la imposibilidad de que los terceros que los recogen, almacenan, y en

⁹ Derechos reconocidos universalmente al titular y denominados como derechos ARCO porque refieren a Acceso, Rectificación, Cancelación y Oposición.

¹⁰ Ley 20.285 sobre acceso a la información pública. Texto completo actualizado en línea <http://www.leychile.cl/Navegar?idNorma=276363> [Fecha de consulta: mayo de 2016].

general, que realizan operaciones de tratamiento, adquieran el dominio de ellos. Del mayor o menor desarrollo de este eje dependerá el régimen de responsabilidad que se defina en un Estado determinado para los actores que intervienen en el tratamiento de los datos personales.

- b) La convicción de que todo dato personal es relevante y por tanto debe protegerse su tratamiento por terceros, distintos de su titular. Esto sin perjuicio de reconocerse que existen datos con mayor relevancia o sensibilidad que otros. El desarrollo de este aspecto conlleva la configuración legal del derecho a tratar datos de terceros y el encasillamiento de cada tipo de dato personal, categoría que se considerará para su nivel de protección.
- c) Los titulares de los datos deben, en todo momento, poder controlar el uso que los terceros hacen de los datos personales que le conciernen. Esta es la base sobre la cual se desarrollan los distintos derechos que se reconocen al titular de datos personales, usualmente conocidos como derechos ARCO.

Bajo esta configuración, el nuevo derecho está siendo reconocido en las constituciones en un número creciente de países¹¹ y regulado bajo estándares comunes, que sin ser obligatorios, constituyen principios y contenidos mínimos, con pretensión de carácter universal, que han de inspirar e informar la forma y la oportunidad en las que se desarrolla el tratamiento de datos personales por parte de los responsables del mismo.

Del mismo modo, los estándares intentan implementar un sistema que sea capaz de articular la concurrencia de ciertos elementos esenciales que contribuyan a ofrecer un nivel satisfactorio de cumplimiento de las normas, conocimiento de los derechos y obligaciones de los actores del tratamiento de datos personales y de las vías y/o recursos que posibiliten amparar los derechos si éstos son amenazados o privados. Lo anterior, pues según se ha reconocido por el Grupo de Trabajo del Artículo 29 (GT 29)¹², una protección adecuada del derecho implica que las normas de protección de datos efectivamente se cumplan en la práctica, por lo que resulta necesario considerar no sólo el contenido de las normas aplicables a los datos personales, sino también el sistema utilizado para asegurar la eficacia de esas normas.

En este contexto, y en base a la Resolución de Madrid¹³ que recoge los principios, conceptos y derechos de los principales instrumentos internacionales

¹¹ El fenómeno se ha denominado Constitucionalización de la Protección de Datos Personales.

¹² El Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales (GT 29), creado por el artículo 29 de la Directiva 95/46/CE, es un órgano consultivo independiente integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea, que realiza funciones de secretariado.

¹³ Resolución de Madrid sobre Estándares Internacionales de Protección de Datos y Privacidad.

en la materia, esto es la Directiva 95/46/CE, las directrices de la OECD sobre protección de la privacidad y flujos transfronterizos de datos personales¹⁴, el marco sobre privacidad de APEC¹⁵, el Convenio 108 del Consejo de Europa¹⁶, y la Resolución 45/95 de las Naciones Unidas¹⁷, a continuación se presentan los principales estándares reconocidos internacionalmente en la materia:

1. Principios del tratamiento de datos personales

De acuerdo a los estándares revisados los siguientes principios deben informar el tratamiento:

- a) Lealtad y legalidad. Exige realizar el tratamiento de manera leal, respetando la legislación nacional aplicable y los derechos y libertades de las personas. En particular, se consideran desleales aquellos tratamientos de datos de carácter personal que dan lugar a una discriminación injusta o arbitraria contra los interesados.
- b) Finalidad. El tratamiento se limitará al cumplimiento de finalidades determinadas, explícitas y legítimas informadas por su responsable al momento de recabar los datos, el responsable se abstendrá de realizar tratamientos no compatibles con estas finalidades, a menos que cuente con el consentimiento inequívoco del interesado.
- c) Proporcionalidad. El tratamiento se limitará a aquello que resulte adecuado, relevante y no excesivo en relación con las finalidades previstas. En particular, el responsable debe realizar esfuerzos razonables para circunscribir los datos tratados al mínimo necesario.
- d) Calidad. Se asegurará en todo momento que los datos sean exactos, y se mantendrán tan completos y actualizados como sea necesario para el cumplimiento de las finalidades para las que sean tratados. Se limitará el periodo de conservación al mínimo necesario y cuando dejen de ser necesarios para el cumplimiento de las finalidades que legitimaron su tratamiento deberán ser cancelados o convertidos en anónimos.
- e) Transparencia. Se deberá contar con políticas de transparencia respecto del tratamiento de los datos. El responsable facilitará a los interesados, al menos, información acerca de su identidad, de la

¹⁴ OECD. *Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales*. 23 de septiembre de 1980.

¹⁵ Asia Pacific Economic Cooperation (APEC). *Marco sobre privacidad*. Noviembre 2004.

¹⁶ Consejo de Europa. *Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*. 28 de enero de 1981.

¹⁷ Asamblea de la Organización de la Naciones Unidas. *Resolución 45/95. Principios rectores para la reglamentación de los ficheros computarizados de datos personales*. 14 de diciembre de 1990.

finalidad del tratamiento, de los destinatarios a los que prevé ceder los datos y del modo en que los interesados podrán ejercer sus derechos, así como cualquier otra información necesaria para garantizar el tratamiento leal de los datos. La información se proporcionará de forma inteligible, empleando para ello un lenguaje claro y sencillo.

- f) **Responsabilidad.** Se deben adoptar las medidas necesarias para cumplir con los principios y obligaciones y disponer los mecanismos necesarios para demostrar con evidencia dicho cumplimiento, tanto ante los interesados como ante las autoridades de control.

2. Tratamiento de datos personales

De acuerdo con los estándares revisados, las siguientes reglas deben ser observadas en la actividad de tratamiento de datos de carácter personal:

- a) **Legitimación.** Los datos de carácter personal sólo podrán ser tratados cuando concurra alguno de los siguientes supuestos:

- Obtención previa del consentimiento libre, inequívoco e informado del interesado;
- Que un interés legítimo del responsable justifique el tratamiento, y siempre y cuando no prevalezcan intereses legítimos, derechos o libertades de los interesados;
- Que el tratamiento sea necesario para el cumplimiento de una obligación impuesta sobre el responsable por la legislación nacional aplicable, o sea llevado a cabo por un organismo público que así lo precise para el legítimo ejercicio de sus competencias;
- Que el tratamiento sea preciso para el mantenimiento o cumplimiento de una relación jurídica entre la persona responsable y el interesado;
- Que concurren situaciones excepcionales que pongan en peligro la vida, la salud o la seguridad del interesado o de otra persona. El responsable deberá habilitar procedimientos sencillos y eficaces que permitan a los interesados revocar su consentimiento en cualquier momento, y que no impliquen demoras o costos para los interesados, ni ingreso pecuniario para el responsable.

- b) **Datos sensibles.** Se consideran tales aquellos que afectan a la esfera más íntima del interesado o cuya utilización indebida pueda originar una discriminación ilegal o arbitraria o conllevar un riesgo grave. En particular, los que revelan aspectos como el origen racial o étnico, las opiniones políticas o las convicciones religiosas o filosóficas; así como los datos relativos a la salud o a

la sexualidad. Respecto de estos datos se establecerán las garantías necesarias para preservar los derechos de los interesados.

c) **Prestación de servicios de tratamiento.** El responsable podrá realizar tratamientos de datos de carácter personal a través de uno o varios prestadores de servicios, debiendo para ello velar porque cada prestador garantice, al menos, el nivel de protección previsto. Del mismo modo se deberá articular la relación jurídica a través de un contrato u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido.

d) **Transferencias Internacionales.** Será posible realizarlas cuando el Estado al que se transfieran ofrezca un nivel de protección de acuerdo a los estándares previstos. Las transferencias a Estados que no ofrezcan este nivel de protección serán excepcionales y deberán constar en documentos contractuales o legales. Se podrá atribuir a las autoridades de control la facultad de autorizar, con carácter previo a su realización, todas o algunas de las transferencias internacionales originadas en su jurisdicción.

3. Tutela del derecho

Los estándares revisados consagran los siguientes derechos y acciones:

a) **Derechos ARCO.** Se reconocen los siguientes.

- Acceso, para recabar toda información relativa a los datos de carácter personal objeto de tratamiento, tal como el origen, finalidades, destinatarios, etc.
- Rectificación y Cancelación, para solicitar la rectificación o cancelación de los datos que puedan resultar incompletos, inexactos, innecesarios o excesivos.
- Oposición al tratamiento de los datos cuando concurra una razón legítima.

b) **Ejercicio de los derechos.** Podrán ser ejercidos directamente por el interesado. El responsable deberá implementar procedimientos que permitan ejercerlos de forma sencilla, ágil y eficaz, y que no impliquen demoras o costes indebidos para ellos, ni ingreso pecuniario alguno para él. Si no procede el ejercicio de los derechos se informará al interesado de los motivos que concurran.

4. Seguridad de la información

En materia de seguridad de los datos de carácter personal administrados por el responsable, los estándares revisados establecen las siguientes reglas:

a) **Deber de protección.** El responsable y los prestadores de servicios de tratamiento deberán proteger los datos que sometan a tratamiento mediante

medidas técnicas y organizativas que resulten idóneas en cada momento para garantizar su integridad, confidencialidad y disponibilidad. Las medidas dependerán del riesgo existente, de sus posibles consecuencias para los interesados, del carácter especialmente sensible de los datos, y por supuesto del estado de la técnica y del contexto en el que se efectúe el tratamiento.

b) **Deber de confidencialidad.** El responsable y quienes intervengan en cualquier fase del tratamiento deberán respetar la confidencialidad de los mismos, aun después de finalizar sus relaciones con el interesado o, en su caso, con la persona responsable.

5. Cumplimiento y ejecución

Dentro de los estándares revisados se consideran una serie de medidas con el objeto de alcanzar una efectiva y eficaz protección del derecho. Entre ellas se destacan:

a) **Prevención y promoción.** Se incentivará el cumplimiento de las normas de protección de datos, entre otras, a través de las siguientes medidas: establecimiento de procedimientos destinados a prevenir infracciones; designación de uno o varios oficiales de protección de datos; realización de programas de concienciación, educación y formación; realización periódica de auditorías al sistema de protección de datos; adaptación de sistemas y/o tecnologías de información destinados al tratamiento de datos de carácter personal; estudios de impacto sobre la privacidad previos a la implementación de nuevos sistemas y/o tecnologías; adhesión a acuerdos de autorregulación y/o implementación de planes de contingencias.

b) **Autoridades de Control.** Existirá una o más autoridades de control que será responsables de supervisar la observancia de los principios establecidos. Dichas autoridades de control deberán ser imparciales e independientes, y contarán con la cualificación técnica, las competencias suficientes y los recursos adecuados para conocer de las reclamaciones que le sean dirigidas por los interesados, y para realizar las investigaciones e intervenciones que resulten necesarias para garantizar el cumplimiento de las normas. Sin perjuicio de lo anterior, el interesado podrá acudir directamente a la vía jurisdiccional.

c) **Cooperación y coordinación.** Las autoridades de control procurarán cooperar entre sí en aras a una más uniforme protección en relación con el tratamiento de datos de carácter personal, tanto a nivel nacional como internacional.

d) **Responsabilidad.** Los daños y/o perjuicios, tanto morales como materiales, que se hubiesen causado a los interesados, serán de cargo del responsable del tratamiento, a menos que pueda demostrar que el daño no le puede ser atribuido. Ello sin perjuicio de cualquier acción que éste pueda ejercer

contra los prestadores de servicios que intervengan en cualquier fase del tratamiento.

4 Deficiencias y desafíos de la regulación chilena a la luz de los estándares internacionales

Como hemos revisado anteriormente, el principal cuerpo normativo referido a la protección de datos personales en Chile es la ley 19.628, de 1999, titulada de protección de la vida privada. Pese a ser una norma pionera a nivel regional, la protección que ella otorga es actualmente insuficiente para garantizar la protección del derecho de acuerdo a los estándares internacionales descritos previamente.

En efecto, es posible afirmar categóricamente que la legislación chilena en esta materia presenta serias deficiencias que ya hemos esbozado, y que a continuación detallamos:

1. Débil consagración del principio de finalidad en el tratamiento de datos personales. Si bien como expusimos, la ley 20.575 vino a reforzar esta materia, lo hizo sólo respecto de determinada categoría de datos y aún persisten las debilidades provenientes de la amplitud que se consagra respecto de la excepción de consentimiento, pues permite que por esa vía se vulneren todas las normas y principios que pretendidamente protege la ley.
2. Existencia de conceptos abiertos, sujetos a interpretación, como por ejemplo lo que ocurre con el concepto de dato de acceso público, que termina radicando en el responsable del registro o banco de datos la facultad de dejar o no abierto al público y por tanto la determinación de su carácter. Estos conceptos generan dificultades interpretativas y en la práctica han servido para vulnerar la protección otorgada por la ley, con el consecuente riesgo de tratamiento de datos sin autorización del titular de los datos.
3. Falta de claridad respecto de quién es el responsable del tratamiento de datos personales. No se distingue entre el responsable del registro o banco de datos y el responsable del tratamiento de datos, como lo estipulan los estándares internacionales y por tanto en la práctica se diluyen las responsabilidades por el uso indebido de los datos personales.
4. Ausencia de regulación e incentivo al deber de información en el tratamiento de datos personales, que en la práctica se traduce en desconocimiento de los titulares de sus derechos y por tanto en la falta de ejercicio efectivo de sus derechos.
5. Ausencia de un régimen sancionatorio adecuado para infracciones a la normativa. No se establece un régimen sancionatorio eficaz ante el incumplimiento de las obligaciones que impone, las sanciones son ínfimas

o inexistentes, por lo que no constituyen mecanismos disuasivos ni correctivos adecuados.

6. Autorización para la recogida y tratamiento de datos para marketing directo, sin autorización del titular. Ello ha conducido a que en nuestro país nos encontremos desbordados por el spam o correo electrónico no deseado.
7. Atrofia del recurso de Habeas Data y abuso del recurso constitucional de protección que resulta más efectivo e inmediato para suspender la vulneración de un derecho fundamental. Entre las dificultades que presenta el recurso de habeas data encontramos las referidas a la determinación del tribunal competente; el desigual tratamiento procesal que tienen las partes en el proceso, lo que trae implícita la vulneración del debido proceso y la bilateralidad de la audiencia; y, finalmente, que no se establece un plazo de prescripción de la acción, con lo que se afecta también la seguridad jurídica.
8. Ausencia de un órgano de control independiente, que vele por el cumplimiento por parte de los organismos públicos y privados, aplique sanciones por el incumplimiento y promueva la protección de datos personales, es un vacío que quizás formalmente aparece como la mayor dificultad de Chile para cumplir el estándar internacional exigido. La facultad otorgada al Consejo para la Transparencia se enmarca dentro de su principal atribución referida a la protección del derecho de acceso a la información pública y resulta insatisfactoria en el ámbito del derecho a la protección de los datos personales.
9. Ausencia de registro de banco de datos privados y deficiencias en el registro de bancos de datos públicos. No existe el mandato de registro de las bases de datos privadas y como no se contempla sanción efectiva a la infracción de la obligación por los registros públicos, en los 16 años de vigencia el número de bancos registrados es ínfimo¹⁸, por lo cual en la práctica el registro carece de validez y confianza.

Las deficiencias antes expuestas conducen inexorablemente a la conclusión de que la legislación sobre protección de datos personales existente en Chile ha debilitado el sistema de derechos y garantías consagrados en su propia Constitución. En efecto, la inadecuada forma en que los organismos públicos y privados, como consecuencia de la tolerancia legal normativa, tratan los datos personales, ha afectado y continúa haciéndolo derechos fundamentales de los ciudadanos, como el derecho a la vida privada, al trabajo, a la educación, a la salud, etcétera.

¹⁸ Registro de Bancos de Datos Personales a cargo de organismos públicos. En línea: <http://rbdp.srcei.cl/rbdp/> [Fecha de consulta: mayo de 2016].

Del mismo modo, el no cumplimiento de los estándares internacionales trae consigo que la integración o incorporación a los bloques de países desarrollados se vea obstaculizado. En virtud de lo anterior, los desafíos son muchos, destacamos los siguientes:

1. La protección de estos datos se debe constituir en un derecho fundamental a ser tutelado por el Estado y resulta indispensable que esta tutela deje de ser estática y negativa, para convertirse en dinámica, interviniendo ante cualquier tipo y momento de tratamiento y circulación de los datos. Para avanzar en este desafío resulta perentorio la incorporación expresa del derecho a la protección de datos al catálogo de garantías fundamentales consagrado en la Constitución de la República.
2. Alcanzar los estándares internacionales de protección de datos exigidos para ser parte de una sociedad global e interrelacionada. Al respecto, se debe tener presente que los esfuerzos de integración regional y global y las exigencias universales de protección de la persona humana revelan una crisis de autosuficiencia de los ordenamientos nacionales, situación que conduce inexorablemente hacia la búsqueda y adopción de modelos y estándares regulatorios que permitan incrementar y asegurar el adecuado respeto a los derechos de las personas, en lo que se relaciona con el tratamiento de datos personales.
3. En lo específico, resulta perentorio actualizar nuestra normativa de manera de resolver el déficit institucional, mejorar el tratamiento que se hace de los principios del tratamiento de datos personales, asegurar que los derechos consagrados en la legislación sean exigibles, que quienes no respeten la ley sean sancionados y que las víctimas del tratamiento ilegal y/o abusivo de datos personales sean reparadas efectivamente, conforme lo establecen los estándares revisados. También es preciso que la normativa impregne todo el ordenamiento jurídico y se eduque a la población respecto del derecho a la protección de datos, de manera que los propios ciudadanos se constituyen en los principales custodios de su información personal.

Diligencias de investigación tecnológicas para la obtención y aportación de mensajes de WhatsApp, Snapchat o Telegram

Dr. Federico Bueno de Mata*

SUMARIO: 1. Las nuevas aplicaciones de mensajería como generadoras de pruebas electrónicas. 2. ¿Cómo obtener pruebas electrónicas de una APP? : Especial referencia al sellado de tiempo. 3. ¿Cómo aportar pruebas electrónicas de una APP? : Especial referencia al soporte electrónico. 4. Reflexiones finales en un contexto iberoamericano.

Resumen

En el presente artículo se analiza la relevancia probatoria de los archivos que a diario millones de usuarios intercambian a través de aplicaciones móviles como WhatsApp y que pueden dar lugar a ilícitos penales que deberán ser probados a través de las evidencias generadas por estas herramientas informáticas. La hipótesis de investigación esta centrada en las novedades jurisprudenciales y legislativas que se han producido en España en los años 2015 y 2016.

Palabras clave: Prueba electrónica. Obtención. Proposición. WhatsApp.

Abstract

The relevance of the files that millions of users exchange daily through mobile applications like WhatsApp and can give rise to criminal offenses that must be proven through the evidence generated by these computer tools is analyzed in this article. The hypothesis of the research is focused in case law and new regulations in Spain in 2015 and 2016.

Keywords: Electronic evidence. Obtaining. Discovery. WhatsApp.

• Aceptado por el Comité Académico para ser presentado en el XX Congreso Iberoamericano de Derecho e Informática celebrado en Salamanca, España durante el mes de octubre, 2016. Aprobado por la Junta Directiva FIADI para ser publicado en la *Revista Derecho y Tecnología*, el 16 de noviembre de 2016.

