DERECHO Y TECNOLOGÍA

UNIVERSIDAD CATOLICA DEL TACHIRA

2019

Vicerrectorado Académico
Decanato de Investigación y Postgrado

Número 5/2019 Edición Digital
Depósito Legal en línea: ppi201602TA4734
ISSN en Línea: (en trámite)

Edición Ordinaria 20/2019
Enero - Diciembre 2019
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

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 5/2019 Edición Digital - Edición Ordinaria 20/2019

La edición impresa de la Revista Derecho y Tecnología llega hasta la N° 15 año 2014, por falta de papel. La edición correspondiente al 2019 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° 5, para efectos de la continuidad de la edición ordinaria es la N° 20.

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

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

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

Derecho y Tecnología

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

Misión

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

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

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

Universidad Católica del Táchira

Revista Derecho y Tecnología **5/2019** Edición Digital
Vicerrectorado Académico **20/2019** Edición Ordinaria
Decanato de Investigación y Postgrado

ÍNDICE

Doctrina

Jurisprudencia

DOCTRINA

El derecho a la protección de datos de las sentencias

Sacha Rohán Fernández Cabrera*

SUMARIO: Introducción. I. Algunos derechos humanos involucrados. 1. Dignidad de la persona humana. 2. Libre desarrollo de la personalidad. 3. Derecho a la intimidad, a la vida privada y a la propia imagen. 4. Derecho a la integridad psicofísica y moral. 5. Derecho al honor y a la reputación. 6. Acceso universal a Internet como derecho humano. 7. Libertades de expresión e información en Internet. II. Mecanismos procesales de protección de los derechos humanos ante la publicación digital de la sentencia. 1. *Habeas Data*. 2. Demanda por intereses colectivos y difusos. 3. El Derecho al olvido. III. Derechos y obligaciones que surgen de las partes, los terceros y el Estado ante la publicación del fallo por internet. IV. Medidas de seguridad informáticas. V. Blockchain. Conclusiones.

Resumen

El objetivo perseguido por el presente trabajo es el de dar a conocer de manera general la problemática jurídica que suscita el encuentro de la Informática y las Telecomunicaciones en el ámbito del "ciberespacio". En particular se estudian los derechos, obligaciones de las partes y personas (naturales o morales) en relación con los mecanismos de protección de la información que contienen las sentencias que se publican en Internet.

Recibido: 20/1/2020 • Aceptado: 9/2/2020

* Universidad Central de Venezuela, abogado (14/366), Especializaciones en Derecho Procesal y Derecho Internacional Económico y de la Integración, Doctor en Ciencias Mención Derecho, ex Auxiliar de Investigación Docente, *Facultad de Ciencias Jurídicas y Políticas, Escuela de Derecho*, ex profesor de Derecho Administrativo II y III, ex profesor de Introducción al Derecho y profesor de Derecho Civil III (Obligaciones), ex profesor de en la Especialización de Derechos Humanos. 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. Conferencista en diferentes eventos. Tribunal Supremo de Justicia, Abogado Auxiliar II. Ponencias, ha participado en diferentes ponencias en materia de créditos indexados, derechos humanos y derecho procesal. Publicaciones, Autor de varias publicaciones en varias revistas especializadas. Email sfernandez_edu@yahoo.com.

Palabras clave: Derechos fundamentales. Protección de datos. Sentencias. Internet.

Abstract

The goal of this paper is to ilustrate, in a general way, the legal problems raised by the confluence of Informatics and Telecommunications in the field of "cyberspace". In particular, it is focused in the study of rights, obligations of the parties and persons (natural or moral) related to the mechanisms of protection of personal information in the judgments published on the Internet.

Key words: Fundamental rights. Data Protection. Sentences. Internet.

Introducción

Ya desde hace algún tiempo existe en nuestras vidas una gran influencia y participación de las tecnologías, las cuales empleamos en muchos aspectos y áreas, entre ellas en el Derecho, siendo que son utilizas como herramientas para enviar y recibir escritos, publicar sentencias, promover pruebas digitales.

Esto ha planteado nuevas formas de usar, crear y acceder a la información a través de las herramientas tecnológicas, lo cual genera repercusiones que en principio son neutrales sobre los derechos de las personas y en particular respecto al derecho a la privacidad y protección de datos personales.