* Profesor de Derecho Procesal, acreditado a Titular. Universidad de SALAMANCA

Revista Derecho y Tecnología N° N° 2/2016 Edic. Digital - 17/2016 Edic. Ordinaria ISSN: 1317-9306 201-213

1. Las nuevas aplicaciones de mensajería como generadoras de pruebas electrónicas

Hoy en día parece que lo que no se comparte en las redes sociales no existe. La identidad digital va caminando de la mano con la identidad física hasta prácticamente mimetizarse. Si a las redes sociales le sumamos las nuevas aplicaciones consistentes en mensajería instantánea vemos que la comunicación tecnológica se ve sobredimensionada hasta el punto en el que poco a poco se va consiguiendo un efecto de aislamiento y el contacto físico va dejando paso a relaciones puramente virtuales. Si volvemos la vista atrás y pensamos cómo han evolucionado las aplicaciones de mensajería en el último lustro puede que sintamos incluso vértigo. Nombres habituales hace una década como *Symbian* o *Blackberry*, van dejando paso a aplicaciones nuevas en constante crecimiento como *Kik*, *Wire*, *Line* o a otras totalmente consolidadas como *WhatsApp*.

En este sentido, a día de hoy *WhatsApp* posee más de mil millones activos de usuarios¹, seguidos por otras aplicaciones como *Telegram* o *Snapchat*, quienes también están logrando acrecentar su número de usuarios². El peligro de estas redes es que en muchas ocasiones se pueden convertir en focos para generar problemas y conflictos con igual trascendencia que en la vida real. Así, se puede vejar, insultar, coaccionar y acosar a través de *WhatsApp* o *Telegram* o se puede utilizar *Snapchat* como una app exclusivamente diseñada para practicar *sexting*, al permitir que las imágenes y mensajes no se almacenasen en el teléfono del receptor.

En definitiva, todas estas aplicaciones son generadoras de un sinfín de pruebas electrónicas que deben ser extraídas de los terminales e incorporadas válidamente a un proceso para su valoración por el juzgador. Concretamente *WhatsApp* ya no solo sirve para enviar documentos si no que podemos encontrarnos con mensajes de audio y video, así como la realización de llamadas a través de estas aplicaciones, lo que ha hecho que la normativa española tenga que renovarse de manera precipitada a través de la promulgación de la LO 13/2015 de regulación de diligencias de investigación tecnológicas para la obtención de pruebas de este tipo. Igualmente esta ley ha sido completado por otro texto legal: la LO 42/2015 de reforma de la LECiv española por la que intenta alcanzar una política de “papel cero” en la Administración de Justicia y se intenta digitalizar y aportar todo el material probatorio en formato electrónico.

Todas estas cuestiones hacen que sea de gran importancia e interés la realización de un estudio de ante qué prueba electrónica nos encontramos y cómo podemos introducir la misma en un proceso judicial a través de un

¹ <https://blog.whatsapp.com/616/Mil-millones/> (Fecha de consulta: 15 de junio de 2016)

² En este caso Telegram o Snapchat aún solo llegan al 10% de usuarios respecto a la App líder: WhatsApp, moviéndose en la cifra de los cien millones de usuarios. Vid. <https://telegram.org/blog/100-million> (Fecha de consulta: 15 de junio de 2016)

procedimiento con unas características que respeta la naturaleza propia de este tipo de evidencia.

En el caso de las pruebas electrónicas que proceden de este tipo de prueba, estaríamos ante evidencias que proceden de medios de reproducción o archivos electrónicos, vídeos, o fotografía digital. Hablaríamos aquí de cualquier prueba que puede ser captada y presentada a través de una imagen fija o de un video a través de un dispositivo digital, con lo que aquí podrían tener cabida desde las fotografías o el video digital, hasta la captación interna de información de dispositivos como los *screenshots* o pantallazos. Las mismas tendrían ya su regulación en los artículos 382 y 384 LECiv. Igualmente podríamos hablar aquí de pruebas que se presentan mediante un *hardware* propiamente informático y que tienen una naturaleza propiamente y puramente electrónica. Entendemos que la superación entre el concepto medio- fuente de prueba podría verse distorsionado de alguna forma al pensar que el *hardware* es el apartado o soporte por el que introducimos evidencias electrónicas en el proceso....pero no es así, puesto que los medios podrían seguir siendo los ya regulados en el art. 299.1 y por tanto el soporte no es en sí un nuevo medio. Simplemente existen pruebas electrónicas que para obtener un resultado probatorio óptimo deben ser incorporadas obligatoriamente en el dispositivo en el que se guardaron o en el que se generaron, en este caso un *Smartphone*.

Por todo ello, a pesar de que demandamos una regulación autónoma, finalmente las pruebas de este tipo de aplicaciones se podrían subsumir perfectamente en la definición que la Ley de Firma Electrónica Española da para el documento electrónico en su art. 3.5 al decir que “Se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado”, y a través del art. 3.8 al regular que “El soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio”.

Pensamos que es necesario que se protocolice de forma más exhaustiva la presentación de pruebas electrónicas sobre elementos extraídos de estas aplicaciones y se regulen unos criterios de autenticación e incorporación de pruebas electrónicas al proceso con especial hincapié en la aportación de al menos de un peritaje electrónico o de un *software* que garantice la autoría de esas conversaciones y de que las pruebas no han sido manipuladas. A tenor de esta postura a mi parecer oscilante y poco contundente, avanzamos tras estudiar la importancia jurisprudencial de la prueba en los distintos órdenes y la incertidumbre respecto a distintos etapas del procedimiento probatorio, a realizar un estudio propositivo a tener de las últimas novedades legislativas españolas.

2. ¿Cómo obtener pruebas electrónicas de una App? : especial referencia al sellado de tiempo³

Cuando deseamos obtener una prueba electrónica de *WhatsApp*, *Snapchat* o *Telegram*, para que la misma sea incorporada a un proceso, lo primero que debemos tener en cuenta son los derechos fundamentales de las partes implicadas y la regulación que las ampara. Así, al hablar de derechos vinculados a este tipo de evidencia el primer artículo que conecta con esta máxima es el 18 de nuestra Constitución, donde en su primer párrafo se regula el derecho a la intimidad y a la propia imagen y en su párrafo tercero el secreto de las comunicaciones, al mismo tiempo estos derechos deberán ser interpretados de conformidad con la Declaración Universal de Derechos Humanos y los Tratados y acuerdos internacionales sobre las mismas materias ratificados por España tal y como reconoce el art. 10.2 del mismo texto legal.

Si en algún momento infringiéramos con la forma de obtención estos preceptos, sería de aplicación lo regulado en el art. 11 LOPJ, el cual nos dice que “no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales”; y por último, de forma aún más específica, debemos referirnos al artículo 287 LECiv, el cual lleva por título “Ilícitud de la prueba”, en el que su apartado primero regula que «cuando alguna de las partes entendiera que en la obtención u origen de alguna prueba admitida se han vulnerado derechos fundamentales habrá de alegarlo de inmediato, con traslado, en su caso, a las demás partes”.

Así las cosas, existen diferentes posibilidades en este escenario, pues tal y como indica acertadamente DELGADO MARTÍN⁴ siempre que la prueba electrónica se encuentre en un dispositivo propio de la parte proponente de la misma y en la que el propietario ha sido partícipe en su creación (ej. conversación mantenida por un *WhatsApp*), no generaría ninguna clase de problema en cuanto a la obtención, aunque si seguiría manteniendo sus problemas en cuanto a autenticidad e integridad. Cuestión distinta sería que la prueba se encontrara en un dispositivo ajeno o la parte aportara conversaciones de un tercero en las que el mismo no ha participado. Para este tipo de cuestiones si necesitaríamos recabar autorización judicial expresa. En este sentido, pensamos que la autorización para la obtención de pruebas vendría autorizada por el juez competente y la misma debería reunir las indicaciones contempladas en la nueva LO 13/2015 en la que se regulan las diligencias de investigación tecnológica.

Como excepción planteada por la misma ley, se especifica que la utilización de dispositivos técnicos de seguimiento y localización y la grabación de la imagen

³ Extracto de un artículo bajo mi autoría BUENO DE MATA, F. “Propuestas y retos en torno a la prueba electrónica a tenor de las últimas reformas procesales”, Revista de Privacidad y Derecho Digital, 2016, págs., 12 y ss.

⁴ DELGADO MARTÍN, J. “La prueba de WhatsApp”, *Diario La Ley*, 2015.

en espacio público puede hacerse sin necesidad de autorización judicial, en la medida en que no se produce afectación a ninguno de los derechos fundamentales del artículo 18 CE. Al mismo tiempo se establece otra excepción respecto a el acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad, ya que para recabar el número IP no será necesaria la autorización judicial al considerarse un dato público; no así otros datos vinculados a una máquina concreta como la numeración IMSI o IMEI o los códigos DNS, para los que si se necesitaría autorización previa.

Pues bien, en dicho texto legal se autoriza la intervención y registro de las comunicaciones de cualquier clase que se realicen a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual a través de una autorización motivada por el juez. Esta medida realmente es la que nos interesa de cara a la práctica judicial puesto que otras como el registro de dispositivos remotos mediante troyanos o el empleo del uso de agentes encubiertos informáticos están enfocados a recabar pruebas en el contexto de organizaciones criminales.

El art. 588 ter b apartado segundo, nos dice que en este caso se hablará de datos electrónicos, y que los mismos son “todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga”.

Pues bien, en primer lugar vemos como la autorización para obtener dichos datos electrónicos, siempre que las comunicaciones emitidas desde terminales o medios de comunicación telemática pertenecientes a una tercera persona, deberá guardar las siguientes características⁵:

- la identificación del número de abonado, del terminal o de la etiqueta técnica,
- la identificación de la conexión objeto de la intervención o
- los datos necesarios para identificar el medio de telecomunicación de que se trate.

A estas características se le tendrá que sumar el fin que persigue dicha autorización judicial respecto a los datos electrónicos. Estos objetivos pueden ser acumulativo, pero mínimamente deberá contener uno de los siguientes puntos:

- Registrar o grabar el contenido de la comunicación, con indicación de la forma o tipo de comunicaciones a las que afecta.
- Conocer el origen o el destino desde un determinado soporte, en el momento en el que la comunicación se realiza.

⁵ Art. 588 ter. LO 13/2015.

- Localizar origen o destino de la comunicación.
- Conocer otros datos de tráfico asociados o no asociados pero de valor añadido a la comunicación, teniendo que identificarlos puntualmente.

Por supuesto, no caben autorizaciones de captación y grabación de conversaciones orales de carácter general o indiscriminadas. La duración máxima inicial de la intervención, que se computará desde la fecha de autorización judicial, será de tres meses, prorrogables mediante escrito motivado por la policía judicial por períodos sucesivos de igual duración hasta el plazo máximo de dieciocho meses. Del mismo modo en el art. 588 ter e, se regula un deber de colaboración para la obtención de las pruebas de “prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática”.

Pues bien, una vez que sabemos exactamente los casos en los que necesitaríamos autorización judicial previa para obtener una prueba electrónica y cuando no, es necesario preservar la prueba desde el mismo momento de su obtención con el fin de garantizar una correcta cadena de custodia. De este modo, para asegurar la autenticidad e integridad de los soportes puestos a disposición del juez, se impone la utilización de un sistema de sellado o firma electrónica que garantice la información volcada desde el dispositivo hacia uno externo, o bien asegurar el propio dispositivo donde reside la prueba y confiscarlo si será el que se aporte al proceso. De esta manera se asegurará la conservación de los datos y la no alteración, manipulación o destrucción de los mismos para que la prueba sea practicada. En concreto la técnica del sellado consiste en hacer una copia espejo de un disco duro, memoria USB, un CD o, incluso, un teléfono móvil. Las dificultades de la realización de esta copia dependerán de los múltiples entresijos de los dispositivos electrónicos concretos⁶. Una vez con la copia hecha se encripta el mensaje a través de la aplicación de una serie de operaciones aritméticas y lógicas proporciona otro mensaje. Por ello, un mínimo cambio en el mensaje original derivará un cambio en mensaje creado.

El aseguramiento de la prueba es un recurso autónomo por el que se apuesta en una de las últimas reformas de la LECiv, concretamente gracias a la introducida por la Ley 19/2006 de 5 de junio, la cual modifica los artículos 297 y 298 LECiv⁷ y que a su vez tiene cabida concreta en la ley 13/2015 mediante la

6 PEREIRA PUIGVERT, S. “Sistema de hash y aseguramiento de la prueba informática. Especial referencia a las medidas de aseguramiento adoptadas inaudita parte”, *Fodertics II: Hacia una justicia 2.0*, Salamanca, 2014, pág. 79.

7 Ley 19/2006, de 5 de junio, por la que se amplían los medios de tutela de los derechos de propiedad intelectual e industrial y se establecen normas procesales para facilitar la aplicación de diversos reglamentos comunitarios. Disponible en <http://www.boe.es/boe/dias/2006/06/06/pdfs/A21230-21238.pdf> (Fecha de consulta: 16 de julio de 2012).

orden de conservación de datos. Esta orden tiene como fin garantizar la preservación de los datos e informaciones concretas de toda clase que se encuentren almacenados en un sistema informático hasta que se obtenga la autorización judicial correspondiente para su cesión. De este modo su posterior aportación como medio de prueba o, en su caso, su análisis forense no se verá frustrado por la desaparición, alteración o deterioro de unos elementos inherentemente volátiles. Esta norma toma como referencia el artículo 16 del Convenio sobre la Ciberdelincuencia, de 23 de noviembre de 2001, ratificado por España el 20 de mayo de 2010.

La técnica concreta avalada por esta ley es la utilización de una firma electrónica reconocida o un sistema de sellado de tiempo que garantice la información volcada o almacenada en el dispositivo original. Tal y como recoge la exposición de motivos, esta medida es paralela a la exigida en otros órdenes jurisdiccionales para la plena validez de los documentos aportados al proceso en formato electrónico y acoge una línea jurisprudencial de la Sala Segunda del Tribunal Supremo.

Ahora bien, permítame el lector de estas líneas dos reflexiones respecto al método de autenticación de la prueba, una sobre el sistema de sellado de tiempo y otra sobre la técnica del aseguramiento desde el punto de vista procesal. La primera de ellas, acerca del sellado de tiempo o técnicas de *time stamping*, hemos podido ir observando cómo han ido proliferando en el mercado a través de distintas webs sistemas de sellado automático en el que diferentes empresas de peritaje electrónico han ofrecido este servicio muchas veces incluso de manera gratuita. No citaré ejemplos de empresas concretas a efectos publicitarios pero si me permito hacer un breve comentario.

Partimos de un gigantesco desconocimiento de las técnicas de autenticación y aseguramiento de pruebas electrónicas por casi el 99% de la población española, entre las que se incluyen también operadores jurídicos como los abogados y aquellas personas encargadas de ejercer exclusiva y excluyentemente el poder jurisdiccional: los jueces. Pasar de un modelo en el que la mayoría de las pruebas electrónicas eran aportadas en formato impreso por la mayoría de los abogados o que incluso eran requeridas en formato papel por el órgano jurisdiccional

El artículo 297 de la LEC regula el aseguramiento de la prueba, estableciendo: “Antes de la iniciación de cualquier proceso, el que pretenda incoarlo o cualquiera de los litigantes durante el curso del mismo, podrá pedir del tribunal la adopción, mediante providencia, de medidas de aseguramiento útiles para evitar que, por conductas humanas o acontecimientos naturales, que puedan destruir o alterar objetos materiales o estados de cosas, resulte imposible en su momento practicar una prueba relevante o incluso carezca de sentido proponerla”. El artículo 298 de la LEC regula los requisitos necesarios para su adopción al decir que: “cuando sea probable que el retraso derivado de la audiencia previa ocasione daños irreparables al derecho del solicitante de la medida o cuando exista un riesgo demostrable de que se destruyan pruebas o que se imposibilite de otro modo su práctica si así se solicita, el tribunal podrá acordar la medida sin más trámites, mediante providencia”.

hace que veamos a día de hoy insólito este tipo de técnicas y que lleguemos a mitificarla o a otorgarle un valor que a mi parecer no es el real.

Las técnicas de sellado de tiempo parten de ser generadas mediante un software automatizado que únicamente sella en el tiempo y “cristaliza” la prueba en un momento concreto y en un estado concreto. Con ello nos olvidamos que esa prueba ha podido ser manipulada previamente y después haberla subido a una plataforma que ofrece este servicio. A través de este sellado no habrá detrás un perito, una persona que cerciore y certifique la no manipulación de dicho material, sino que un software aplicando determinadas algoritmos nos dará de manera automática un sellado y un reporte concreto de las características de los datos que estamos sometiendo a esta técnica. Por supuesto, nos encontramos ante una técnica atractiva para el consumidor, pues es mucho más barata que un peritaje electrónico y mucho más rápida...si a eso le sumamos que la propia legislación española le otorga el nivel de Firma Electrónica Reconocida...estamos ante un reconocimiento “inflado” para lo que realmente es.

Es cierto que puede ser un nuevo campo de negocio para peritos electrónicos pero realmente no estamos ante un verdadero peritaje. Un técnico en la materia incluso sacará mucho más defectos al sellado y abriría muchas más brechas de las que ahora yo estoy exponiendo, pero por el lado contrario contamos con un modelo de mercado sencillo y rápido que les puede hacer llegar de manera instantánea a miles de potenciales usuarios al tiempo que es admitido directamente por el juez y rara vez impugnado por la contraparte.

Con esto no quiero hacer ni mucho menos una crítica a los peritos informáticos, pero si poner sobre la mesa el debate sobre la validez real y precisa de este tipo de técnica y poder llegar a atisbar ciertos comportamientos ligados a la picaresca que pueden llegar a darse si se da el caso en el que una de las partes o su defensa técnica tienen unos conocimientos mucho más avanzados que la contraparte o el propio juez, cuestión que a mi entender se pudo haber dado en la famosa STS 300/2015.

Así, pensamos que se debe diferenciar bien lo que significa integridad y lo que comprende la autenticidad de la prueba, pues tal y como disocia perfectamente DELGADO MARTIN, debemos entender por autenticidad “la coincidencia de su autor aparente con su autor real, es decir, es la característica que garantiza la autenticidad del origen de los datos”, mientras que hablaríamos de la integridad de la prueba electrónica como “la característica que asegura que los datos contenidos no han sido alterados o modificados de manera no autorizada”⁸.

Con todo ello, y siguiendo además la misma línea que la sentencia citada, pienso que realmente se debería apostar más por un peritaje electrónico al margen del sellado como medida de aseguramiento....pues entiendo que a día

8 DELGADO MARTIN, J. “La prueba de WhatsApp”, *Diario La Ley*, 2015, pág. 6.

de hoy el legislador y los jueces están confundiendo esta medida con una de autenticación de la prueba electrónica...cosa distinta que si que se obtendría con la firma electrónica por la parte proponente y no por un *software* externo o más aún con la práctica de una verdadera prueba pericial en el que el informe y un examen a través de una verdadera conducta humana verifique los extremos de la prueba que se incorpora al proceso con todas las garantías.

En segundo lugar, me gustaría apuntar igualmente una reflexión procesal más profunda, tal y como ya he apuntado en otros estudios⁹, esta figura no debe confundirse con otras como la anticipación de la prueba, las diligencias preliminares o las medidas cautelares porque aunque el fundamento sea el mismo, como bien apunta GIL VALLEJO, las finalidades son distintas. En este sentido como bien indica la autora, se decide usar por el legislador en ocasiones las diligencias preliminares y las medidas cautelares para anticipar o asegurar la prueba, con el fin de agarrarse a técnicas legislativas más laxas intentando eludir los requisitos formales establecidos por la LECiv. De esta forma las medidas de aseguramiento en sí ni son medidas destinadas a la investigación de lo sucedido ni se adoptan para asegurar lo que es o será el objeto principal del pleito, sino para asegurar lo que será el objeto de prueba. Es decir, el aseguramiento de la prueba no está destinado a asegurar la efectividad de la sentencia, sino a asegurar la práctica de los medios de prueba mediante el aseguramiento de la fuente.

Por todo ello pensamos que el sellado es un mecanismo idóneo para garantizar la cadena de custodia ante una prueba tan volátil como la electrónica, pero que seguiremos valorándola con todas las cautelas, pues debería quedar completamente autenticada con el acompañamiento de un verdadero informe pericial sobre la materia en la que el propio perito esté involucrado de forma presencial.

3. ¿Cómo aportar pruebas electrónicas de una App? : especial referencia al soporte electrónico¹⁰

Entendemos por aportación el acto procesal por el cual se indica al juzgador o a los miembros del tribunal el medio o medios de prueba que se pretenden utilizar para obtener la convicción del juez; así el momento será distinto dependiendo del orden jurisdiccional en el que nos encontremos. La prueba electrónica deberá guardar por tanto los mismos plazos preclusivos que se dan para el resto de medios probatorios, por lo que esto no generaría ningún debate o propuesta añadida. Del mismo modo, siguiendo el art. 284 LECiv; la forma de proposición se hará de forma separada respecto al resto de medios de prueba

⁹ BUENO DE MATA, F., Prueba Electrónica y Proceso 2.0, págs. 232 y ss. Valencia, 2013.

¹⁰ Extracto de un artículo bajo mi autoría BUENO DE MATA, F. “Propuestas y retos en torno a la prueba electrónica...” *op. cit* , págs.. 18 y ss.

en el escrito correspondiente, es decir que cada medio de prueba se expresará con separación y haciendo constar si el medio podrá practicarse. En el caso concreto de la prueba electrónica será necesario, a tener con lo que hemos defendido en su conceptualización, que se identifiquen los elementos intangibles y tangibles de la misma. Por ejemplo deberemos señalar el *software* a través del cual se han creado los datos electrónicos y el soporte donde se encuentran ubicados. En cuanto al momento de aportación vemos que sufre un cambio desde el 1 de enero de 2016, pues la posibilidad temporal de presentar documentos ante la sede judicial electrónica se amplía hasta el infinito gracias al sistema LexNet es “es un medio de transmisión seguro de información que mediante el uso de técnicas criptográficas garantiza la presentación de escritos y documentos y la recepción de actos de comunicación, sus fechas de emisión, puesta a disposición y recepción o acceso al contenido de los mismos”¹¹.

En este sentido y conforme a lo regulado en la Ley 42/2015 vemos como la eventualidad de presentar documentos por vía electrónica está disponible las veinticuatro horas del día, todos los días del año. Así, esta manera no supone una variación en las leyes procesales sobre el tiempo hábil para las actuaciones, los plazos y su cómputo, puesto que la presentación de un documento fuera de las horas de audiencia será computado en la primera hora hábil del día siguiente. Ahora bien, para evitar una de las cuestiones más polémicas y que más quejas habría recibido la plataforma LexNet desde su implantación, acerca de los errores de envío y recepción de documentos, se exige para poder utilizar este canal que el servidor de correo electrónico usado por cualquier usuario deba contener de manera obligada la emisión de confirmaciones de envío y recepción de archivos para generar evidencias electrónicas siempre que existan fallos técnicos, paradas de sistema o indisponibilidad del servicio. Así, se dispone que el responsable último de la utilización del sistema es el Ministerio de Justicia, quién se responsabiliza de la disponibilidad del sistema.

Pero sin duda, la cuestión relevante para la prueba es la forma concreta o soporte por el que se va aportar la misma, puesto que hasta que entró en vigor la implementación de la LO 42/2015, de 5 de octubre, de reforma de la Ley 1/2000 de Enjuiciamiento Civil, la práctica extendida era la de intentar convertir en papel mediante su impresión cualquier contenido informático. En este sentido, en relación con el artículo 135 LECiv, donde se dictamina la obligatoriedad, cuando la ley lo exija, de la presentación de escritos a través de medios telemáticos, cuestión esta que recoge de manera concreta el Real Decreto 1065/2015, de 27 de noviembre, sobre comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia y por el que se regula el sistema LexNET.

El texto impone una forma concreta de presentación de pruebas electrónicas por canales electrónicos distintos, ya sea si el mismo tiene representación por

¹¹ Art. 13 Real Decreto 1065/2015, de 27 de noviembre.

procurador y asistencia por abogado o no. Si tuviera representación procesal, el art. 3 del RD expone que “todos los documentos, dictámenes, informes u otros medios o instrumentos deberán ir acompañados de un formulario normalizado y homogéneo con el detalle o índice comprensivo del número, orden y descripción somera del contenido de cada uno de los documentos. En cambio, si los ciudadanos no tuviera por qué tener postulación y quieren optar por usar medios tecnológicos para relacionarse con la administración de justicia, deberán utilizar las sedes judiciales electrónicas habilitadas para tal efecto a través de “el Servicio Compartido de Gestión de Notificaciones Electrónicas y la Carpeta Ciudadana provistos por el Ministerio de Hacienda y Administraciones Públicas siempre que los medios tecnológicos lo permitan”. Y por último, si los actos de comunicación se realizan entre procuradores, los mismos deberán utilizar la plataforma del Consejo General de Procuradores de España, la cual se encuentra aprobada técnicamente por el Ministerio de Justicia y conectada a LexNet.

Por tanto, se deberá remitir todo por canales tecnológicos y curiosamente se invertirá el procedimiento que comúnmente llevábamos arrastrando sistemáticamente....ya no imprimimos el material que estaba digitalizado sino que ahora no solo dejamos lo digital en su formato originario, sino que convertimos lo que teníamos en papel al formato digital, de ahí que tanto la LO 42/2015 como este RD se conozca popularmente como las leyes “papel cero”. Asimismo se protocoliza que esa prueba que hemos digitalizado deberá ir acompañada también de un formulario digital normalizado donde se muestre con el detalle o índice comprensivo del número, orden y descripción somera del contenido de cada uno de los documentos, así como, en su caso, del órgano u oficina judicial o fiscal al que se dirige y el tipo y número de expediente y año al que se refiere el escrito¹².

Igualmente, alguien podría pensar que este texto solo incide en los documentos que sirven para iniciar el procedimiento, pero realmente esta indicación del material tecnológico va más allá, puesto que el artículo 17 regula la incorporación del resto de evidencias por esta vía, al decir que “otros anexos, uno por cada uno de los documentos electrónicos que se deban acompañar. El usuario podrá visualizar los documentos electrónicos incorporados como anexos”.

Llegados a este punto podríamos llegar a pensar que esta indicación se podría llegar a enfrentar con una serie de obstáculos pues ¿qué ocurre si el sistema no tiene capacidad para enviar pruebas electrónicas que o bien contentan una excesiva cantidad de información o bien que ocupen excesivos bytes? El RD también da solución a esta cuestión a través de su art. 19 al regular que “se presentará en soporte digital o en cualquier otro tipo de medio electrónico que sea accesible para los órganos y oficinas judiciales y fiscales”.

¹² Este formulario normalizado se ajustará a las disposiciones del Reglamento 2/2010, sobre criterios generales de homogeneización de las actuaciones de los servicios comunes procesales (LA LEY 4125/2010), aprobado por Acuerdo, de 25 de febrero de 2010, del Pleno del Consejo General del Poder Judicial.

De esta manera el texto especifica que si estamos ante un caso de exceso de capacidad nunca recurriremos al formato papel, por lo que deberemos estregar dichas prueba en un soporte electrónico como una memoria USB, un CD o un DVD. En estos casos, los archivos deberán ser analizados con software antivirus antes de proceder a su volcado en los sistemas de gestión procesal por el personal de la oficina judicial.

La última de las dudas que se nos podría plantear es en qué formatos se deben aportar los documentos electrónicos o las imágenes digitalizadas. Para ello debemos acudir al anexo del RD, el cual regula que el escrito o documento principal deberá ser presentado en el formato PDF/A con la característica OCR (reconocimiento óptico de caracteres), es decir, deberá haber sido generado o escaneado con *software* que permita obtener como resultado final un archivo en un formato de texto editable y en el que se puedan buscar palabras. Del mismo modo deberá ir firmado electrónicamente por los profesionales actuantes.

El resto de pruebas electrónicas que se quieran aportar deberán ser presentadas según su contenido en alguno de los formatos que la Guía de Interoperabilidad y Seguridad de Catálogo de Estándares y la Guía de Interoperabilidad y Seguridad del Documento Judicial Electrónico. Pienso que es un error que la guía se refiera únicamente al documento electrónico, pues aunque el RD haga referencia igualmente a mensajes de audio, fotografía digital o video; los formatos admitidos dejan excluidos distintas pruebas electrónicas¹³, por lo que se debería ampliar aún más dichos modelos. Igualmente, aunque el resto de las pruebas únicamente sean documentos digitalizados o escaneados, no podremos presentar todas en un único PDF que contenga todos los documentos, por lo que será necesario a la hora de aportarlos, realizar una diferenciación y numeración.

Por todo lo anterior vemos como estamos ante un verdadero paso de gigante a través de una normativa que protocoliza los primeros pasos del procedimiento probatorio de pruebas electrónicas. Nos encontramos ante un texto que impone una forma concreta de presentación de pruebas electrónicas, ya que incorpora ese “mecanismo de traducción” que exige la aportación de una evidencia de este tipo al tiempo que se consigue no desnaturalizar la prueba.

4. Reflexiones finales en un contexto iberoamericano

Debemos reconocer que la legislación española se convierte en pionera respecto a la digitalización de procedimientos, pues ya no hablamos solo de sistemas de gestión de procesal informatizados sino que la digitalización llega a figuras tan importantes como la propia prueba. “El arte del proceso es, en

¹³ Punto 3, ANEXO IV. RD 1065/2015. Se recomiendan los siguientes formatos para los archivos: .pdf, .rtf, .jpeg, .jpg, .tiff, .odt, .zip. Estos últimos, los “.zip” al ser archivos comprimidos, solo podrán llevar incorporados archivos con las extensiones anteriores.

realidad, el arte de la prueba”, decía BENTHAM hace casi dos siglos¹⁴. La importancia de la fase probatoria en el proceso se infiere a través de múltiples referentes, lo cual nos revela hasta qué punto sin prueba no habría proceso, o hasta qué punto el proceso sólo se justifica porque existe algo que probar. Aún así no debemos olvidar que la gran parte de los conflictos generados ante las nuevas tecnologías tienen un componente transfronterizo, lo que obliga a que las legislaciones de los diferentes países se armonicen para dar una respuesta conjunta y lograr una verdadera interoperabilidad a la hora de obtener y aportar pruebas electrónicas en los distintos países.

No debemos olvidar que el 1 de junio de 2007 los países iberoamericanos tomaron conciencia de la necesidad perentoria que suponía incorporar las TICs a la Administración de Justicia a través de la firma de la Carta Iberoamericana de Gobierno Electrónico. En el Preámbulo de la carta nos encontramos ante un objetivo final y directo consistente en “reconocer a los ciudadanos un derecho que les facilite su participación en la gestión pública y sus relaciones con las Administraciones Públicas y que contribuya también a hacer éstas más transparentes y respetuosas con el principio de igualdad, a la vez que más eficaces y eficientes”. Así, desde un punto de vista de gestión procesal nos encontramos con el objetivo de modernizar la tramitación de los procesos y que puedan ser los propios ciudadanos los que se relacionen con las administraciones públicas a través de la vía electrónica con una serie de opciones entre las que destacaría la aportación de pruebas de este tipo

Por todo ello, debemos apostar y caminar unidos desde España no solo con Europa, sino también con Iberoamericana y crear así protocolos mundiales para la obtención, aportación y admisión de pruebas electrónicas en un proceso; sin olvidar en último caso la estandarización en la educación y capacitación de nuestros juzgadores con el fin de que tomen contacto con las especialidades de este material probatorio, pues sin duda, ellos son a quienes debemos enfocar la presentación y fundamentación de nuestras pretensiones las cuales se sustentan en muchos tipos de prueba, entre ellas, las electrónicas.

¹⁴ BENTHAM, J. *Antología*. (Traducciones de HERNÁNDEZ ORTEGA, G. y VANCELLS, M.) Barcelona, 1991, pág. 35.

Nanotecnología y Derecho: una aproximación al tema desde México

José Heriberto García Peña*

“El hecho de que la creación y la aplicación del Derecho se retrasen frente al continuo avance científico y tecnológico, ha sido hasta ahora algo comprensible e incluso justificable”.

(Rodríguez Manzanera, 2011, p. 232).

SUMARIO: I. Introducción. II. Globalización y nanotecnología: hacia una visión regulatoria. III. Nanotecnología y sus efectos jurídicos: el caso de México. IV. Principales consideraciones.

Resumen

En este trabajo se presenta una perspectiva general de las aplicaciones de la nanociencia y la nanotecnología, algunos de sus conceptos principales, y una revisión general de su status regulatorio internacional adentrándonos en el pobre desarrollo legal que coexiste en México. Asimismo, mostramos que la falta de una clara política de promoción, y la necesidad por parte de los centros de investigación de apoyos externos bilaterales, ha creado un futuro incierto para un desarrollo sostenido y articulado de una tecnociencia que promete constituir las bases de la próxima Revolución Industrial.

Palabras clave: Nanociencia. Nanotecnología. Globalización. Regulación

• Aceptado por el Comité Académico para ser presentado en el XX Congreso Iberoamericano de Derecho e Informática celebrado en Salamanca, España durante el mes de octubre, 2016. Aprobado por la Junta Directiva FIADI para ser publicado en la *Revista Derecho y Tecnología*, el 16 de noviembre de 2016.

* El autor es Maestro y Doctor en Derecho por la UNAM de México y Profesor-Investigador de tiempo completo del Tecnológico de Monterrey. Es miembro de número de la Federación Iberoamericana de Derecho e Informática (FIADI) desde 2006 y miembro pleno de la Asociación Nacional de Abogados de Empresa (ANADE) y de la Academia Multidisciplinaria de Derecho y Tecnologías A. C. (AMDETIC) en México desde su refundación. Actualmente pertenece al Grupo de Investigación de Estudios Estratégicos en el área de Derecho en la Sociedad del Conocimiento dentro de la Escuela Nacional de Ciencias Sociales y Gobierno del propio Tecnológico de Monterrey. Doctor en Derecho, Profesor-Investigador

Abstract

This paper presents an overview of the applications of nanoscience and nanotechnology, some of its main concepts, and a general review of its international regulatory status, focusing in the poor legal development that coexists in Mexico. We also show that the lack of a clear promotion policy, and the need for bilateral external support research centers has created an uncertain future for a sustained and articulated development of a technoscience that promises to form the basis of the next industrial Revolution.

Keywords: Nanoscience. Nanotechnology. Globalization. Regulation

I. Introducción

Aun cuando el desarrollo de la nanociencia y nanotecnología en el mundo pueda traer en economía o en salud entre otras áreas, pueda aportar beneficios; se hace imprescindible su regulación. Desde el punto de vista jurídico, a pesar de que las posturas son tan diversas son muchos los beneficios pero también los perjuicios. En este sentido *“no se trata de decir “no” a la ciencia y a la tecnología, sino de garantizar la socialización de los beneficios y la minimización de los riesgos para hacer ciencia y tecnología responsable”* (Delgado, UNAM, 2011).

A pesar de los avances en nanotecnología y de pensar que puede ser perfecta, en el mundo se discute sobre el peligro que podría representar para la salud humana. La aplicación de la nanotecnología en la industria farmacéutica, médica e incluso cosmética ha permitido posicionar a nivel mundial a países como Estados Unidos, China, Japón, Alemania y en Latinoamérica a Brasil, México y Argentina, como futuras potencias industriales, gracias a su nivel de inversión y número de patentes producidas en los últimos años. Especialmente relevante en la materia es la Recomendación de la Comisión Europea que contiene el *Código de conducta para una investigación responsable en el campo de la nanociencia y nanotecnología* cuyo objetivo es orientar conductas y al que deberán atenerse las disposiciones gubernamentales¹.

Cada vez hay mayor interés sobre el tema y su encuadre en el papel que juegan las nuevas tecnologías en la actual sociedad internacional, con claras evidencias en la dimensión económica y su consideración de factor para el

¹ No obstante, es conveniente poner de manifiesto que la asunción del mencionado Código por parte de la comunidad investigadora es voluntaria y que, pese a la apuesta económica realizada por la Unión Europea en este campo, no ha llegado a establecerse un código con fuerza jurídica plenamente vinculante.

desarrollo como se establece en los Objetivos del Milenio, que destacan sobre todo *la creciente necesidad de ordenar la investigación científica con la participación de todos los actores en presencia y la identificación de su incidencia en la protección de los derechos humanos internacionalmente reconocidos*.

II. Globalización y nanotecnología: hacia una visión regulatoria

La globalización actual está caracterizada por un conjunto de problemas acuciantes de difícil resolución. Desde crisis y turbulencias financieras exportadas desde los países más avanzados hasta relaciones de intercambio desigual, fuertes tensiones migratorias, debates sobre el crecimiento sostenible, cambio climático, reducción de la pobreza, desigualdades, agresiones al medio ambiente. La globalización potenciará los efectos y rápida difusión de la revolución nanotecnológica, pero ¿resultará importante estar preparados?

En principio, las actividades de producción de bienes y de servicios deberían tener por objetivo un enriquecimiento de lo humano, un aumento de potencia, en el sentido que atribuimos anteriormente a esta palabra. Por ejemplo: *aumentar las competencias de los individuos y de los grupos, favorecer la sociabilidad y el reconocimiento mutuo, ofrecer los instrumentos de la autonomía, crear diversidad, variar los placeres, etcétera*. Ahora bien, lo que quizás era solamente un imperativo moral, y por ende facultativo, a los fines de la economía clásica, tiende a convertirse en una obligación limitante, una condición del éxito. En efecto, la transformación continua de las técnicas, de los mercados y del entorno económico conlleva a que las organizaciones abandonen sus modos de organización rígidos y jerarquizados y desarrollen las capacidades de iniciativa y de cooperación activas entre sus miembros. Nada de ello es posible a menos que se incluya y se movilice de manera efectiva la subjetividad de los individuos. Pero ni la economía del conocimiento, ni la economía ampliada de las cualidades humanas deben desarrollarse como economías dirigidas, pues ello implicaría utilizar medios radicalmente opuestos a los objetivos buscados. *No mercantil no significa forzosamente estatal, burocrático, monopolista, hostil a la iniciativa privada, ni alérgico a toda forma de evaluación*. El problema de la ingeniería del vínculo social es inventar y mantener los modos de regulación a partir de un liberalismo generalizado. Según este liberalismo ampliado, *cada uno sería productor (y consumidor) individual de cualidades humanas en una gran variedad de “mercados” o contextos, sin que nadie pueda jamás apropiarse de los “medios de producción” de los que serían despojados los demás*.

La economía del futuro es, sin dudas, innovadora. Pero es también, desde los orígenes, el pedestal inmemorial de las otras economías, aquella cuyos balances invisibles deciden la ruina o el florecimiento de los pueblos. La ingeniería del vínculo social no se establece en absoluto de la nada. El Derecho por su parte,

a través de sus códigos, sus constituciones, su jurisprudencia, y sus modelos han puesto a punto técnicas conceptuales, hermenéuticas o calculatorias al servicio de una aprehensión natural, de una conmensurabilidad y de una regulación de los hechos racionales ¿Cómo negar estos fondos inmensos? Pero, “ni las religiones, los derechos y la economía clásica han enfocado explícitamente a la dinámica abierta e inmanente de la inteligencia colectiva, la valoración máxima de las cualidades humanas, el aumento y la diversificación de los poderes del ser” (Lévy, 2004).

Por otra parte, la evolución de las técnicas contemporáneas –y sobre todo técnicas de comunicación- sugiere enfoques aún inconcebibles hace algunas décadas. Ella renueva profundamente la gama de soluciones posibles a los problemas de la gestión del vínculo social y de la maximización de las cualidades humanas². Es el caso ya de la nanotecnología cuya presencia mediática ha alimentado más la imaginación que los pronósticos serios y las estrategias válidas para las empresas y para los países. La nanotecnología es fundamental dado que puede proporcionar herramientas potentísimas para el ingenio inorgánico y orgánico que pueden ser capaces de propiciar una reorganización de la sociedad, las empresas y la estructura de nuestras economías. Muchos sectores productivos y con ello países enteros podrían experimentar convulsiones importantes en sus sistemas económicos y la necesidad de adoptar cambios drásticos a efectos de garantizar su competitividad dentro de las exigencias de la actual economía global.