Sin duda alguna, el Derecho se ha visto influenciado por el uso de las tecnologías de donde surge lo que se ha dado en llamar Derecho telemático, entendido como algo que forma parte de la informatización de la sociedad para establecer una relación entre las computadoras y las telecomunicaciones, siendo que la televisión, la telefonía y los computadores, entre otros, convergen para trasmitir sonido, imagen, datos y textos a través de líneas telefónicas, fibras ópticas, cables submarinos y enlaces satelitales, motivo por el cual estos hechos conllevan connotaciones políticas y éticas con significativas proyecciones en el campo jurídico.

Por otra parte el Derecho informático es entendido como un conjunto de principios y normas que regulan los efectos jurídicos de la relación entre el Derecho y la Informática, involucrando varios aspectos como la contratación informática, los delitos cometidos mediante su uso, las relaciones laborales que se pueden producir de ella, los litigios sobre la propiedad de programas o datos, etcétera. Sin embargo, se suele usar este término y el de Derecho telemático como sinónimos, así como el de Derecho de las nuevas tecnologías, Derecho de la sociedad de la información, Iuscibernética, Derecho tecnológico, Derecho del ciberespacio, Derecho de internet, etcétera.

En tal sentido, en internet, los programas y aplicaciones que son los más exitosos son aquellos que se alimentan a través de la aportación de información por parte de los propios individuos que las emplean, donde el usuario se convierte en difusor de información personal, propia y de terceros y no es un mero espectador, lo cual ha hecho que surjan nuevos conflictos relacionados con la privacidad, tratando de aportar el nuevo "derecho al olvido" de dar una solución a los mismos.

De lo anterior y en función de esa realidad, el objetivo perseguido por el presente trabajo es el de dar a conocer de manera general la problemática jurídica que suscita el encuentro de la Informática y las Telecomunicaciones, que se da en el "ciberespacio", expresión con la que se suele designar el ámbito de acción de Internet, que constituye su soporte, en particular con relación a los derechos y obligaciones de las partes y personas (naturales o morales) sobre las que aparece información mencionada en las sentencias; así como aquellas que surgen también en el órgano judicial y el Estado. Esto toma mayor relevancia cuando notamos que se le ha caracterizado a la telemática como "un microcosmos digital en el que no existen fronteras, distancias ni autoridad centralizada", lo cual no implica la ausencia total de regulaciones, sino que la determinación y aplicación de las normas jurídicas ya existentes revisten una particular complejidad como consecuencia de su vocación extraterritorial.

De allí que se mencionan cuales son las posibles acciones que se pueden interponer para la protección de los derechos fundamentales y constitucionales involucrados, indicar cuáles son los derechos, obligaciones y responsabilidades de los posibles actores, así como las medidas de seguridad que se han de tomar.

I. Algunos derechos humanos involucrados

Para poder entender algunos de los derechos involucrados en el Derecho telemático, primero debemos aclarar qué son los derechos humanos, siendo que una de las características de los mismos es su estrecha relación entre todos ellos para con la dignidad humana y su imprescindibilidad en el sistema democrático[1], por lo que los derechos humanos son la proyección jurídica de la dignidad de la persona y la condición de su desarrollo, lo cual a su vez subraya la dimensión individual de los mismos[2], por lo que abarcan a toda de persona, entendiendo esta como una construcción técnico-jurídica que surge de una

1 En donde los derechos humanos son el objetivo que justifica el sistema político.

2 SOLOZÁBAL ECHEVARRÍA, Juan José, "Una revisión de la Teoría de los derechos fundamentales", *Revista Jurídica*, Universidad Autónoma de Madrid, N° 4, UAM Ediciones. Madrid, 2001, pp. 106-107. Igualmente lo señalan RUBIO LLORENTES, Francisco. "Derechos fundamentales, derechos constitucionales y derechos humanos". *Revista Politeia*, N° 26. Instituto de Estudios Políticos de la Universidad Central de Venezuela, Facultad de Ciencias Jurídicas y Políticas. Primer Semestre de 2001, p. 133-137; AYALA CORAO, Carlos M. "Recepción de la jurisprudencia internacional sobre derechos humanos por la jurisprudencia constitucional". *Revista*

necesidad lógico-formal en razón de las relaciones sociales, y en la medida en que éstas generan derechos y obligaciones, en la que el Estado debe garantizarlos.