Por ello, se destaca la necesidad de reflexionar sobre los aspectos económicos, sociales, éticos y ambientales de la nanotecnología. Desde la perspectiva de las ciencias sociales, consideramos que estas nuevas ciencias pueden tener más beneficios que perjuicios, pero que hay casos específicos de nanomateriales a los que hay que ponerles más atención. Habría que prever como afectarían las innovaciones fundamentales derivadas de la nanotecnología a mercado inmaduros y a sectores frágiles y, en general, a empresas poco preparadas para cambios importantes y rápidos derivados de la transformación industrial. Los descubrimientos actuales permiten avances importantísimos.

Regulación jurídica:

Es difícil encontrar dentro de la normatividad jurídica de algún estado del mundo referencia directa a la regulación de la nanotecnología, sin embargo

² La experiencia reciente muestra que ha habido una muy escasa capacidad para pronosticar con precisión innovaciones, como la Internet, las comunicaciones inalámbricas, o el mapa del genoma humano. A veces, la ciencia ficción se ha aproximado más a la realidad que las previsiones de economistas o de científicos de otras especialidades.

algunos países han intentado desarrollar políticas que en el futuro pueden conducir a algún tipo de regulación³. El debate está en el terreno de la necesidad de regulación, sin embargo ningún Estado se ha atrevido a hacerlo. En los países de la Unión Europea, Reino Unido y en los EEUU, que son las primeras potencias mundiales, se han encargado de investigar y llevar a cabo el estudio minucioso del impacto social que la aplicación de la nanotecnología y su regulación legal pueden ocasionar en el mundo. Dentro de las políticas desarrolladas se destacan a continuación tres de las más importantes:

1. La UNIÓN EUROPEA, en el 2004, elaboró un documento denominado “Hacia una estrategia europea para las nanotecnologías”, en el cual se destacan aspectos fundamentales como el fomento a la investigación y desarrollo de Nanotecnología. Desde el punto de vista jurídico se destacan aspectos fundamentales para su regulación, entre los cuales cabe destacar temas fundamentales como: “Registro de patentes, Regulación en salud pública, Protección al medio ambiente y al consumidor, Metrología y normalización, Desarrollo responsable de la Nanotecnología (principios éticos), Cooperación internacional”. Producto de ella se expide por parte de la comisión de las Comunidades Europeas un comunicado al Consejo, al Parlamento Europeo y al Comité Económico y Social Europeo “*Nanociencia y Nanotecnologías: Un plan de acción para Europa 2005-2009*”, dentro del cual en el acápite 5 INTEGRAR LA DIMENSION SOCIAL RESPONDER A LAS EXPECTATIVAS Y A LAS PREOCUPACIONES, propone el reconocimiento abierto desde el principio de los riesgos que conllevan los avances nanotecnológicos.

2. En el REINO UNIDO en el año 2004, el Departamento de Comercio e Industria informó la intención de financiar el 50% del valor de 25 proyectos centrados en la nanotecnología. El total de la inversión por parte del Gobierno es más de 22 millones de Euros. El gobierno Británico no solo fomenta la investigación aplicada por medio de su programa de micro y nanotecnología, sino que fomenta la creación de instalaciones que permiten investigar en este campo. Adicionalmente el gobierno aportó más financiación durante el período 2004-2009.

3. En ESTADOS UNIDOS por su parte, desde la administración estatal se ha venido interviniendo la Nanotecnología. Los Presidentes Clinton, y Bush han apoyado con grandes fondos la investigación y desarrollo de nanotecnología, uno de esos actos es el NANOTECHNOLOGY ACT, expedido en el año 2003 por el presidente Bush. Por su parte el sector privado ha realizado grandes debates sobre los riesgos y beneficios de la nanotecnología. Es el caso del

³ De hecho en los Estados Unidos de Norteamérica, la Agencia de Protección Ambiental, defiende la posición de la necesidad de establecer una nueva legislación federal frente al manejo de las nanopartículas.

Centro para la responsabilidad de la Nanotecnología (Center for Responsible Nanotechnology-CRN-<http://www.crnano.org/>) que es uno de los ejemplos en el mundo en el análisis y divulgación de las ventajas y desventajas de la Nanotecnología. La misión de CRN es: *“Conocimiento del aumento de las ventajas, de los peligros, y de las posibilidades del uso responsable de la Nanotecnología; Desarrollar una revisión cuidadosa de las implicaciones ambientales, humanas, económicas, militares, políticas, sociales, médicas, y éticas de la fabricación molecular; y apoyo en la creación y puesta en práctica de planes y políticas adecuadas, uniformes y equilibradas para el uso mundial responsable de esta tecnología”*.

Es importante destacar que frente a la Nanotecnología, puede existir un gran interés por regular estos desarrollos y establecer controles legales. Difícilmente se podría establecer una legislación uniforme por el interés de las naciones más desarrolladas o aquellas que están ingresando en el mundo de la nanotecnología, por participar activamente dentro del desarrollo social. Algunos tendrán mayor conciencia de sus efectos y responsabilidades, y otros, por el contrario empezarán su desarrollo para comercializarla de manera irresponsable, sin que exista límite en su actuar. Coordinar esfuerzos, planificar estratégicamente, lograr establecer escenarios que posibiliten una mejor capacidad de adaptación, son tareas realmente importantes si nuestras economías quieren mirar al futuro con confianza y capacidad de explotar sus potencialidades. Una regulación que coadyuve en beneficio de los investigadores ayudaría a tomar mejores decisiones y definir prioridades para invertir el dinero que el Estado, pero también de otros actores, destinan a la nanociencia y la nanotecnología⁴.

Aunque la visión de los especialistas frente a la nanotecnología es la de mejorar los niveles de calidad, principalmente al comprender y, por tanto, combatir enfermedades con la creación de nanomedicamentos; también coinciden en la necesidad de asumir responsabilidades frente al tema: *“Podemos desarrollar mejores medicinas, empezar a combatir las grandes enfermedades de nuestro tiempo como el cáncer y la diabetes, pero igualmente podemos hacernos mucho daño por el afán de satisfacer ciertas ideas, como sucede con el uso de la nanotecnología cosmética. En ese caso hay que ver la manera de avanzar antes de desarrollar productos, en mecanismos de evaluación a nivel de toxicidad, por ejemplo”*, (Ineke Malsch, 2011)

Pese a las condiciones de responsabilidad que implica esta tecnología y las diversas discusiones que se han generado por su aplicación; la Nanotecnología y sus aplicaciones son una realidad potencial para todos los campos científicos.

4 Hasta ahora, a nivel internacional, la Organización Internacional de Estandarización ha emitido *documentos* que son guías no vinculantes y de los cuales los fabricantes de nanomateriales o nano productos pueden tomar únicamente las sugerencias que consideren pertinentes; pero falta aún mucho por hacer.

Las implicaciones del nuevo paradigma comienzan apenas a esbozarse, pero es un hecho que transformará de manera substancial el mundo tal cual ahora lo concebimos. Los cambios abarcarán no sólo lo concerniente al ámbito material, natural o económico, sino a las formas de relacionarnos y de percibirnos como seres humanos, tanto a nivel social como individual. Una de las primeras manifestaciones del proceso se gesta en los propios laboratorios. El avance de estas tecnologías requiere de visiones transdisciplinarias y, con ello, de la construcción de nuevos protocolos de investigación, con lenguajes, marcos conceptuales y metodologías creados *ex profeso* para la interacción de las disciplinas⁵. También supone nuevas formas de colaboración entre colegas de diversas áreas del conocimiento e instituciones, en muchos casos en franca competencia, y que ahora deben unir sus esfuerzos para ser capaces de atenderlo en toda su complejidad como nuevo paradigma científico. Según (Foladori Guillermo & Invernizzi Noela, 2006), *“la nanotecnología, implica una serie de riesgos, de los cuales se destacan los siguientes: para la salud de los seres vivos; para el medio ambiente; para la guerra y para la libertad individual entre otros”*.

III. Nanotecnología y sus efectos jurídicos: el caso de México

Puesto que en la nanotecnología convergen varias disciplinas, como ya se expuso es previsible que su efecto se perciba en muchos y variados campos. A mediano plazo (digamos unos 10 años) se pueden desarrollar aplicaciones múltiples y variadas. De igual modo, en los campos de la electrónica, la optoelectrónica y las tecnologías de la información y comunicaciones las nanotecnologías comienzan a jugar un papel en la fabricación de chips para computadora y en dispositivos para almacenamiento de datos. En el futuro próximo también habrá microprocesadores nanoestructurados, sistemas de comunicación en bandas diez veces más anchas que las actuales, sistemas de almacenamiento informativo con dimensiones cada vez más reducidas y capacidades mil veces superiores; también se vislumbran aplicaciones en sistemas integrados de nano sensores.

En cuanto a la medicina, el diagnóstico de enfermedades y el suministro de fármacos se investigan intensamente. Actualmente, está en fase de experimentación el uso de nanopartículas para curar enfermedades genéticas como la fibrosis quística. Y en la misma situación se encuentran las nanopartículas magnéticas que permitirían posicionar fármacos en sitios específicos mediante sistemas de campos magnéticos externos.

5 En el terreno económico, la irrupción de las tecnologías convergentes ha agudizado la competencia entre las grandes empresas globalizadas por mantenerse a la delantera y ser capaces de generar gran diversidad de productos y aplicaciones muy rentables.

Asimismo, las nanotecnologías también pueden ayudar a resolver problemas de contaminación y uso de fuentes de energía. A corto y mediano plazo se espera aprovechar ya películas nanas estructuradas en los sistemas de conversión de la energía solar, campo que asimismo se beneficiará de manera indirecta pues las nanotecnologías permitirán fabricar mejores materiales aislantes, más livianos y con mucha más resistencia. Por último, la aplicación de las nanotecnologías llegará también al sector agrícola. A nivel mundial todas las empresas que dominan el negocio de los transgénicos están invirtiendo en nanotecnologías⁶.

Hasta aquí en lo que hemos notado y se ha visto, la Nanotecnología traerá grandes beneficios a la vida humana, pero se necesita revisar los efectos negativos que puedan haber; las propiedades especiales que poseen los dispositivos nanométricos y que son las que se intenta explotar (alta reactividad superficial, habilidad de cruzar membranas celulares, etc.) Se dice que tal vez traigan consigo riesgos para la salud y el medio ambiente. Además algunos científicos han expresado su preocupación acerca de los efectos a largo plazo asociados con las aplicaciones médicas de las nanotecnologías y de si los materiales nanoestructurados serían biodegradables⁷. Hasta hoy la mayoría de los estudios realizados se basan en analogías con resultados de investigaciones sobre la contaminación del aire.

Por otra parte, la industria podría beneficiarse de contar con una instancia gubernamental que certifique los productos que contienen materiales o usan procesos nanos⁸. Asimismo, existen materiales de construcción que emplean nanopartículas diversas, nano catalizadores que se emplean en la industria petrolera y química, y otros materiales nanoestructurados utilizados en la industria automotriz, sea en las cabezas de los motores o en la propia pintura de la carrocería). Sobre todos estos productos no existe una instancia que certifique que en efecto contienen lo que dicen tener, o que hacen lo que prometen, tampoco que no exista ningún riesgo para la salud o el medio ambiente (al menos hasta donde la ciencia pueda verificar) y, por supuesto, no hay ninguna NORMA para su etiquetado.

6 Ejemplo empresas como Pfizer promueven la creación de nano cápsulas de liberación lenta que se usarán en agentes biológicos, por ejemplo, como fármacos, insecticidas, fungicidas, plaguicidas, herbicidas y fertilizantes

7 Al respecto se han encontrado algunos estudios con ejemplos relevantes: Partículas de dióxido de titanio/óxido de zinc, usadas en filtros solares, causan radicales libres en la piel, con lo que dañan el ADN; Nanotubos en los pulmones de ratas producen respuestas tóxicas mayores que el polvo de cuarzo; En 2004 se presentaron los primeros resultados sobre nano partículas de oro que pueden moverse desde la madre hasta el feto a través de la placenta; y los fullerenos causan daño al cerebro de peces y modifican las funciones de los genes.

8 Por ejemplo ya se encuentran en el mercado mexicano cepillos de dientes, edredones, antibacteriales y lavadoras que contienen o usan nanopartículas de plata; cosméticos y bloqueadores solares con nanopartículas diversas como las de dióxido de titanio.

Un panorama jurídico muy complejo:

Por su propia naturaleza, las nanotecnologías son tecnologías «universales» que sirven de plataforma para la fabricación de procesos y productos en múltiples tecnologías e industrias. Si bien su carácter transectorial ha generado un enorme revuelo acerca de su potencial, esta misma cualidad plantea importantes retos a cualquiera que desee desarrollar y comercializar productos en este campo. En el terreno de la propiedad intelectual, una patente de base de nanotubos de carbono, de nano cristales semiconductores o de procesos para su puesta en función, (por ejemplo, tiene aplicaciones en muchos campos: diseño de semiconductores, biotecnología, construcción, productos farmacéuticos, agricultura y telecomunicaciones). El titular de la patente, sin embargo, puede que sólo trabaje en uno o dos de estos campos. Por lo tanto, cualquier empresa que desee desarrollar y comercializar un producto relacionado con la nanotecnología debe examinar exhaustivamente el entorno de las patentes de nanotecnología para cerciorarse de que localiza todas las patentes bajo la titularidad de terceros. Esto, junto con una estrategia bien planificada de obtención de licencias, para asegurarse de que se dispone de licencia para todas las tecnologías patentadas pertinentes, puede facilitar enormemente la creación de un marco de trabajo, de libertad y contribuir a evitar litigios potencialmente costosos e imprevistos. Se trata de que al elaborar las reivindicaciones de una patente, los titulares de patentes nanotecnológicas también deben tener presente la complejidad del panorama internacional. El hecho de que diferentes jurisdicciones interpreten los principios que rigen la ley de patentes de diferentes maneras puede afectar a la hora de patentar una invención. Las dificultades que entrañan la detección de la infracción de patentes y la observancia de éstas sin duda han dado a los investigadores e inventores una libertad tácita y muy necesaria para actuar. Sin embargo, a medida que lleguen más productos de nanotecnología al mercado resultará más arriesgado y más difícil vigilar estas patentes.

Asimismo, en teoría además se podría retrasar los avances de la nanotecnología molecular mediante una regulación jurídica muy dura, pero esto podría empeorar las cosas a largo plazo. Si se retrasase el desarrollo hasta que fuese relativamente sencillo, entonces sería más complicado estar al día con todos los programas de nanotecnología que estén en marcha. Además, con una base tecnológica más avanzada, el desarrollo de productos nanomoleculares llegaría incluso antes de lo previsto, dejando menos tiempo para la adaptación necesaria a los cambios socioeconómicos

Es así que hoy existen Riesgos muy claros derivados de la Nanotecnología:

- Desequilibrio económico debido a una proliferación de productos baratos
- Opresión económica debido a precios inflados de forma artificial

- Riesgo personal por uso de la nanotecnología molecular por parte de criminales o terroristas.
- Riesgos para las libertades personales o sociales por restricciones excesiva
- Desequilibrio social por nuevos productos o formas de vida
- Carrera inestable de armas fabricadas con la nanotecnología.
- Daños medioambientales colectivos derivados de productos no regulados

Nanotecnología en México:

La nanotecnología representa la revolución tecnológica del siglo XXI, por lo que México (OCDE, Indicadores de Ciencia, Tecnología e Industria, 2013, consultado en sitio web: www.oecd.org/sti)⁹ debería estar a la vanguardia tanto en recursos humanos como tecnológicos para hacerle frente. Estados Unidos, Japón y la Unión Europea ya se han dado cuenta de la importancia de financiar la nanociencia y las nanotecnologías, por lo que han creado institutos específicamente dedicados a la investigación en estas áreas.

La investigación y desarrollo de nuevas tecnologías en los países en vías de desarrollo (como es el caso del nuestro) están sujetos a algunas situaciones clave, entre las de mayor importancia se encuentran: infraestructura; capacidad humana; dinero; derechos de propiedad intelectual; educación; barreras comerciales y contexto político. Estas situaciones no solo afectan al desarrollo de las nanotecnologías, deficiencias preexistentes relacionadas con la biotecnología y las tecnologías de la información pueden traducirse en otras

9 México es la séptima mayor economía de la OCDE y uno de los principales exportadores de productos manufacturados del mundo. El país ha estado atravesando un periodo de importantes reformas estructurales pero sigue enfrentándose a una serie de desafíos económicos y sociales. En líneas generales, México padece las consecuencias de un entorno de innovación débil, y la inversión en ciencia y tecnología se mantiene en un nivel bajo para los estándares de la OCDE, principalmente debido a la limitada inversión empresarial en I+D. El financiamiento público de I+D ha venido creciendo en los últimos años pero sigue situándose muy por debajo del promedio de la OCDE. Entre los obstáculos que dificultan el desarrollo del potencial innovador del país se encuentran sus patrones de especialización industrial, la elevada prevalencia de las microempresas, las brechas de competencias y una infraestructura TIC insuficientemente desarrollada y de un elevado coste. Los vínculos existentes entre la base investigadora y la economía siguen estando poco desarrollados: en comparación con economías de niveles similares de investigación en I+D, México cuenta con pocas publicaciones científicas al más alto nivel y el ritmo de colaboración entre las empresas activas en el ámbito de la innovación y las instituciones de educación superior es bajo. (Nota: La información incluida en esta nota se basa en la publicación de octubre de 2013 de OECD Science, Technology and IndustryScoreboard. Los datos se encuentran disponibles a través de www.oecd.org/sti/scoreboard)

para las nanotecnologías debido a que éstas, como ya se ha explicado, son inter y multidisciplinarias¹⁰.

En 2002, por iniciativa de varios investigadores del Instituto de Física de la UNAM, se fundó la Red de Grupos de Investigación en Nanociencia (REGINA), cuyo objetivo es promover la colaboración multidisciplinaria para generar proyectos de investigación en nanociencia optimizando el uso de recursos humanos y materiales y organizar eventos académicos para informar y difundir las investigaciones realizadas por los grupos que la integran. En abril de 2004, en el seno de esta institución, se propuso elaborar un proyecto nacional con las siguientes características:

- El uso de las nanotecnologías para solucionar problemas sociales
- Ambicioso desde el punto de vista académico.
- Formación de una red que incluya tantos grupos como sea posible.
- Factible de satisfacerse a mediano plazo.
- Los resultados deben ser, tanto como sea posible, de interés industrial.

Esto es un indicador de que el interés por las nuevas tecnologías lo comparten centros de investigación, universidades, empresas privadas y grandes corporaciones, pues ellos saben que su éxito se debe a la fuerte interrelación academia-industria, además de que en sus laboratorios de investigación y desarrollo una alta cantidad de científicos se forman y/o toman experiencia. Hoy en día, dicha política se fomenta de manera amplia, especialmente en etapas embrionarias, cuando incluso el mismo académico aún no tiene claro para qué pueda servir tal idea o resultado. Entre los obstáculos que dificultan el desarrollo del potencial innovador del país se encuentran sus patrones de especialización industrial, la elevada prevalencia de las microempresas, las brechas de competencias y una infraestructura TIC insuficientemente desarrollada y de un elevado costo.

En México no hay todavía un plan, Programa o iniciativa nacional en Nanotecnología; todo ello a pesar de que desde el 2002, la investigación en nanotecnología pasa a ser reconocida como un área de investigación estratégica. El Programa Especial de Ciencia y Tecnología 2001- 2006, consideró la nanotecnología como un área estratégica de los materiales avanzados, señalando la necesidad de contar con un Programa Nacional de Nanotecnología, y de sostener una red de intercambio científico en el área. Una de las áreas estratégicas de desarrollo del sector energético, esta relacionándolo particularmente con el Instituto Mexicano del Petróleo (IMP). Sin embargo, en 2008 se hizo un diagnóstico y en el Plan Nacional de Desarrollo 2007-2012 se

¹⁰ En México existen 17 centros académicos que realizan investigación en nanociencia y nanotecnologías, principalmente en nuevas estructuras, nano partículas, nano películas y polímeros nanos estructurados.

considera a la nanotecnología, mecatrónica y biotecnología como sectores estratégicos, según se establece en el *Eje 2. Economía competitiva y generadora de empleo*. A pesar de ser un Programa Especial no incluyó una mecánica de operación, ni un presupuesto para lograrlo, quitándole efectividad¹¹.

Ejerciendo el derecho a pensar y al bien pensar, la interrogante se manifiesta cuando nos acercamos a la voluntad real del hombre acerca de si en realidad estamos jugando o no por nuestra capacidad cada vez mayor de manipular la naturaleza a nuestro antojo y de crear instrumentos que del mismo modo nos faciliten la vida: ¿tendremos esta vez que pagar algún precio? En la actualidad esta misma pregunta que se formuló ronda en los principales foros de debate y coloquios que se han multiplicado en las principales naciones en donde la Nanotecnología ha iniciado su marcha, en los que se analizan sus consecuencias y como estas superan las fronteras del conocimiento más allá de lo que somos capaces de controlar y de prever. Pero ¿Será estéril este debate? Aun cuando el desarrollo de la nanociencia y nanotecnología en el mundo pueda traer mejoras en economía o en salud entre otras áreas, y puede aportar beneficios; se hace imprescindible la regulación legal, ya que las posturas son tan diversas como los beneficios¹².

En nuestro país NO se ha legislado eficazmente al respecto, solamente existe algo en lo que se refiere al tema medioambiental que dice tener relación con los alimentos transgénicos, por lo cual se hace necesario el análisis de estudios publicados que profundicen en el análisis de los efectos que podría tener la aplicación de la nanotecnología en los diferentes productos que consumimos y usamos a diario nos obliga como ciudadanos a conservar una constante reflexión en torno a ellas.

En realidad la nanotecnología representará un paso de gigantes en nuestra capacidad de gestionar cambios a gran escala con retos complejos y muy estimulantes desafíos. Los países harían bien activar a sus empresas y fomentar una conciencia social para prepararse para el futuro¹³.

11 Sobra decir que en el mapa mundial de la nanotecnología, México no aparece, salvo para informar que se encuentra entre los tres países de América Latina que han abordado el tema de la nanotecnología (Brasil y Chile son los otros dos).

12 Europa por ejemplo a nivel de consumidores por medio de la organización de consumidores y usuarios de la Unión Europea se ha denunciado la falta de información sobre la seguridad en el uso de nano materiales proponiendo establecer una legislación que regule su uso, puesto que a nivel de comunidad europea sólo existe un código de conducta que intenta inculcar cierta ética en el desarrollo de la investigación.

13 Un esfuerzo editorial de tal naturaleza es el de la revista MUNDO NANO. Revista Interdisciplinaria en Nanociencias y Nanotecnología. Es una publicación semestral editada por la Universidad Nacional Autónoma de México a través del Centro de Ciencias Aplicadas y Desarrollo Tecnológico, el Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades y el Centro de Nanociencia y Nanotecnología. Nació desde 2008.

IV. Principales consideraciones

Primera: La Nanotecnología puede ser un ejemplo a medio plazo de la rentabilidad de la sociedad del conocimiento.

Segunda: La Nanotecnología ofrece nuevas oportunidades y desafíos para los gobiernos. Sin embargo, el desbloqueo de este potencial requerirá un enfoque responsable y coordinado para asegurar que los posibles retos se están abordando en paralelo con el desarrollo y el uso de la tecnología.

Tercera: Resulta imprescindible la predisposición de una nación para preparar a gran escala un cambio económico de extraordinaria entidad. Es una difícil y compleja tarea.

Cuarta: En nuestro país México no se ha legislado al respecto, por lo cual se hace necesario el análisis de estudios publicados que profundicen en el análisis de los efectos que podría tener la aplicación de la nanotecnología en los diferentes productos que consumimos y usamos a diario.

Quinto: Si se contara con una regulación expresa, el Estado también podría lograr su interés de garantizar la seguridad, tanto para la salud como para el medio ambiente, de los productos nanotecnológicos que se desarrollan o comercializan en México.

Sexta: México cuenta con los recursos humanos y la infraestructura necesaria para empezar a hacer frente a esta nueva revolución tecnológica, pero, estrictamente, falta más apoyo por parte del gobierno y sus instituciones para que se alcance a plenitud la formación de más grupos interdisciplinarios y con interacción internacional.

Séptima: OCDE está jugando su parte en este proceso y se está desarrollando un gran cuerpo de trabajo. Al trabajar juntos, los países miembros buscan alcanzar una mejor comprensión de los retos y oportunidades de la nanotecnología potenciales para que puedan apoyar su desarrollo responsable y el uso.

Octava: Las nanotecnologías mejorarán muchos aspectos de la vida cotidiana y ayudarán a resolver otros que no lo son tanto, como algunas enfermedades; pero ello está condicionado por el financiamiento y aceptación del gobierno y población de cada país con algo de gran importancia: más y mejores estructuras regulatorias.

Novena: El reto para el futuro será fomentar la innovación sostenida de la Nanotecnología, asegurando que el sistema de propiedad intelectual otorgue una amplia libertad a los creadores e innovadores a la hora de desarrollar nuevas aplicaciones nanotecnológicas, sin socavar sustancialmente los incentivos para la divulgación de las patentes y la inversión que se hace en ellas.

LEGISLACIÓN

REPÚBLICA BOLIVARIANA DE VENEZUELA
TRIBUNAL SUPREMO DE JUSTICIA
SALA DE CASACIÓN PENAL

RESOLUCIÓN N° 2016-001

12 de diciembre de 2016

El Tribunal Supremo de Justicia en ejercicio de las atribuciones que le confiere el artículo 267 de la Constitución de la República Bolivariana de Venezuela, actuando en Sala de Casación Penal, previamente convocada por su Presidente, el Magistrado Doctor MAIKEL JOSÉ MORENO PÉREZ, en uso de la facultad conferida en el artículo 101 de la Ley Orgánica del Tribunal Supremo de Justicia, dicta la siguiente Resolución sobre

**PARTICIPACIÓN TELEMÁTICA DE LOS SUJETOS
PROCESALES EN LAS AUDIENCIAS DE LA SALA DE
CASACIÓN PENAL**

CONSIDERANDO

Que el artículo 26 de la Constitución de la República Bolivariana de Venezuela consagra el derecho de toda persona de acceder "... a los órganos de administración de justicia para hacer valer sus derechos e intereses, incluso los colectivos o difusos; a la tutela efectiva de los mismos y a obtener con prontitud la decisión correspondiente...", garantizando "... una justicia gratuita, accesible (...) idónea (...) y expedita, sin dilaciones indebidas, sin formalismos..."; lo que genera el deber del Estado de ofrecer nuevos medios para facilitar el ejercicio efectivo de tales derechos.

CONSIDERANDO

Que el artículo 110 de la Constitución de la República Bolivariana de Venezuela prevé que: "El Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación y 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..."; de donde resalta el deber del Poder Público, y concretamente de los órganos jurisdiccionales, de valerse de los avances tecnológicos para su optimización.

CONSIDERANDO

Que el artículo 101 de la Ley Orgánica del Tribunal Supremo de Justicia prevé que: “El Presidente o Presidenta de la Sala convocará a todos los Magistrados o Magistradas que constituyan la Sala respectiva (...) para adoptar las medidas que requieran la celeridad de los procesos y el normal y eficaz funcionamiento del Tribunal Supremo de Justicia”, por lo que la Sala de Casación Penal tiene la facultad de dictar resoluciones o adoptar cualquier otra medida necesaria para cumplir con tales fines garantizando su observancia.

CONSIDERANDO

Que el artículo 85 de la Ley Orgánica del Tribunal Supremo de Justicia prevé que: “... El Tribunal Supremo de Justicia en cada una de sus Salas favorecerá la utilización de las herramientas tecnológicas disponibles para la sustanciación de las causas sometidas a su conocimiento, para la implementación de trámites transparentes y expeditos”; de ahí que sea jurídicamente válido disponer de un sistema telemático para garantizar la participación de cualquier sujeto procesal en las audiencias que se celebren en la sede del Tribunal Supremo de Justicia.

CONSIDERANDO

Que el artículo 120 de la Ley Orgánica del Tribunal Supremo de Justicia prevé que: “... El Tribunal Supremo de Justicia y sus órganos auxiliares deberán crear, mantener y actualizar un sistema de información físico y electrónico que contenga, entre otros, el esquema actualizado de su organización y funcionamiento, así como un mecanismo de comunicación e información electrónica disponible para todas las personas”; y en consecuencia, que ese mecanismo de comunicación e información electrónica disponible para todas las personas puede consistir en un sistema de videoconferencia, por tratarse de una herramienta que posibilita la comunicación electrónica.

CONSIDERANDO

Que el artículo 2 de la Ley de Infogobierno prevé que: “Están sometidos a la aplicación de la presente Ley: 1. Los órganos y entes que ejercen el Poder Público Nacional”, y el Tribunal Supremo de Justicia forma parte del Poder Público Nacional, conforme se establece en el título V de la Constitución de la República Bolivariana de Venezuela.

CONSIDERANDO

Que el artículo 3 de la Ley de Infogobierno establece entre sus fines: "... Facilitar el establecimiento de relaciones entre el Poder Público y las personas a través de las tecnologías de información..." y "... Garantizar el ejercicio de los derechos y el cumplimiento de los deberes de las personas, a través de las tecnologías de información..."; por tanto, con esta norma se ratifica el uso de tecnologías de información y comunicación en las relaciones con el Tribunal Supremo de Justicia, donde no se excluyen las relaciones procesales.

CONSIDERANDO

Que el artículo 1 de la Ley que Regula el Uso de la Telefonía Celular y la Internet en el Interior de los Establecimientos Penitenciarios prescribe que su objeto es prevenir que se ejecuten delitos desde el interior de dichos establecimientos, mediante el uso de telefonía celular, internet y cualquier servicio de voz y datos que ofrezcan las compañías de telecomunicaciones, por lo que, sería factible autorizar el uso de tales tecnologías para fines procesales.

CONSIDERANDO

Que el artículo 11 de la Ley que Regula el Uso de la Telefonía Celular y la Internet en el Interior de los Establecimientos Penitenciarios prevé como excepción a la prohibición de instalar redes alámbricas de comunicación destinadas a prestar servicios de Internet, voz y datos en los establecimientos penitenciarios del país, su uso por parte de los reclusos bajo estricta supervisión y control de la autoridades penitenciarias, de donde se advierte la posibilidad de usar tales servicios para garantizar la participación telemática en la sala de audiencias evitando el traslado de los reclusos a la sede del Tribunal Supremo de Justicia, en especial de aquellos ubicados fuera del Área Metropolitana de Caracas.

CONSIDERANDO

Que la ubicación de la Sala de Casación Penal del Tribunal Supremo de Justicia supone que la parte procesal o su abogado, que tenga la carga de intervenir en la audiencia que convocare este órgano jurisdiccional deberá trasladarse hasta la sede del Tribunal Supremo de Justicia, localizada en la ciudad de Caracas, lo cual representa un esfuerzo adicional para acceder a la administración de justicia por parte de quienes estén domiciliados o residenciados fuera del Área Metropolitana de Caracas.

CONSIDERANDO

Que la videoconferencia u otro medio de comunicación telemático, audiovisual, bi o multidireccional e instantáneo, de prestaciones iguales o superiores, facilita el acceso a la justicia, evitando traslados, viáticos, ahorrando tiempo a las partes y a sus abogados, además de generar la optimización de la gestión judicial en salvaguarda de los derechos de los justiciables.

RESUELVE

TÍTULO I ACCESO TELEMÁTICO

**Artículo 1.
Participación
telemática**

Cualquier persona que pudiera ser citada a las audiencias que convocare la Sala de Casación Penal del Tribunal Supremo de Justicia podrá participar por medios telemáticos, ya sea mediante telepresencia, videoconferencia u otro medio de comunicación telemático, audiovisual, bi o multidireccional e instantáneo, previa aprobación emitida por el Presidente o Presidenta de la Sala de Casación Penal, siempre que los equipos y servicios tecnológicos necesarios estuvieren disponibles para tal fin y no se perjudicare el desarrollo de la audiencia o del proceso. La autorización otorgada no impide a los demás sujetos procesales, así como al público, presentarse en la sala de audiencias para el acto convocado, salvo las excepciones de ley.

**Artículo 2.
Lapso para la
solicitud de
participación
telemática**

La solicitud de participación telemática deberá consignarse en la Corte de Apelaciones cuya decisión se recurra, antes de que conste en el expediente el auto de remisión a la Sala de Casación Penal.

Fuera de ese lapso, la solicitud de participación telemática en la audiencia que convocare la Sala de Casación Penal podrá requerirse directamente al Presidente o Presidenta de la Sala de Casación Penal, mediante escrito en papel consignado en la oficina de atención al público de la Secretaría de esta Sala, o en formato electrónico dotado de firma electrónica certificada dirigido a la dirección de correo electrónico scp.secretaria@tsj.gob.ve, respetando el lapso previsto en el primer aparte del artículo siguiente. La Secretaria de la Sala dejará constancia en el expediente de la petición digital, sin necesidad de imprimirla e incorporarla al mismo.

La Secretaría de la Sala de Casación Penal deberá contar con un sistema informático de alerta sobre la recepción diaria de mensajes de datos en la dirección de correo electrónico antes indicada, sin perjuicio del deber de revisar diariamente, al cierre de la oficina de atención al público, el buzón de entrada de dicho servicio.

Las solicitudes recibidas fuera del horario de atención al público se entenderán entregadas al día hábil siguiente.

**Artículo 3.
Notificación de la
decisión**

La autorización o negativa para participar por telepresencia, videoconferencia u otro medio de comunicación telemático, audiovisual, bi o multidireccional e instantáneo, cuando se hubiere presentado antes de la admisión del recurso de casación o de la pretensión de extradición, se comunicará con la citación para la audiencia y se publicará en las cuentas del portal de Internet del Tribunal Supremo de Justicia.

Si la solicitud se presentare luego de la citación, deberá notificarse la respuesta al menos siete (7) días hábiles antes de la fecha para la cual fue fijada la audiencia.

En ambos casos, se podrá comunicar por cualquier medio tecnológico indicado al efecto, conforme a lo previsto en el numeral 3 del artículo 91 de la Ley Orgánica del Tribunal Supremo de Justicia.

**Artículo 4.
Derecho a
presentarse
directamente**

La autorización para intervenir por medios telemáticos en la audiencia convocada por la Sala de Casación Penal no impide que el solicitante pueda acudir directamente a la sala de audiencias el día fijado para ello. La Secretaría de la Sala dejará constancia en acta de lo ocurrido.

**Artículo 5.
Suspensión o
cancelación de la
audiencia telemática
desde una sede
oficial venezolana**

En caso de imposibilidad o inidoneidad de la intervención telemática desde una sede oficial venezolana, el Presidente o Presidenta de la Sala de Casación Penal deberá suspender la audiencia, fijando su continuación o reinicio, una sola vez, para otra oportunidad del mismo día o reiniciándola en otra fecha.

Ante tal evento, podrá ordenar que la audiencia se celebre directamente en la sala de audiencias, notificando la nueva fecha al interviniente, conforme al lapso previsto en el artículo 458 del Código Orgánico Procesal Penal.

**Artículo 6.
Suspensión o
cancelación de la
audiencia
telemática fuera de
la sede oficial
venezolana**

Si la intervención fuera autorizada desde algún lugar distinto a una sede oficial venezolana, la audiencia no se suspenderá sino que se celebrará con quienes comparezcan, como lo prevé el artículo 458 del Código Orgánico Procesal Penal, salvo que el Presidente o Presidenta de la Sala de Casación Penal tome otra decisión, a solicitud de parte interesada, conforme a lo previsto en el párrafo anterior.

Si no asistiere el defensor privado, directamente o por medio de las tecnologías de información y comunicación permitidas, la defensa ante la Sala de Casación Penal será ejercida, de igual manera, por el defensor público a quien se le hubiese asignado formalmente en la causa.

**Artículo 7.
Medio alternativo de
comunicación**

Deberá ponerse a disposición de la autoridad encargada de presenciar la intervención telemática, si fuere el caso, o del propio interviniente desde el lugar de emisión, un teléfono o algún otro medio de comunicación oral o audiovisual con la Sala de Casación Penal del Tribunal Supremo de Justicia, para resolver cualquier eventualidad que pudiera surgir durante el desarrollo de la audiencia, en especial en caso de imposibilidad o inidoneidad de la transmisión.

El equipo de comunicación deberá permanecer en modo silencioso durante la audiencia.

Artículo 8.

Las audiencias en la Sala de Casación Penal del Tribunal Supremo de Justicia se realizan en el horario comprendido entre las 10:00 a. m. y la 1:00 p. m., salvo que el Presidente o la Presidenta de la Sala ordenare su celebración en otro horario, de oficio o a petición de parte interesada.

TÍTULO II LUGAR DE EMISIÓN DE LA INTERVENCIÓN

**Artículo 9.
Emisión de la
intervención desde
sede oficial del
Estado**

Quien solicitare participar por medios telemáticos en la audiencia podrá ser autorizado para hacerlo desde un espacio adecuado para ello, ubicado en cualquier sede oficial de la República Bolivariana de Venezuela, bien sea judicial, administrativa o, incluso, diplomática en el extranjero, según el caso.

La participación telemática en la sala de audiencias de la Sala de Casación Penal desde los establecimientos penitenciarios indicados en el artículo 2 de la Ley que Regula el Uso de la Telefonía Celular y la Internet en el Interior de

los Establecimientos Penitenciarios deberá realizarse, con estricta supervisión y control de las autoridades penitenciarias, en cumplimiento de lo previsto en el artículo 11 del referido texto legal.

**Artículo 10.
Emisión de la
intervención fuera
de una sede oficial**

El Presidente o Presidenta de la Sala de Casación Penal también podrá autorizar la participación telemática desde espacios distintos a alguna sede oficial del Estado, a petición de parte, siempre que ello no afectare los derechos de los demás sujetos procesales, ni perjudicare el desarrollo de la audiencia o del proceso en general.

En este caso, la autorización quedará condicionada a los resultados positivos de la prueba de conexión prevista en el artículo 13 y a que el interviniente garantice por escrito, en la misma solicitud de participación por medios telemáticos, que la actuación se realizará desde un área ordenada y sin ruidos molestos, y que mantendrá la confidencialidad de la transmisión de la audiencia.

**Artículo 11.
Participación de
funcionarios de
misiones diplomáticas
acreditadas en la
República Bolivariana
de Venezuela**

Los funcionarios adscritos a las misiones diplomáticas extranjeras, acreditadas en la República Bolivariana de Venezuela, podrán ser autorizados a intervenir en la audiencia de extradición desde dicha sede. En este caso, deberá garantizarse por escrito la confidencialidad de la transmisión de la audiencia.

**Artículo 12.
Presencia de
funcionario**

En el supuesto previsto en el artículo 10 de esta Resolución, el Presidente o Presidenta de la Sala de Casación Penal podrá ordenar la presencia de uno o más funcionarios judiciales y/o de los cuerpos de seguridad del Estado, a fin de velar por el cumplimiento de garantías suficientes para el desarrollo del referido acto procesal telemático.

En los supuestos de solicitud de participación desde territorio extranjero o desde sedes diplomáticas extranjeras ubicadas y acreditadas en la República Bolivariana de Venezuela, el Presidente o Presidenta de la Sala de Casación Penal podrá condicionar la aprobación de la solicitud de intervención procesal telemática, a la presencia del o los funcionarios referidos en el encabezado de esta norma.

El funcionario designado podrá comprobar la identidad del interviniente, la presencia de elementos que pudieran

interrumpir el buen desarrollo de la audiencia telemática y mantener el orden durante la exposición, en cumplimiento de las instrucciones que emita el Presidente o Presidenta de la Sala de Casación Penal.

**Artículo 13.
Prueba de conexión**

Cuando la declaración se emitiera fuera de alguna sede oficial venezolana, se realizará una prueba de conexión, dentro de los cinco (5) días hábiles siguientes a la admisión del recurso o pretensión, con participación de los técnicos informáticos dispuestos por la Sala de Casación Penal del Tribunal Supremo de Justicia y los técnicos o la persona que se encontrare en el lugar de emisión, a fin de asegurar que se cuenta con suficiente calidad en la imagen y el sonido.