Por ello, todos los Estados, independientemente de cuál sea su sistema político, económico y cultural, tienen la obligación de promover y proteger todos los derechos humanos y libertades fundamentales, asumiendo la responsabilidad, de conformidad con los distintos tratados internacionales sobre la materia, de respetar estos derechos y las libertades fundamentales, sin distinción de ningún tipo por motivos de raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento u otra condición. En este sentido la paz, la seguridad, el desarrollo y los derechos humanos son los pilares del sistema de los Estados, lo cual crea los cimientos de la seguridad y el bienestar colectivo, encontrándose estos aspectos vinculados entre sí, reforzándose mutuamente, y por ello, la importancia de garantizar la universalidad, objetividad y no selectividad en el examen de las cuestiones de derechos fundamentales y de eliminar la aplicación de un doble rasero y la politización, donde la promoción y protección de los derechos humanos debe basarse en los principios de la cooperación y el diálogo genuino, obedeciendo al propósito de fortalecer la capacidad de los Estados para cumplir sus obligaciones en materia de estos derechos en beneficio de toda la humanidad.

1. Dignidad de la persona humana

La dignidad de la persona humana es considerada como un núcleo axiológico constitucional y por lo tanto un valor jurídico supremo[3], reconocido en el primer párrafo del Preámbulo y en el artículo 1 de la Declaración Universal de Derecho Humanos del 10 de diciembre de 1948[4], así como el Preámbulo del Pacto Internacional de Derechos Civiles y Políticos, suscrito en Nueva York el 16 de

Politeia, N° 26. Instituto de Estudios Políticos de la Universidad Central de Venezuela, Facultad de Ciencias Jurídicas y Políticas. Primer Semestre de 2001, p. 139; FERNÁNDEZ SEGADO, Francisco. "Sistemas de Protección Judicial de los Derechos Fundamentales". *Revista de Derecho Constitucional*, N° 1 septiembre-diciembre 1999. Editorial Sherwood. Caracas, Venezuela, pp. 55-56; y, NOGUEIRA ALCALÁ, Humberto. "Las Dignidad de la Persona, Derecho Esenciales y Derecho a la Igual Protección de la Ley". *Revista de Derecho Constitucional*, N° 1 septiembre-diciembre 1999. Editorial Sherwood. Caracas, Venezuela, pp. 241-265.

3 FERNÁNDEZ SEGADO, Francisco. "La dignidad de la persona como valor supremo del ordenamiento jurídico". *Revista Tachirense de Derecho*, Universidad Católica del Táchira, N° 7. Editorial Universidad Católica del Táchira. San Cristóbal, Estado Táchira. Enero-Diciembre 1995. p. 5.

4 El Preámbulo dice: "Considerando que la libertad, la justicia y la paz en el mundo tienen por base el reconocimiento de la dignidad intrínseca y de los derechos iguales e inalienables de todos los miembros de la familia humana".

diciembre de 1966[5], siendo que según Von Wintrich[6] la dignidad del hombre es aquella que consiste en que *"el hombre, como ente ético-espiritual, puede por su propia naturaleza, consciente y libremente, autodeterminarse, formarse y actuar sobre el mundo que lo rodea"*. De este modo los derechos humanos o fundamentales deben tener a la dignidad humana como origen y fundamento del cual emanan, siendo considerada su existencia, por la doctrina mayoritaria, incluso previa a la propia Constitución que la reconoce y garantiza.

De allí que el ser humano puede actuar con libertad de decisiones sobre las acciones que va a efectuar u omitir, incluyendo la posibilidad de actuar de hecho en forma consecuente con la decisión asumida, ya sea con una visión religiosa, ontológica, ética y social, donde, toda actuación en contra del individuo que implique desprecio genera una violación de la dignidad, debiendo tener en cuenta que el Estado existe, surge y se fundamenta en los derechos humanos y estando al servicio del hombre y no el hombre para la existencia del Estado, por lo que cualquier norma, actuación, omisión o situación que contravenga o ignore la dignidad de la persona se debe considerar nula, ya que esta es la fuerza ordenadora del ordenamiento jurídico, mucho más cuando el concepto de dignidad humana no es estática sino dinámica[7]; ante lo cual el Estado se encuentra obligado a realizar sus actuaciones e interpretaciones de conformidad con este valor y en función del mismo.