En caso de resultar suficiente, según dictamen escrito de los técnicos dispuestos por la Sala de Casación Penal, el Presidente o Presidenta de la Sala de Casación Penal autorizará la participación telemática en la audiencia previamente admitida, lo cual se notificará al requirente por el medio indicado para ello, al menos siete (7) días hábiles antes de la fecha para la cual fue fijada la audiencia.

**Artículo 14.
Asistencia técnica en
el uso de los medios
telemáticos**

Durante la audiencia telemática deberán estar presentes técnicos informáticos en la sala de audiencias de la Sala de Casación Penal, para resolver cualquier problema de conexión, audio o video que pudiere suscitarse.

El Presidente o Presidenta de la Sala de Casación Penal podrá ordenar la presencia de técnicos informáticos en el lugar de emisión de la declaración. En caso de emitirse desde fuera de una sede oficial venezolana la presencia del técnico será responsabilidad del solicitante atendiendo a lo previsto en el artículo 34 de la presente Resolución.

En todo caso, la ausencia de los técnicos a los que se refiere esta disposición no acarrea la nulidad del acto.

**Artículo 15.
Publicidad en el
lugar de la
declaración**

A petición de parte, la Sala de Casación Penal podrá autorizar la presencia de público en el lugar desde donde se emitirá la declaración, siempre que ello no perjudique el desarrollo de la audiencia, del proceso en general o la seguridad de los presentes en el lugar de la intervención.

En todo caso, la publicidad de la audiencia se garantiza con la presencia del público en la sala de audiencias de la Sala de Casación Penal, salvo la excepción prevista en el artículo siguiente.

Artículo 16.
Audiencia telemática
privada

Si la audiencia debiere ser privada por disposición legal, la transmisión de la declaración únicamente deberá efectuarse desde una sede oficial venezolana, pero también podrá practicarse desde sede oficial extranjera si el interviniente se encontrare fuera del territorio nacional.

Artículo 17.
Intercepción y
difusión no
autorizada

La interceptación y difusión no autorizada de la audiencia, de la participación de alguno de los sujetos procesales intervinientes o la difusión del registro sonoro o audiovisual de tal acto procesal, será sancionada conforme a la Ley Especial Contra los Delitos Informáticos.

El registro sonoro o audiovisual del acto procesal estará disponible para consulta en la sala de audiencias de la Sala de Casación Penal conforme lo prevé el Código Orgánico Procesal Penal en el artículo 317, para las audiencias de juicio oral y público.

TÍTULO III

ASISTENCIA JURÍDICA

Artículo 18.
Asistencia jurídica de
la persona privada de
libertad en la Repú-
blica Bolivariana de
Venezuela.

En caso de que el interviniente a distancia fuere el imputado privado de libertad en la República Bolivariana de Venezuela, deberá estar asistido de uno o dos defensores presentes en el lugar desde donde declarare y de uno o dos defensores presentes en la sala de audiencias, sin que en su conjunto superen el número de tres, conforme a lo dispuesto en el artículo 141 del Código Orgánico Procesal Penal. En ambos casos, podrá nombrarlos y pagar sus honorarios él mismo, o en su defecto, la República Bolivariana de Venezuela se los asignará de forma gratuita. Pero si el imputado estuviere sometido al proceso penal estando en libertad, podrá participar en la audiencia aunque el abogado defensor no compartiere igual espacio físico tangible.

En caso de estar asistido por dos defensores públicos, se encargará de la defensa, en cuanto al recurso de casación o a la pretensión de extradición, el abogado autorizado para actuar ante la Sala de Casación Penal; en este caso, las funciones del defensor público presente en el lugar de privación de libertad se limitarán a garantizar sus derechos en el sitio, salvo que también estuviere autorizado para actuar ante la Sala de Casación Penal.

Si la defensa estuviera constituida por un defensor privado y uno público autorizado para actuar ante la Sala de Casación

Penal, ambos podrán intervenir en el orden que le manifiesten a la Secretaria de la Sala, respetando el tiempo previsto para ello.

Artículo 19.
Asistencia jurídica
fuera de la República
Bolivariana de Vene-
zuela.

En los procesos de reextradición o de ampliación de la extradición, la República Bolivariana de Venezuela solicitará al Estado requirente, con base en el principio de reciprocidad internacional, que la persona ubicada en el extranjero, impedida de pagar su propia defensa, cuente con asistencia jurídica a cargo del referido Estado. En todo caso, se le asignará un defensor público en la República Bolivariana de Venezuela, autorizado para actuar ante la Sala de Casación Penal.

Artículo 20.
Confidencialidad de
la comunicación
con el defensor o
defensora

El Estado venezolano garantizará un sistema de comunicación confidencial entre el imputado y su defensor o defensora presente en la sala de audiencias de la Sala de Casación Penal desde antes del inicio de la audiencia y hasta diez minutos después de la finalización de la audiencia, a solicitud del imputado, a fin de informarse sobre el proceso.

Artículo 21.
Intérprete.

La Sala de Casación Penal garantizará la presencia de intérprete público para el interviniente, y los defensores, en la sala de audiencias de la Sala de Casación Penal, cuando fuere necesario.

TÍTULO IV

IDENTIFICACIÓN DEL INTERVINIENTE Y DEL TRIBUNAL

Artículo 22.
Identificación
telemática

Cualquier persona citada a una audiencia en la Sala de Casación Penal será identificada con su cédula de identidad o pasaporte vigentes, según el caso.

Los defensores, apoderados judiciales y asistentes privados, deberán identificarse, adicionalmente, con su carnet de inscripción en el Colegio de Abogados y en el Instituto de Previsión Social del Abogado; mientras que el defensor público y el fiscal del Ministerio Público lo harán con la credencial emitida por el Tribunal Supremo de Justicia para actuar ante la Sala de Casación Penal.

El interviniente mostrará el documento que corresponda, ante la cámara, de modo que el Secretario o la Secretaria de la Sala de Casación Penal deje constancia en autos.

Artículo 23.
Identificación fuera
de una sede oficial
venezolana

El autorizado para intervenir en la audiencia penal por medios telemáticos fuera de alguna sede oficial de la República Bolivariana de Venezuela se identificará conforme al artículo 21 de la presente Resolución y, si lo estimare necesario el Presidente o Presidenta de la Sala de Casación Penal, ordenará que se proceda de acuerdo con lo estipulado en el artículo 12.

Así mismo, el Presidente o Presidenta de la Sala de Casación Penal podrá solicitarle que envíe copia digitalizada del documento de identidad a la Secretaría de la Sala de Casación Penal mediante la dirección de correo electrónico: scp.secretaria@tsj.gob.ve o por cualquier otro medio telemático que le indicare, pudiendo exigir, además, que el mensaje de datos que contiene la copia digital del documento de identificación, tuviere firma electrónica certificada.

Artículo 24.
Identificación desde
la sede oficial de
participación

Cuando la intervención se emita desde una sede judicial de la República Bolivariana de Venezuela, el Presidente o Presidenta de la Sala de Casación Penal podrá ordenar que la verificación de la identidad sea realizada por el secretario del órgano judicial comisionado, aunada o excluyendo la identificación telemática.

Para tal fin, se anexará al oficio de comisión una copia de los documentos donde constare la designación y juramentación del defensor o del poder otorgado al representante judicial de la víctima, cuando se tratare de ese supuesto.

Igualmente, si la declaración se emitiera desde una sede oficial no judicial venezolana, incluyendo el lugar de privación de libertad o una oficina diplomática venezolana, la máxima autoridad de la institución desde donde participará la persona citada, o el funcionario designado por aquella, podrá comprobar la identidad del interviniente, sin perjuicio de lo establecido en el artículo 21, por indicación del Presidente de la Sala de Casación Penal.

Artículo 25.
Identificación en caso
de reextradición o
ampliación de extra-
dición

En los casos de reextradición o ampliación de la extradición, aunado o excluyendo el procedimiento de identificación telemática, el órgano jurisdiccional extranjero podrá comprobar la identidad del declarante y del defensor según su legislación, así como también con el pasaporte vigente, si lo tuviere.

Si la participación telemática en la sala de audiencias se emitiera desde una sede diplomática venezolana en el extranjero se procederá conforme al único aparte del artículo anterior.

**Artículo 26.
Identificación de la
Sala de Casación
Penal**

Para garantizar al declarante que la audiencia se está realizando ante la Sala de Casación Penal deberá crearse un enlace en la página de Internet del Tribunal Supremo de Justicia para tal fin. En su defecto, la Sala de Casación Penal notificará al interviniente, en el texto de la citación, el método de conexión.

**Artículo 27.
Acto de comprobación de identidad**

La comprobación telemática de la identidad se realizará, al menos, dentro del lapso de treinta (30) minutos previos al inicio de la audiencia. Este trámite será comunicado en la citación para la audiencia telemática o en la notificación por la que se admita la intervención telemática solicitada, luego de verificarse la prueba de conexión prescrita en el artículo 13.

**Artículo 28.
Juramentación a distancia**

En el supuesto de revocación del defensor para el momento de la audiencia o designación de un defensor adicional hasta el límite permitido por el Código Orgánico Procesal Penal, el abogado que se incorpore al proceso deberá juramentarse, bien sea directamente o por medios telemáticos ante la Sala de Casación Penal o directamente ante el órgano jurisdiccional desde donde intervendrá, según el caso.

Si el defensor revocado no pudiere ser suplido por otro defensor de confianza, la audiencia se celebrará con el defensor público presente en la sala de audiencias, previamente designado para intervenir en la causa.

**Artículo 29.
Acta de identificación y de juramentación**

En caso de comprobarse la identidad o practicarse la juramentación por medios telemáticos la Secretaria de la Sala de Casación Penal, en atención a lo previsto en el artículo 153 del Código Orgánico Procesal Penal, lo hará constar en autos, especificando la imposibilidad de firmar el acta por parte del interviniente por medios telemáticos.

Si la identidad se comprobare en el lugar desde donde se emita la intervención, el Presidente o Presidenta de la Sala de Casación Penal podrá ordenar que se levante un acta firmada por los participantes, la cual se remitirá a la Sala al

finalizar la audiencia. Esta acta complementará la elaborada en la sala de audiencias.

TÍTULO IV ASPECTOS OPERATIVOS

**Artículo 30.
Organización de la
sala de audiencias
telemáticas**

La sala de audiencias deberá adaptarse a la participación por medios telemáticos. En consecuencia, deben incorporarse:

a. Una o más cámaras que permitan al interviniente a distancia observar a los Magistrados, y a la otra parte presente en la sala de audiencias o interviniendo a distancia, así como también disponer de una vista general de la sala y del público asistente.

b. Micrófonos y sistema de sonido por los que se comunicarán los presentes, que capten y difundan con suficiente claridad las intervenciones, para garantizar el derecho a la defensa.

c. Un sistema de proyección de la imagen del declarante a distancia, la cual deberá ser percibida por los Magistrados de la Sala de Casación Penal, y demás sujetos procesales, de la manera más parecida posible a la presencia personal en la sala de audiencias, de quien interviniera valiéndose de la telemática.

d. Un equipo electrónico que permita la videoconferencia o algún otro sistema de telecomunicación audiovisual, bi o multidireccional e instantánea, entre los intervinientes en la audiencia.

e. Un programa informático que permita la telecomunicación entre los intervinientes en la audiencia.

f. Un teléfono celular o algún otro medio de comunicación oral que permita la conexión clara y continua entre el lugar de emisión y la sala de audiencias en la Sala de Casación Penal del Tribunal Supremo de Justicia.

g. Un sistema de transferencia de datos de uso exclusivo del Poder Judicial o en su defecto, conexión a Internet.

- Artículo 31.
Bidireccionalidad** El interviniente por medios telemáticos deberá contar con el equipo técnico necesario para ver y escuchar, en tiempo real, a los presentes en la sala de audiencias de la Sala de Casación Penal, así como también para participar cuando se le autorice y para contestar las preguntas que pudieren hacerle los Magistrados. Tales equipos deben permitirle percibir con calidad suficiente, lo ocurrido en la sala de audiencias.
- Artículo 32.
Rango de visión** Los Magistrados deberán contar con una visión amplia de la persona interviniente a distancia a fin de apreciar sus expresiones corporales en el curso de la participación.
- Artículo 33.
Intervenciones** El orden y la duración de las intervenciones de los sujetos procesales por medios telemáticos serán indicados por el Presidente o Presidenta de la Sala de Casación Penal al comenzar la audiencia o al momento de ceder la palabra, con base en las previsiones del Código Orgánico Procesal Penal y de la Ley Orgánica del Tribunal Supremo de Justicia.
A fin de cumplir con el tiempo otorgado para intervenir, el Alguacil de la Sala de Casación Penal, por indicación del Secretario o Secretaria o del Presidente o Presidenta de la Sala, le comunicará al declarante que dispone de determinado lapso para culminar su intervención. La comunicación podrá realizarse por un sistema informático o simplemente mostrando ante la cámara el cartel con la información pertinente.
- Artículo 34.
Vestimenta** El uso de la toga es obligatorio para los abogados. Los demás intervinientes deberán vestirse acorde a la solemnidad del acto.
- Artículo 35.
Costos** Los gastos necesarios para intervenir por medios telemáticos en la audiencia que convocare la Sala de Casación Penal serán pagados exclusivamente por el interviniente, cuando participe desde fuera de una sede oficial venezolana. En este supuesto quedan excluidos los gastos en que deba incurrir la Sala de Casación Penal para emitir, recibir y proyectar la imagen y el sonido del interviniente por medios telemáticos.
Si la emisión de la declaración se produjere desde alguna sede oficial venezolana equipada para tal fin, los costos de transmisión serán a cargo del Estado.

En caso de ampliación de la extradición o de reextradición, el Tribunal Supremo de Justicia exhortará al Estado requirente a cubrir los costos de la declaración que se presente desde territorio extranjero, salvo que la declaración se emitiera desde una sede diplomática o consular de la República Bolivariana de Venezuela, en cuyo caso, los gastos de transmisión telemática de la declaración serán por cuenta del Estado venezolano.

Artículo 36.
Interoperabilidad.

Los órganos y entes del Estado deberán disponer de sistemas telemáticos que les permitan intercambiar los datos y documentos necesarios para garantizar la participación telemática de quienes fueren autorizados para ello, en la sala de audiencias de la Sala de Casación Penal, conforme a lo previsto 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.

Publíquese en la Gaceta Judicial de la República Bolivariana de Venezuela en cumplimiento de lo previsto en el artículo 126 de la Ley Orgánica del Tribunal Supremo de Justicia.

Dada, firmada y sellada en la Sala de Casación Penal del Tribunal Supremo de Justicia, a los doce (12) días del mes de diciembre de dos mil dieciséis (2016). Años: 206° de la Independencia y 157° de la Federación.

El Magistrado Presidente,
Maikel José Moreno Pérez

La Magistrada Vicepresidenta,
Francia Coello González

La Magistrada,
Elsa Janeth Gómez Moreno

El Magistrado,
Juan Luis Ibarra Verenzuela

La Magistrada,
Yanina Beatriz Karabin de Díaz

La Secretaria,
Ana Yakeline Concepción de García

JURISPRUDENCIA

Recopilación de sentencias del Tribunal Supremo de Justicia relacionadas con el uso y la valoración jurídica de las Tecnologías de la Información¹ durante 2016

Gustabo Adolfo Amoni Reverón*

Durante el año 2016 fue notable la producción de decisiones de las distintas salas del Tribunal Supremo de Justicia venezolano que consideraron el valor jurídico de los mensajes de datos, las firmas electrónicas, los portales de Internet², el uso de la videoconferencia en audiencias procesales, así como de otros medios probatorios y actos jurídicos relacionados con las Tecnologías de la Información.

A continuación presentamos la referencia de los fallos más importantes relacionados con estos aspectos:

1. Decisiones relacionadas con el valor de los mensajes de datos y firmas electrónicas

SSCC³ N° 126 del 2 de marzo de 2016. Valor de las facturas enviadas por correo electrónico.

Disponible en:

<http://historico.tsj.gob.ve/decisiones/scc/marzo/185720-RC.000126-2316-2016-14-693.HTML>

* Abogado *summa cum laude* de la Universidad Carabobo, especialista *Cum Laude* en Derecho Administrativo de la Universidad Católica Andrés Bello, abogado de la Sala de Casación Penal del Tribunal Supremo de Justicia desde 2005, profesor de pregrado de la Universidad Central de Venezuela y profesor de postgrado de la Universidad Católica «Andrés Bello»; dirección de correo electrónico: gustavoamoni@hotmail.com.

¹ El numeral 17 del artículo 5 de la Ley de Infogobierno, publicada en la Gaceta Oficial N° 40.274 del 17 de octubre de 2016, se refiere a las Tecnologías de la Información y las Comunicaciones (TIC) como Tecnologías de Información, por tanto, se usará tal denominación en la presente recopilación.

² Denominación usada en el artículo N° 18 de la Ley de Infogobierno, publicada en la Gaceta Oficial N° 40.274 del 17 de octubre de 2016.

³ Sentencia de la Sala de Casación Civil.

SSCS⁴ N° 809 del 8 de agosto de 2016. Valor de los mensajes de correo electrónico.

Disponible en:

<http://historico.tsj.gob.ve/decisiones/scs/agosto/189830-0809-8816-2016-15-491.HTML>

SSC⁵ N° 163 del 14 de marzo de 2016. Valor de la sentencia impresa a partir del sistema informático del Poder Judicial.

Disponible en:

<http://historico.tsj.gob.ve/decisiones/scon/marzo/186168-163-14316-2016-15-1371.HTML>

SSCC N° 369 del 15 de junio de 2016. Valor de los mensajes de correo electrónico.

Disponible en:

<http://historico.tsj.gob.ve/decisiones/scc/junio/188346-rc.000369-15616-2016-15-909.html>

SSCC N° 497 del 8 de agosto de 2016. Valor de la impresión de mensajes de correo electrónico.

Disponible en:

<http://historico.tsj.gob.ve/decisiones/scc/agosto/189841-rc.000497-8816-2016-16-081.html>

SSCS N° 986 del 18 de octubre 2016. Valor de la impresión de los mensajes de correo electrónico.

Disponible en:

<http://historico.tsj.gob.ve/decisiones/scs/octubre/191006-0986-181016-2016-15-1212.html>

SSCS N° 1125 del 7 de noviembre de 2016. Valor de la impresión de los mensajes de correo electrónico.

Disponible en:

<http://historico.tsj.gob.ve/decisiones/scs/noviembre/191994-1125-71116-2016-13-1229.html>

SSCP⁶ N° 446 del 11 de noviembre de 2016. Tipos de firmas electrónicas y valor de los mensajes de datos.

4 Sentencia de la Sala de Casación Social.

5 Sentencia de la Sala Constitucional.

6 Sentencia de la Sala de Casación Penal.

Disponible en:

<http://historico.tsj.gob.ve/decisiones/scp/noviembre/192949-446-111116-2016-e16-211.html>

SSC N° 1066 del 9 de diciembre de 2016. El uso de la firma electrónica en la convocatoria de accionistas

Disponible en:

<http://historico.tsj.gob.ve/decisiones/scon/diciembre/193697-1066-91216-2016-16-0826.html>

2. Decisión que considera los requisitos para notificar actos administrativos por medios telemáticos

SSPA⁷ N° 381 del 5 de abril de 2016. Contenido de la notificación telemática del acto administrativo.

Disponible en:

<http://historico.tsj.gob.ve/decisiones/spa/abril/186853-00381-5416-2016-2015-1186.HTML>

3. Decisiones que consideran el valor jurídico de los portales de Internet

SSCP N° 75 del 19 de febrero de 2016

Disponible en:

<http://historico.tsj.gob.ve/decisiones/scp/febrero/185355-075-19216-2016-e15-503.html>

SSCS N° 866 del 12 de agosto de 2016

Disponible en:

<http://historico.tsj.gob.ve/decisiones/scs/agosto/190251-0866-12816-2016-14-1332.html>

SSCS N° 929 del 4 de octubre de 2016

Disponible en:

<http://historico.tsj.gob.ve/decisiones/scs/octubre/190634-0929-41016-2016-15-870.html>

SSCS N° 999 del 18 de octubre de 2016

Disponible en:

<http://historico.tsj.gob.ve/decisiones/scs/octubre/190978-0999-181016-2016-15-1185.html>

⁷ Sentencia de la Sala Político Administrativa.