Aunque la dignidad de la persona es difícil de definir, no hay duda que implica un elenco de deberes impuestos a los miembros del grupo social en sus relaciones con todos los otros integrantes intrínseca de todas y cada una de las personas, por lo que se puede apreciar su vulneración, cada vez que se perturba, amenaza o priva de sus derechos esenciales o cuando se ponen cualquier tipo obstáculos para su plena realización y cada vez que el Estado la utiliza como un medio o instrumento de su propio fin. Se trata de una realidad ontológica supraconstitucional que el Estado y la Constitución la reconocen y garantizan pero no la crean. De este modo, el ser persona es ser un fin en sí mismo y se viola la dignidad humana cuando la persona es convertida en un objeto o se constituye como un mero instrumento para el logro de otros fines[8].

5 Que dice:
Considerando que, conforme a los principios enunciados en la Carta de las Naciones Unidas, la libertad, la justicia y la paz en el mundo tienen por base el reconocimiento de la dignidad inherente a todos los miembros de la familia humana y de sus derechos iguales e inalienables.

6 VON WINTRICH. *Zur Problematik der grunderechte*. 1957, p. 15, citado por FERNÁNDEZ SEGADO, Francisco. *Op. Cit.*, p. 8.

7 Es así como se habla de derechos humanos de primera, segunda, tercera y cuarta generación, en donde la dignidad humana se encuentra presente en todos ellos como conjunto, es el valor y principio que los nutre y forma parte de su núcleo esencial, teniendo en cuenta que esto se emplea como una mera clasificación y no como orden de creación y reconocimiento por el ordenamiento jurídico.

8 NOGUEIRA ALCALÁ, Humberto. *Op. Cit.*, p. 242.

2. Libre desarrollo de la personalidad

El libre desarrollo de la personalidad supone la facultad de todo individuo de hacer uso de todas sus potencialidades físicas, intelectuales y morales, en su propio beneficio, siendo que además se vincula de manera intrínseca con la posibilidad de que todo individuo pueda realizar y lograr su proyecto de vida. Este derecho apoyado en los demás derechos humanos, otorga al individuo la posibilidad de hacer todo aquello que esté a su alcance, siempre que ello no suponga la afectación injustificada de otros bienes jurídicos, para realizar el proyecto de vida libre y voluntariamente elegido por el sujeto, resguardando ese espacio de libertad individual en el cual el sujeto es realmente el soberano de su propio destino.

3. El derecho a la intimidad, a la vida privada y a la propia imagen

El artículo 60 de la Constitución, en el artículo V de la Declaración Americana de los Derechos y Deberes del Hombre, el artículo 12 de la Declaración Universal de Derechos Humanos, en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos; y el artículo 11 de la Convención Americana sobre Derechos Humanos, reconocen estos derechos. Así dentro de los elementos de la vida privada estará la vida familiar (filiación, matrimonio y divorcio), la vida amorosa, la imagen, los recursos económicos, los impuestos.

La *intimidad* se refiere a ese ámbito interior que sólo conoce uno mismo, en lo más interior y profundo, por ello, es el derecho a la reserva de la vida privada, por lo que no se puede poner de manera pública actos y datos personales sin permiso de la persona afectada (natural o jurídica, pública o privada, individual o grupal), quien determinará por sí misma cuándo, cómo y con qué extensión puede ser comunicada a terceros la información acerca de ella, por eso, es que puede ser entendida no solamente como una garantía (sentido negativo), sino también como presupuesto del ejercicio de otros derechos con proyección social e incluso económica (sentido positivo). Es un derecho personalísimo ligado a la existencia misma del individuo, que garantiza la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás (ya sea un particular o el Estado), necesario para mantener una la calidad de vida mínima sobre lo que recae la protección constitucional. Igualmente es un derecho dinámico, contingente y de delimitación casuística, por lo que la determinación del bien jurídico protegido por el derecho y las acciones efectuadas por terceros que se puedan considerar intromisiones ilegítimas dependerá de cada caso concreto y corresponderá a los órganos judiciales establecerlos.

Desde el punto de vista jurídico, es el derecho a la reserva de *la vida privada*, vinculado al derecho a la libertad, en cuanto derecho del individuo a hacer lo que le parece, esto es, a estar sólo, a no ser incomodado, a tomar decisiones en

la esfera privada sin la intervención de terceros y la estatal, pero que puede ser limitado, pero manteniendo una cierta área mínima de libertad personal que no debe ser violada, conocido también como núcleo esencial, y que en caso de ser invadido, por lo que el Estado o sus autorizados serán los únicos que podrán obligar a una persona a dar acceso a un dato, tanto al organismo estatal como a terceras personas, llegando así a la autodeterminación informativa y la protección de datos personales, con el derecho a la información contemplado en el numeral 19 de la Declaración Universal de Derechos Humanos.