SSCS N° 1081 del 27 de octubre de 2016

Disponible en:

<http://historico.tsj.gob.ve/decisiones/scs/octubre/191561-1081-271016-2016-15-1363.html>

SSCS N° 1343 del 13 de diciembre de 2016

Disponible en:

<http://historico.tsj.gob.ve/decisiones/scs/diciembre/193858-1343-131216-2016-16-121.html>

4. Decisiones relacionadas con el uso de la videoconferencia en los procesos jurisdiccionales

SJSCS⁸ N° 123 del 12 de diciembre de 2016

Disponible en:

<http://historico.tsj.gob.ve/decisiones/jscs/febrero/185431-123-1216-2016-15-64.html>

SSCS N° 104 del 29 de febrero de 2016

Disponible en:

<http://historico.tsj.gob.ve/decisiones/scs/febrero/185609-0104-29216-2016-15-623.html>

ASCP⁹ N° 74 del 19 de febrero de 2016

Disponible en:

<http://historico.tsj.gob.ve/decisiones/scp/febrero/185354-074-19216-2016-e15-493.html>

5. Decisiones sobre experticias informáticas e inspecciones judiciales

SJSPA¹⁰ N° 236 del 3 de marzo de 2016. Inspección judicial en base de datos.

Disponible en:

<http://historico.tsj.gob.ve/decisiones/jspa/agosto/189767-236-3816-2016-2011-1190.html>

⁸ Sentencia interlocutoria del Juzgado de Sustanciación de la Sala de Casación Social.

⁹ Auto de la Sala de Casación Penal.

¹⁰ Sentencia interlocutoria del Juzgado de Sustanciación de la Sala Político Administrativa.

SSCC N° 550 del 11 de agosto de 2016. Experticia informática.
Disponible en:
<http://historico.tsj.gob.ve/decisiones/scc/agosto/190167-rc.000550-11816-2016-15-762.html>

SSCS N° 236 del 18 de marzo de 2016. Experticia informática.
Disponible en:
<http://historico.tsj.gob.ve/decisiones/scs/marzo/186462-0236-18316-2016-12-1149.html>

6. Extradición por delito informático

SSCP N° 183 del 9 de mayo de 2016
Disponible en:
<http://historico.tsj.gob.ve/decisiones/scp/mayo/187653-183-9516-2016-e16-90.html>



ÍNDICE ACUMULADO

ARTÍCULOS

CONFERENCIAS

CONTRIBUCIONES ESPECIALES

COMENTARIOS ESPECIALIZADOS

RESEÑA LEGISLATIVA

CRÓNICA JURÍDICA

SECCIÓN MONOGRÁFICA

LEGISLACIÓN

NACIONAL
INTERNACIONAL

JURISPRUDENCIA

COMENTARIOS
SENTENCIAS

RECENSIÓN

COMENTARIOS SOBRE BIBLIOGRAFÍA JURÍDICA
ESPECIALIZADA

ARTÍCULOS

AGUILAR TORRES, Jorge.

- El ejercicio de los derechos políticos de los accionistas a través de medios electrónicos en las sociedades anónimas no cotizadas en España. **10**, (2008-2009), 75-91.

ALBA FERNÁNDEZ, Manuel.

- El Convenio de Montreal para la Unificación de ciertas reglas para el Transporte Aéreo Internacional de 1999: el comienzo de una nueva etapa. **5**, (Julio/Diciembre 2004), 121-145

ALVÁREZ CABRERA, Carlos.

- Patentabilidad de las invenciones relacionadas con la computación. **3**, (Julio/Diciembre 2003), 37-50.

ÁLVAREZ CUESTA, Henar.

- El software libre y su posible repercusión en el ámbito universitario español. **6-7**, (Enero/Diciembre 2005), 171-181.

AMONI REVERÓN, Gustavo Adolfo.

- Regulación económica de Internet como elemento de gobierno electrónico en Venezuela. **9**, (Enero/Diciembre 2007), 117-131
- La democracia electrónica: buscando nuevos medios para la participación. **12**, (2011), 127-145
- Posibles soluciones a problemas de la audiencia de casación penal telemática. **16**, (2015), 117-141
- La audiencia telemática de extradición. Análisis del auto número 74/2016 de la Sala de Casación Penal del Tribunal Supremo de Justicia venezolano. **2** Ed. Digital / **17**, (2016), 49-79.

APARICIO VAQUERO, Juan Pablo.

- Derecho y tecnología de protección de las obras en formato

electrónico. **6-7**, (Enero/Diciembre 2005), 203-227.

ARIAS DE RINCÓN, María Inés.

- La perfección del contrato en el Decreto-Ley de Mensajes de Datos y Firmas Electrónicas. **2**, (Enero/Junio 2003), 131-150.
- La protección al consumidor en el comercio electrónico. **6-7**, (Enero/Diciembre 2005), 53-71.
- La alternativa de la conciliación por vía electrónica en los conflictos de consumo. **14**, (2013), 37-53

ARRIETA ZINGUER, Miguel.

- Régimen jurídico de la interconexión en las telecomunicaciones en Venezuela. **1**, (2002), 111-128.
- Los aportes en ciencia, tecnología e innovación en Venezuela. **9**, (Enero/Diciembre 2007), 89-116.
- Normativa respecto de las declaraciones de impuestos nacionales por Internet en Venezuela. **11**, (2010), 97-105.
- Comercio electrónico y redes sociales: nuevo paradigma negocial. **16**, (2015), 177-191

BARZALLO, José Luis.

- Derechos de autor y tecnología. **3**, (Julio/Diciembre 2003), 7-36.

BERROCAL LANZAROT, Ana Isabel .

- La defensa de los derechos al honor, intimidad personal y familiar y a la propia imagen de los menores de edad en Internet. **14**, (2013), 55-98

BUITRAGO RODRÍGUEZ, Mariana

- La convocatoria electrónica como vía de notificación alternativa a las asambleas de accionistas en el

- Derecho venezolano. **10**, (2008-2009), 93-109
- La electrificación en las sesiones del sistema de mercado bursátil en el Derecho venezolano. **13**, (2012), 87-105
 - Domicilio fiscal electrónico obligatorio para la notificación de comunicaciones o actos administrativos emanadas de la Administración Tributaria venezolana. **2** Ed. Digital / **17**, (2016), 153-170.
- CÁRDENAS, Gilberto.
- Análisis jurisprudencial del artículo 90 del Tratado de la Unión Europea como fundamento jurídico para la liberalización del mercado de las telecomunicaciones. **1**, (2002), 93-110.
- CONTRERAS ZAMBRANO, Josué.
- Manuel. Valoración probatoria del documento electrónico y firma electrónica en el proceso judicial venezolano. **13**, (2012), 27-46
- CREMADES, Javier y SANMARTIN, Javier.
- España: La nueva Ley General de Telecomunicaciones. **5**, (Julio/Diciembre 2004), 7-16.
- CUADRADO GAMARRA, Nuria.
- Los Códigos tipo en la legislación española. **6-7**, (Enero/Diciembre 2005), 73-90.
- CHACÓN GÓMEZ, Nayibe.
- La perspectiva electrónica de los títulos valores: desmaterialización del título valor. **10**, (2008-2009), 133-155.
 - La transferencia tecnológica: ¿Desarrollo de una política pública en Venezuela?. **16**, (2015), 105-116
- CHIQUITO, Andreina.
- El cheque electrónico en la legislación venezolana. **9**, (Enero/Diciembre 2007), 69-88.
- DE LA VEGA JUSTRIBÓ, Bárbara.
- Las nuevas tecnologías en la publicidad del concurso de acreedores. **11**, (2010), 107-130.
 - La mediación por medios electrónicos en la Ley española de mediación de asuntos civiles y mercantiles. **13**, (2012), 133-157
- DELPIAZZO, Carlos E.
- La Informática Jurídica y el Derecho de la Integración del Mercosur. **8**, (Enero/Diciembre 2006), 95-111.
 - Aspectos de la contratación pública electrónica. **11**, (2010), 11-31
- FERNÁNDEZ CABRERA, Sacha Rohán
- Privacidad de los correos electrónicos en el trabajo. **2** Ed. Digital / **17**, (2016), 9-48.
- FERNÁNDEZ DELPECH, Horacio.
- Nueva Directiva de la Unión Europea sobre Conservación de Datos de Tráfico. **8**, (Enero/Diciembre 2006), 11-25.
 - La *Cloud Computing*. Una visión Argentina. **16**, (2015), 47-64.
- GALINDO, Fernando.
- Democracia electrónica, Internet y gobernanza. **12**, (2011), 109-125
- GARCÍA CACHAFEIRO, Fernando y GARCÍA PÉREZ, Rafael.
- La tensión entre las restricciones a la libre prestación de servicios de la Sociedad de la Información y los derechos fundamentales y libertades públicas. **3**, (Julio/Diciembre 2003), 151-165.
- GARCÍA MANDALONIZ, Marta y RODRÍGUEZ DE LAS HERAS BALLELL, Teresa.
- "La inquebrantabilidad del principio de la unicidad en la junta general electrónica". **8**, (Enero/Diciembre 2006), 27-47.

- GARRO, Alejandro M., PERALES VISCASILLAS, Pilar y PÉREZ PEREIRA, María.
- Comunicaciones Electrónicas en la Convención de Viena de 1980 sobre compraventa internacional de mercaderías (CISG): primera opinión del Consejo Consultivo de la Convención (CISG-AC), **5**, (Julio/Diciembre 2004), 17-40
- GÓMEZ CORDOBA, Ana Isabel y Nelson REMOLINAANGARITA.
- Los sistemas de identificación biométrica y la información biométrica desde la perspectiva de la protección de datos personales. **12**, (2011), 69-108
- GRAHAM., James A.
- *La Uniform Dispute Resolution Policy*: Una tentativa de calificación. **2**, (Enero/Junio 2003), 151-159.
- GUISADO MORENO, Ángela.
- La unificación del Derecho contractual europeo en la Era de la Información: movimientos e instrumentos unificadores. **9**, (Enero/Diciembre 2007), 133-158.
- HERNÁNDEZ, Juan Carlos.
- La protección de datos personales en internet y los derechos fundamentales: El Habeas Data. **13**, (2012), 61-85
- HERRERABRAVO, Rodolfo.
- Los registros de ADN y los derechos fundamentales: ¿Cómo esquivar sin despellejar? **2**, (Enero/Junio 2003), 21-41.
- ILLESCAS ORTIZ, Rafael.
- La equivalencia funcional como principio elemental del Derecho del comercio electrónico. **1**, (2002), 9-23.
 - La Ley 22/2007 sobre Comercialización a Distancia de Servicios Financieros destinados a los Consumidores y la dogmática contractual electrónica. **9**, (Enero/Diciembre 2007), 11-26.
- INOSTROZA SÁEZ, Mauricio
- El convenio arbitral electrónico en la Ley de arbitraje española y los textos de Derecho uniforme. **12**, (2011), 53-67
- IRIARTE AHON, Erick.
- Sobre nombres de dominio: una propuesta para el debate. Análisis de la Radicación 1376 del Consejo de Estado colombiano. **2**, (Enero/Junio 2003), 103-129.
- JELEZTCHEVA, María y RODRÍGUEZ GRILLO, Luisa
- Los contratos electrónicos. **11**, (2010), 159-188.
- LAGUNA, Rosa.
- ¿Nueva pedagogía para el *e-learning*? **3**, (Julio/Diciembre 2003), 127-150.
- LASTIRI SANTIAGO, Mónica.
- Autorregulación publicitaria. **1**, (2002), 157-182.
 - El uso de la marca en Second Life. **10**, (2008-2009), 7-43
- LEÓN PARADA, Alejandra de los A.
- Valor probatorio de los mensajes de datos y firmas electrónicas en la Sala Civil del Tribunal Supremo de Justicia venezolano. **2** Ed. Digital / **17**, (2016), 81-95.
- LÓPEZ JIMÉNEZ, David
- La autorregulación de la publicidad relativa a apuestas y juegos virtuales: una aproximación desde la perspectiva española. **12**, (2011), 147-185
 - Los deberes precontractuales de información en el ámbito de las transacciones virtuales: a propósito del principio de la buena fe. **13**, (2012), 107-131

- LÓPEZ JIMÉNEZ, David y BARRIO, Fernando.
- Los códigos de conducta reguladores del comercio electrónico en el espacio europeo. Los casos de Alemania, España e Italia. **11**, (2010), 33-68.
- LÓPEZ ZAMORA, Paula.
- Nuevas perspectivas del derecho a la información en la Sociedad de la Información. **6-7**, (Enero/Diciembre 2005), 11-25.
- MACHTA CHENDI, Zulay.
- El servicio público en el sector eléctrico venezolano y Derecho de las Telecomunicaciones. **5**, (Julio/Diciembre 2004), 41-80
- MADRID MARTÍNEZ, Claudia
- La internacionalización del consumo: el consumidor electrónico y la realidad venezolana. **12**, (2011), 7-51
- MARESCA, Fernando.
- Protección jurídica del software: un debate abierto. **1**, (2002), 147-156.
- MARTÍNEZ NADAL, Apollònia.
- Derechos de sociedades y Nuevas Tecnologías: aplicaciones presentes y futuras en el Derecho español. **10**, (2008-2009), 45-74
 - Las polémicas cláusulas de paridad en la contratación turística electrónica: ¿Prohibición absoluta o aceptación de cláusulas de paridad relativa?. **16**, (2015), 65-80
- MARTÍNEZ NADAL, Apollònia y FERRER GOMILÀ, Josep Luis.
- Delimitación de responsabilidades en caso de revocación de un certificado de firma electrónica: soluciones legales de Derecho europeo. **1**, (2002), 53-71.
- MATA, Miguel Ángel.
- La protección al consumidor en la contratación a distancia. **8**, (Enero/Diciembre 2006), 73-94.
- MATTUTAT MUÑOZ, Marjorie.
- La electrificación del procedimiento constitutivo de las sociedades mercantiles en Venezuela. **10**, (2008-2009), 111-131
- MONSALVE GONZÁLEZ, Karlith.
- Valor jurídico de la firma electrónica en el sistema legal venezolano. **10**, (2008-2009), 157-177
- MUNIVE CORTÉS, Erika Yamel.
- 2000 - 2015: 15 aniversario del Sistema Nacional e-México. **16**, (2015), 143-175
- NAHABETIÁN BRUNET, Laura.
- Responsabilidad civil en el marco del Gobierno de la Información. **16**, (2015), 9-46
- OLIVER LALANA, A. Daniel.
- Estrategias de protección de datos en el comercio electrónico. **3**, (Julio/Diciembre 2003), 51-71.
 - Internet como fuente de información accesible al público: pensando el derecho de protección de datos en su contexto social y jurídico. **8**, (Enero/Diciembre 2006), 49-72.
- PANIZA FULLANA, Antonia.
- Análisis jurídico de los *spyware*, *web bugs* y *mail bugs*. (*Su problemática utilización en la protección de los derechos de autor*). **6-7**, (Enero/Diciembre 2005), 91-113.
 - E-consumidores: aspectos problemáticos en la normativa española. **9**, (Enero/Diciembre 2007), 51-68
- PAZ CALZADILLA, Belinda
- El uso de las nuevas tecnologías en el procedimiento contencioso administrativo en Venezuela. **2** Ed. Digital / **17**, (2016), 125-152.

- PERALES VISCASILLAS, M^a del Pilar.
- Sobre la perfección del contrato en España: el “popurrí” de los “nuevos” artículos 1262 del Código Civil y 54 del Código de Comercio. **2**, (Enero/Junio 2003), 7-19.
 - ¿Forma *escrita* del convenio arbitral?: Nuevas disposiciones de la CNUDMI/UNCITRAL. **9**, (Enero/Diciembre 2007), 27-49
- PÉREZ LUÑO, Antonio Enrique.
- Reflexiones sobre la contratación informática. **4**, (Enero/Junio 2004), 11-21
- PÉREZ PEREIRA, María.
- Proveedores de servicios de certificación: aspectos venezolanos y europeos. **1**, (2002), 33-51.
- PLAZA SOLER, Juan Carlos.
- Los correos electrónicos comerciales no solicitados en el Derecho español, europeo y estadounidense. **3**, (Julio/Diciembre 2003), 73-98.
- PONCE HEINSOHN, Ivonne
- Intervención notarial en la contratación electrónica: Especial referencia a la incorporación del documento público electrónico en el ordenamiento jurídico español y chileno. **11**, (2010), 131-157.
- QUIRÓS HIDALGO, José Gustavo.
- “El régimen de propiedad intelectual del profesorado universitario en España y su relación con los sistemas Open Access”. **6-7**, (Enero/Diciembre) 2005, 183-202.
- RAMÍREZ COLINA, Sulmer Paola.
- El teletrabajo y su sujeción a la Ley Orgánica del Trabajo. **2**, (Enero/Junio 2003), 61-80
 - El contrato electrónico laboral. **16**, (2015), 81-104
- REUSSER MONSÁLVEZ, Carlos.
- Las Bases de Datos de Perfiles de ADN y su (des) Protección en Europa. **5**, (Julio/Diciembre 2004), 147-157
- RICO CARRILLO, Mariliana.
- Firmas electrónicas y criptografía. **2**, (Enero/Junio 2003), 81-101.
- RÍOS M., Desirée J.
- Visión social de la prueba. Especial referencia a los medios electrónicos. **2** Ed. Digital / **17**, (2016), 97-123.
- RODRÍGUEZ DE LAS HERAS BALLELL, Teresa
- La responsabilidad de los prestadores de servicios de intermediación y los estratos de la intermediación en la Red. **11**, (2010), 69-96
- RODRÍGUEZ, Gladys Stella.
- Principios jurídicos del contrato electrónico en el marco del comercio B2B: especial referencia a las PYMEs de los países en el desarrollo. **14**, (2013), 11-36.
- SALGADO SEGUÍN, Víctor Alberto.
- La Directiva europea sobre comercio electrónico. **1**, (2002), 73-91.
- SALGUEIRO A., José Ovidio.
- La Ley sobre Mensajes de Datos y Firmas Electrónicas de Venezuela. **1**, (2002), 25-32.
- SÁNCHEZ RODRÍGUEZ, Antonio Jesús.
- Monopolio y competencia en el Derecho comunitario europeo de las telecomunicaciones. **1**, (2002), 129-146.
- SANTANDER RENGIFO, Antonio.
- Una nueva vieja propuesta: la oferta al público por internet bajo la lupa de la Doctrina del Derecho Civil. **5**, (Julio/Diciembre 2004), 81-120.

SARMIENTO, María Gabriela.

- Anteproyecto de Convención sobre la Contratación Electrónica llevado a cabo por el Grupo de Trabajo IV sobre Comercio Electrónico de la CNUDMI. **3**, (Julio/Diciembre 2003), 99-125.

SEMENT VIDAL, María José.

- La protección jurídica del denominado “conocimiento libre”. **6-7**, (Enero/Diciembre 2005), 141-170.

SOTO, Alberto.

- Derecho penal y delitos informáticos: Seguridad de la información, seguridad legal y seguridad jurídica. Una visión en Argentina. **3**, (Julio/Diciembre 2003), 167-178.

USECHE CASTRO, Yasmin Carolina.

- El dilema entre el derecho a la intimidad y el secreto a las comunicaciones del trabajador y el poder de vigilancia y control del patrono. **13**, (2012), 47-59

VALERO TORRIJOS, Julián.

- El acceso telemático a la información administrativa: un presupuesto inexcusable para la e-Administración (Análisis desde la perspectiva del Derecho español). **6-7**, (Enero-Diciembre 2005), 27-51.

VARGAS LEAL, Luis.

- Regulación de las telecomunicaciones en un ámbito de convergencia tecnológica. **4**, (Enero/Julio 2004), 23-62.

VÁSQUEZ SÁNCHEZ, María Alejandra.

- La influencia de las nuevas tecnologías en el derecho probatorio venezolano: Los desafíos de la administración de justicia del siglo XXI. **13**, (2012), 9-25

VÁZQUEZ, Víctor.

- La propuesta de Tratado de la OMPI sobre protección de las interpretaciones y ejecuciones audiovisuales. **6-7**, (Enero/Diciembre 2005), 229-245.

WACHOWICZ, Marcos y REZENDE, Denis Alcides.

- La Tecnología de la Información y sus impactos en la propiedad intelectual. **2**, (Enero/Junio 2003), 43-59.

YAYA NARVÁEZ, León David y CANO M., Jeimy J.

- Consideraciones legales y comerciales sobre VoIP en Colombia. **6-7**, (Enero-Diciembre 2005), 115-140.

CONFERENCIAS

ÁLVAREZ CABRERA, Carlos S.

- Propiedad intelectual y nuevas tecnologías. **4**, (Enero/Julio 2004), 93
- La ley y la seguridad de la información: una perspectiva regional. **8**, (Enero/Diciembre 2006), 261-272.

AMONI REVERÓN, Gustavo Adolfo.

- El testamento electrónico. **4**, (Enero/Julio 2004), 193.

ANTEQUERA, Ricardo Enrique.

- La propiedad intelectual: una herramienta de competitividad para las PYME. **8**, (Enero/Diciembre 2006), 197-208.

ARAUJO - JUÁREZ, José.

- El nuevo “modelo de regulación” de las telecomunicaciones en Venezuela. **4**, (Enero/Julio 2004), 65-91.

- ARIAS DE RINCÓN, María Inés.
- El derecho de retractarse de los consumidores y usuarios electrónicos. **8**, (Enero/Diciembre 2006), 247-259.
- ARRIETA ZINGÜER, Miguel.
- Tributación e Internet. **4**, (Enero/Julio 2004), 145
- BARZALLO, José Luis.
- Derecho de autor, Internet y libre competencia. **8**, (Enero/Diciembre 2006), 221-245.
- BAUZÁ, Marcelo.
- Datos abiertos, ¿derecho humano?, ¿política pública? o ambas cosas. **16**, (2015), 237-252
- BRANDT GRATEROL, Leopoldo.
- Páginas Web: modalidades de aplicación en el comercio electrónico. **4**, (Enero/Julio 2004), 165
- BUENO DE MATA, Federico
- Diligencias de investigación tecnológicas para la obtención y aportación de mensajes de WhatsApp, Snapchat o Telegram. **2 Ed. Digital / 17**, (2016), 201-213
- COTINO HUESO, Lorenzo.
- Protección de datos y servicios públicos y privados de *Cloud Computing* en España y Europa. **16**, (2015), 195-216
- DÍAZ GARCÍA, Alexander.
- Desnaturalización del documento electrónico judicial con la apelación de la sentencia. El nuevo sistema penal acusatorio (El juicio oral) colombiano. **8**, (Enero/Diciembre 2006), 275-301.
- ESPINOSA VERA, Jefferson Stewart
- Derechos humanos en la protección ética de los menores en las redes sociales. Caso Colombia y Perú. **2 Ed. Digital / 17**, (2016), 173-186.
- GARCIA PEÑA, José Heriberto
- Nanotecnología y Derecho: una aproximación al tema desde México. **2 Ed. Digital / 17**, (2016), 215-227
- GUERRERO CARRERA, Jacqueline.
- Democracia deliberativa y participación ciudadana electrónica. **16**, (2015), 217-223
- GUERRERO LEBRÓN, María Jesús.
- Trámites de constitución de la Sociedad Limitada Nueva Empresa. **8**, (Enero/Diciembre 2006), 161-175.
- ILLESCAS ORTÍZ, Rafael.
- La continuada –y, a veces, desaparecida– electrificación del Derecho de sociedades mercantiles. **8**, (Enero/Diciembre 2006), 117-159.
- MENDOZA ENRÍQUEZ, Olivia Andrea.
- Plataformas ciudadanas de participación como herramientas del ejercicio de la libertad de expresión en Internet. **16**, (2015), 225-235
- NOVAS, Natalia Soledad; NOVAS, Jorge Alberto; RUANI, Humberto Félix; RUANI, Humberto Martín.
- Historia clínica electrónica. **16**, (2015), 253-262
- ORTA MARTÍNEZ, Raymond J.
- Importancia de la descripción de software y hardware en las pericias informáticas y otros actos judiciales. **4**, (Enero/Julio 2004), 187
- PÉREZ PEREIRA, María.
- España y las nuevas tecnologías: aspectos jurídicos. **4**, (Enero/Julio 2004), 177
 - La evolución de los sistemas de cifrado. **8**, (Enero/Diciembre 2006), 189-193.
- RAMOS HERRANZ, Isabel.
- Presentación VII Jornada de Derecho del Comercio Electrónico. **8**, (Enero/Diciembre 2006), 115-116.

REMOLINAANGARITA, Nelson.

- Data protection: aproximación global con énfasis en el caso colombiano. **4**, (Enero/Julio 2004), 109

REYES OLMEDO, Patricia

- Regulación de la protección de datos personales en Chile a la luz de los estándares internacionales. Deficiencias y Desafíos. **2** Ed. Digital / **17**, (2016), 187-200

RICO CARRILLO, Mariliana.

- El uso de medios electrónicos en la convocatoria a la Junta General de Accionistas. **8**, (Enero/Diciembre 2006), 177-188.

SÁNCHEZ, Diego.

- Las nuevas tecnologías, el acceso a la información y la participación ciudadana. **8**, (Enero/Diciembre 2006), 209-219.

CONTRIBUCIONES ESPECIALES

CUBEROS DE QUINTERO, María Antonia

- La participación ciudadana y el gobierno electrónico. **9**, (Enero/Diciembre 2007), 161-172.

CANO, Jeimy J.

- Informáticos forenses: los criminalistas informáticos en la sociedad de la información. **9**, (Enero/Diciembre 2007), 173-182.

- ¿Compartir o proteger? Tensiones en la gerencia de la seguridad de la información. **13**, (2012), 161-169

MARTÍNEZ NADAL, Apolonia, HERRERA-JOANCOMARTÍ, Jordi y PÉREZ-SOLÁ, Cristina

- Análisis técnico-jurídico del proceso de Iniciativa Legislativa Popular con recogida de firmas digitales en España, **11** (2010), 191-216.

COMENTARIOS ESPECIALIZADOS

RÍOS RUIZ, Wilson Rafael

- Análisis del Acuerdo Inicial y sus enmiendas planteadas por Google a los autores. Su situación actual. **11**, (2010), 219-244.

MUNIVE CORTÉS, Erika Yamel

- Voto electrónico y protección de datos personales: los avances de la democracia universitaria en el País Vasco. **12**, (2011), 189-208

RESEÑA LEGISLATIVA

ARRIETA ZINGUER, Miguel.

- Comentario al Proyecto de Ley de Responsabilidad Social en Radio y Televisión. **2**, (Enero/Junio 2003), 283-309.

AMONI REVERÓN, Gustavo Adolfo.

- Comentarios a las disposiciones generales del Decreto Ley de Interoperabilidad Electrónica. **13**, (2012), 173-187

CRÓNICA JURÍDICA

ORTA MARTÍNEZ, Raymond J.

- La Informática forense como medio de prueba. **3**, (Julio/Diciembre 2003), 255-260

ALTAMIRA, Matías.

- Mesa virtual de entrada judicial: derechos y responsabilidades. **8**, (Enero/Diciembre 2006), 329-336.

SÁNCHEZ RODRÍGUEZ, Antonio Jesús

- El servicio de telecomunicaciones a través de las redes eléctricas: *Power Line Communications* (PLC). **3**, (Julio/Diciembre 2003), 261-268.

BUENO DE MATA, Federico.

- Presente y futuro de los dispositivos telemáticos de localización de presos utilizados en España. **12**, (2011), 211-220

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

consecuencias jurídico laborales. **14**, (2013), 187-205

CHACÓN GÓMEZ, Nayibe.

- La responsabilidad de los proveedores de servicio en las redes sociales. **14**, (2013), 207-230

RICO CARRILLO, Mariliana y LÓPEZ JIMÉNEZ, David.

- Las redes sociales en Internet: consideraciones generales y problemática jurídica. **14**, (2013), 101-112

LÓPEZ JIMÉNEZ, David.

- Las redes sociales como espacios publicitarios: el papel de la autorregulación. **14**, (2013), 165-186

RICO CARRILLO, Mariliana.

- El ejercicio de los derechos fundamentales y las libertades públicas a través de *Facebook*. **14**, (2013), 113-134

RAMÍREZ, Sulmer Paola.

- Los contenidos publicados por el trabajador en *Facebook* y sus

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 N° 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 N° 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 N° 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 Servicio Universal de Telecomunicaciones. **4**, (Enero/Julio 2004), 301-322.

Decreto N° 3.335, de fecha 12 de diciembre de 2004, mediante el cual se decreta el Reglamento Parcial del Decreto Ley sobre Mensajes de Datos y Firmas Electrónicas. **6-7**, (Enero/Diciembre 2005), 331-344.

Decreto N° 3.390, de fecha 23 de diciembre de 2004, sobre el uso del software libre en la Administración Pública. **6-7**, (Enero/Diciembre 2005), 345-349.

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. **13**, (2012), 191-215

Leyes

Ley especial contra los Delitos Informáticos. **1**, (2002), 275-285.

Ley Orgánica de Telecomunicaciones. **1**, (2002), 189-253.

Ley de Responsabilidad Social en Radio y Televisión. **6-7**, (Enero/Diciembre 2005), 249-298.

Ley Orgánica de Ciencia, Tecnología e Innovación. **6-7**, (Enero/Diciembre 2005), 299-329.

Ley para la protección de niños, niñas y adolescentes en salas de uso de internet, video juegos y otros multimedia. **8**, (Enero/Diciembre 2006), 305-314.

Ley de Tarjetas de Crédito, Débito, Prepagadas y demás Tarjetas de Financiamiento o Pago Electrónico, **10**, (2008-2009), 181-202

Ley Orgánica de Ciencia, Tecnología e Innovación. **12**, (2011), 223-246

Reglamentos

Reglamento sobre facturación y recaudación a solicitud y por cuenta de los operadores de los servicios de telefonía de larga distancia nacional y larga distancia internacional de fecha 8 de noviembre de 2004. **8**, (Enero/Diciembre 2006), 315-326.

Reglamento Parcial de la Ley Orgánica de Ciencia, Tecnología e Innovación referido a los Aportes e Inversión de fecha 9 de octubre de 2006. **9**, (Enero/Diciembre 2007), 207-220.

Resoluciones

Resolución contentiva de los atributos de las Habilitaciones Administrativas publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 37.215 de 8 de junio de 2001. **2**, (Enero/Junio 2003), 247-254.

Resolución N° 400 de fecha 20 de febrero de 2004, Normas para el Registro de contribuyentes de los tributos de telecomunicaciones. **5**, (Julio/Diciembre 2004), 253-255.

Resolución N° 401 de fecha 20 de febrero de 2004, Requisitos para declarar y pagar los tributos de telecomunicaciones. **5**, (Julio/Diciembre 2004), 257-261.

Resolución N° 408 de fecha 9 de marzo de 2004, Condiciones bajo las cuales los operadores de los servicios móviles de telecomunicaciones podrán ofrecer itinerancia o roaming a sus abonados. **5**, (Julio/Diciembre 2004), 263-266.

Resolución por la cual se dictan “Normas que Regulan los Procesos Administrativos relacionados a la Emisión y Uso de las Tarjetas de Crédito, Débito, Prepagadas y demás Tarjetas de Financiamiento o Pago Electrónico”, **10**, (2008-2009), 203-226.

Resolución por la cual se dictan “Normas relativas a la Protección de Usuarios y Usuaris de los servicios Financieros”. **12**, (2011), 247-265

Resolución N° 2016-001 de fecha 12 de diciembre de 2016, sobre Participación Telemática de los sujetos procesales en las Audiencias de la Sala de Casación Penal. **2** Ed. Digital / **17**, (2016), 231-245

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 22/2007, de 11 de julio, sobre Comercialización a Distancia 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 Audiovisual. **12**, (2011), 313-393

Real Decreto 322/2008 de 29 de febrero sobre el régimen jurídico de las entidades de dinero electrónico, **10**, (2008-2009), 303-322.

Real Decreto 899/2009 de 22 de mayo, se aprueba la carta de derechos del usuario de los servicios de comunicaciones electrónicas. **11**, (2010), 305-340.

Ley 5/2012, de 6 de julio, de Mediación en Asuntos Cíviles y Mercantiles. **13**, (2012), 217-244

Unión Europea

Reglamento (UE) N° 524/2013 del Parlamento Europeo y del Consejo de 21 de mayo 2013 sobre resolución de litigios en línea en materia de consumo y por el que se modifica el Reglamento (CE) n° 2006/2004 y la Directiva 2009/22/CE. **16**, (2015), 265-289

JURISPRUDENCIA

AMONI REVERÓN, Gustavo Adolfo.

- La citación electrónica. Comentarios al auto N° 339 dictado por el Juscago de Sustanciación de la Sala Político Administrativa del Tribunal Supremo de Justicia, el 7

de agosto de 2012. **14**, (2013), 233-245

- Recopilación de sentencias del Tribunal Supremo de Justicia relacionadas con el uso y la valoración jurídica de las Tecnologías de la

Información durante el 2016. **2** Ed. Digital / **17**, (2016), 249-253

ARRIETA ZINGÜER, Miguel.

- La gravabilidad de las actividades de telecomunicaciones y la potestad tributaria municipal. Comentario a la sentencia de 03 de agosto de 2004 del Tribunal Supremo de Justicia venezolano. **5**, (Julio/Diciembre 2004), 269-275.
- Procedencia de la suspensión de los efectos del acto recurrido en materia sancionatoria de telecomunicaciones. Comentario a la sentencia de 09 de noviembre de 2005 del Tribunal Supremo de Justicia. **6-7**, (Enero/Diciembre 2005), 357-364.
- Consideraciones acerca de las redes sociales en Internet como elemento de convicción en la radicación de juicios penales en decisiones del Tribunal Supremo de Justicia. **14**, (2013), 295-304

FERRER CASTRO, Mileidi Paola y Jenny QUINTERO MENDOZA, Carolina.

- Consideraciones sobre el reciente criterio del Tribunal Supremo de Justicia venezolano respecto al tratamiento de los correos electrónicos impresos como medios de prueba. **13**, (2012), 247-252

LASTIRI SANTIAGO, Mónica.

- El contrato de licencia y los nombres de dominio. Comentario a la Sentencia del Tribunal de Justicia de la Unión Europea (Sala Segunda), de 19 de julio de 2012 asunto C-376/11, *Pie Optiek SPRL & Bureau Gevers SA, European Registry for Internet Domains ASBL*. **14**, (2013), 249-252

PALAZZI, Pablo A.

- Google y el derecho a la privacidad sobre las búsquedas realizadas en

Internet. **8**, (Enero/Diciembre 2006), 339-349.

RAMÍREZ, Sulmer Paola.

- Valor jurídico probatorio del correo electrónico promovido en formato impreso. Comentarios a la sentencia de la Sala de Casación Civil del Tribunal Supremo de Justicia el 30 de mayo de 2013. **14**, (2013), 265-269

RICO CARRILLO, Mariliana.

- Interposición del recurso de amparo a través de medios electrónicos. Sentencias y comentarios jurisprudenciales. **1**, (2002), 289-319.
- La notificación por medios electrónicos. Comentario a la sentencia de 01 de febrero de 2000 del 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
- La posición del Tribunal Supremo de Justicia venezolano respecto a las pruebas documentales electrónicas. **16**, (2015), 293-299

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 de los medios electrónicos. **9**, (Enero/Diciembre 2007), 261-317.

Sentencia de la Sala de Casación Social del Tribunal Supremo de Justicia venezolano de 5 de marzo de 2007. **10**, (2008-2009), 331-354.

Sentencia de la Sala Político Administrativa del Tribunal Supremo de Justicia venezolano de 12 de febrero de 2008. **10**, (2008-2009), 355-400.

Sentencia de la Sala Político Administrativa del Tribunal Supremo de Justicia venezolano de 12 de agosto de 2009. **11**, (2010), 359-373

Sentencia de la Sala de Casación Social del Tribunal Supremo de Justicia venezolano de 2 de julio de 2010. **12**, (2011), 401-407

Sentencia de la Sala de Casación Civil del Tribunal Supremo de Justicia venezolano de 5 de octubre de 2011. **13**, (2012), 253-277

Sentencia de la Sala Político Administrativa. Juzgado de Sustanciación del Tribunal Supremo de Justicia

- de 7 de agosto de 2012. **14**, (2013), 247-248
- Sentencia del Tribunal de Justicia de la Unión Europea (Sala Segunda), 19 de julio de 2012. **14**, (2013), 253-264
- Sentencia de la Sala de Casación Civil del Tribunal Supremo de Justicia de 30 de mayo de 2013. **14**, (2013), 271-293
- Sentencia de la Sala de Casación Penal del Tribunal Supremo de Justicia de 13 de abril de 2013. **14**, (2013), 305-312
- Sentencia de la Sala de Casación Penal del Tribunal Supremo de Justicia de 12 de abril de 2012. **14**, (2013), 313-324
- Sentencia de la Sala de Casación Penal del Tribunal Supremo de Justicia de 28 de abril de 2011. **14**, (2013), 325-332

RECENSIÓN

PÉREZ PEREIRA, María.

- BARRAL VIÑALS, Immaculada (Coord.) *La regulación del comercio electrónico*. Edt. Dykinson, Madrid 2003, 207 págs. **3**, (julio/Diciembre 2003), 281-282.
- BRANDT GRATEROL, Leopoldo. *Páginas web: condiciones, políticas y términos legales*. Editorial Legis, Caracas, 2001, 358 págs. **3**, (Julio/Diciembre 2003), 283-284.
- RAMOS HERRANZ, Isabel: *Marcas versus nombres de dominio en Internet*, Iustel, Madrid, 2004, págs. 351. **5**, (Julio/Diciembre 2004), 309-310.
- RICO CARRILLO, Mariliana: *Comercio electrónico, Internet y Derecho*. Edt. Legis, Caracas, 2003, 277 págs. **3**, (Julio/Diciembre 2003), 285.

RANGEL GÓMEZ, Horacio.

- LASTIRI SANTIAGO, Mónica. *La comercialización del nombre de dominio*. Los bienes jurídicos digitales, el derecho de control y los nombres de dominio. Ed. Mar-

cial Pons, España (2014), **16**, (2015), 303-309

RICO CARRILLO, Mariliana.

- BRICEÑO, Francisco (Coord.): *Aspectos legales del comercio electrónico*, Cavecom, Caracas, 2004, 294 págs. **4**, (Enero/Julio 2004), 341-245.
- BATUECAS CALETIRIO, Alfredo: *Pago con tarjeta de crédito: Naturaleza y régimen jurídico*, Revista Aranzadi de Derecho Patrimonial N° 15 (monográfico), Thomson-Aranzadi, Navarra, 2005, 429 págs. **6-7**, (Enero/Diciembre 2005), 377-378.
- MARTÍNEZ NADAL, Apol.lonia. *El pago capitativo en la prestación de servicios médicos*. Civitas Thomson Reuters Aranzadi, España 2015. **16**, (2015), 311-314
- KOZOLCHYK, Boris, Ph. D. *Comparative Commercial Contracts: Law, Culture and Economic Development*. West Academic Publishing, United States of America, 2014 . **16**, (2015), 315-319

ALBA FERNÁNDEZ, Manuel.

- 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.

- 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 Windows™ 3.0 o superiores. Los gráficos o imágenes que contenga el artículo deben estar especificados con los formatos o extensiones en que se hicieron (Excel™, Corel Draw™, 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. Al 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 la 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 información¹.

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 Tachirens 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 WindowsTM 3.0 or higher. The graphics or images that present the article must be specified with the formats or extensions where they were made (ExcelTM, Corel DrawTM, 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 they 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 information¹.

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 Tachirenses 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**

2/2016 Edición Digital

17/2016 Edic Ordinaria

Revista de Derecho y Tecnología, Enero / Diciembre 2016,
de la Universidad Católica del Táchira.
San Cristóbal - Venezuela



Universidad Católica del Táchira
San Cristóbal - Venezuela
RIF: J- 09011253-7