El derecho a la *propia imagen* se encuentra reconocido en el artículo 60 constitucional, pero también en el artículo 65 de la LOPNNA, así como en el artículo 12 de la Declaración Universal de los Derechos Humanos. Este debe ser entendido como una manifestación del derecho a la intimidad, consistente en la facultad exclusiva del interesado a difundir o publicar su propia imagen y, por tanto, su derecho a impedir la reproducción o divulgación por cualquier medio, a no ser que medie consentimiento a autorización[9]. Este implica la representación gráfica de la figura humana, mediante la cual se precisa visualmente su aspecto físico, lo que implica que nadie puede disponer de la imagen de una persona sin su autorización[10], es su proyección física, la reproducción material de la personalidad corporal, por lo que nadie puede disponer de ella sin su autorización[11].

Estos derechos se vuelven relevantes ante la gran capacidad que posee el Estado así como los particulares para acumular y acceder a gran cantidad de información sobre las personas de toda índole que puede afectar el derecho al honor y a la reputación, así como a la privacidad y a la intimidad. Por lo que el derecho a la intimidad no pretende anular el derecho a la información, sino otorgar una protección de este derecho sin hacer nugatorio al otro.

Para poder desarrollar la personalidad, ejercer plenamente los derechos y disfrutar de la existencia, se debe tener cierta independencia y tranquilidad, ya que lo contrario viola la privacidad o *vida privada*, que requiere no ser molestado y que se respete cierto sector de nuestra vida, al sustraer de la intervención de los terceros determinados aspectos de nuestra existencia, que aunque no sean secreto, merece una especial consideración en función de las relaciones en juego, diferenciándose de la intimidad, en que la primera está en un ámbito más amplio y no secreto, mientras la segunda, lo privado no es necesariamente secreto[12], siendo por tanto "el conjunto de modos de ser y de vivir, de estados

9 OCHOA E., Oscar G. *personas. Derecho Civil I*. Universidad Católica Andrés Bello. Caracas, Venezuela, 2006. p. 482.

10 DOMÍNGUEZ GUILLEN, María Candelaria. "Algunos aspectos de la personalidad jurídica del ser humano en la Constitución de 1999". *Op. Cit.*, pp. 246-247.

11 DOMÍNGUEZ GUILLEN, María Candelaria. "Aproximación al estudio de los derechos de la personalidad». *Op. Cit*., pp. 232-247.

12 DOMÍNGUEZ GUILLEN, María Candelaria. "Aproximación al estudio de los derechos de la personalidad". *Op. Cit*., pp. 204-216.

afectivos, de acciones y reacciones que se desarrollan en el hogar, y que no tienen por qué transcender a la vida social pública de una colectividad", por lo que se deben respetar los derechos individuales de toda intromisión de terceros[13].

El derecho a la intimidad es la individualidad del propio ser, por lo que no puede ser siempre expuesta, porque se afectaría seriamente e ilegítimamente los derechos fundamentales de la persona, por ello, los alemanes han hablado del derecho a la autodeterminación informativa (Ley Federal de Protección de Datos de 27 de febrero de 1977)", por lo que en ellos existen "datos sensibles"[14].

Sin bien embargo, se debe tener presente que en el caso de las colectivas no podemos hablar de un derecho a la intimidad, por ser ésta una característica exclusiva de los seres humanos, si detentan un derecho a la imagen, y ciertamente no cabe duda que pueden verse afectados por un manejo indebido, discriminatorio o malicioso de las informaciones relacionadas con ellas.

4. El derecho a la integridad psicofísica y moral

Este derecho lo consagra el artículo 46 de la Constitución y en el artículo 5 numeral 1 de la Convención Americana sobre Derechos Humanos. La doctrina nos indica que dentro de este derecho se encuentran: la libertad, el honor, la vida privada, la intimidad, la autodeterminación informativa, la imagen y la voz[15]. Se refiere a los derechos vinculados con el aspecto no corporal del ser humano o la persona, sino con lo espiritual e intangible, aunque esto no significa que alguno de ellos tienen conexión en el plano físico o material.

5. Derecho al honor y a la reputación

La persona y la dignidad se encuentran muy vinculadas con el honor como uno de los aspectos más relevantes del individuo, ya que se trata de la apreciación de nuestra dignidad efectuada por nuestra propia persona (sentido subjetivo o autoestima) o por terceros (sentido objetivo o reputación).

Respecto al *honor* se dice que consiste en algo indefinible ya que se trata del sentimiento que cada quien tienen de su propia dignidad y de la manera que los extraños capturan la misma[16], o como la evaluación social de la persona, la

13 CHIOSSONE, Tulio. "Temas Procesales y Penales". Universidad Central de Venezuela. Facultad de Ciencias Jurídicas y Políticas. Instituto de Ciencias Penales y Criminológicas. Caracas, Venezuela, 1977, p. 277.

14 DELPIAZZO, Carlos E. "Protección de los datos personales en tiempos de internet. El nuevo rostro del derecho a la intimidad". *Revista de Derecho*, Universidad Católica del Uruguay, N° III. Uruguay, 2002, pp. 259-260.

15 DOMÍNGUEZ GUILLEN, María Candelaria. "Aproximación al estudio de los derechos de la personalidad". *Op. Cit*., p. 91.

16 DOMÍNGUEZ GUILLEN, María Candelaria. "Aproximación al estudio de los derechos de la personalidad". *Op. Cit*., p. 196; y en DOMÍNGUEZ GUILLEN, María Candelaria. "Ensayos

medida de sus cualidades sociales y espirituales como miembro de la sociedad, la cual dependerá principalmente del propio sujeto, ya que se basa en la conducta del individuo, su comportamiento y actitud ante los intereses de la sociedad, el Estado, el colectivo y las demás personas[17].

Por lo que la divulgación de expresiones o hechos a través de cualquier medio de comunicación puede vulnerar el derecho al honor (como las páginas web de los tribunales), lo cual se vincula al "derecho a una comunicación libre"[18] y al ejercicio del derecho a la libre información[19], pero se requiere el requisito de veracidad[20], por lo que se debe ponderar el interés público de la noticia o la dimensión institucional de esta libertad que tiene por objeto la transmisión de hechos, en sentido estricto y no susceptible de apreciación subjetiva[21], estando limitado por el derecho al honor y a la reputación, a la intimidad, o por la seguridad de Estado, independientemente que dicha información sea veraz.

La libertad de expresión[22] tiene por objeto la transmisión de pensamientos, ideas y opiniones, que se refieren a creencias y juicios de valor susceptibles de crítica política y difusión ideológica[23], tiene sus límites en cuanto no afecte o vulnere otros derechos constitucionales[24], por lo que toda en toda información se debe: a) rechazar el uso de todo tipo de apelativo que sea injurioso y degradante en cualquier contexto, genera un daño injustificado al prestigio de las personas, innecesario para la información, aunado al hecho que no existe un derecho al insulto; b) rechazar la emisión de imágenes que utilicen asuntos personales

sobre capacidad y otros temas de derecho civil". Tribunal Supremo de Justicia. *Colección Nuevos Autores*, N° 1. Caracas, Venezuela, 2010, pp. 632-634.

17 Así lo indica NICOLÁI MELÉIN, citado por OCHOA E. Oscar G. "Personas". Derecho Civil I. Universidad Católica Andrés Bello. Caracas, Venezuela, 2006, p. 479.

18 Que según la doctrina alemana incluye el derecho a la libertad de expresión y el derecho a la información. Así lo indica ARAGÓN REYES, Manuel. "El derecho al honor de las personas jurídicas y sus posibles colisiones con el derecho a la información". *Revista Jurídica*. Universidad Autónoma de Madrid. N° 1. UAM Ediciones. Madrid, 1999, p. 28.

19 Artículo 58 de la CRBV.

20 La veracidad se ha de entender no como un límite sino como un presupuesto indisociable de ese derecho, del cual no puede prescindir el legislador porque es un elemento impuesto por la Constitución, al igual que la oportunidad y la imparcialidad. Esto no significa que no se pueda incurrir en un error, pero se obliga a extremar la diligencia en la comprobación de la información, entre los hechos transmitidos con los datos objetivos, que dependiendo del tipo de medio de comunicación y de la gravedad de la noticia exigirá mayor o menor comprobación. Por lo tanto, sólo la información dada en cumplimiento de estos elementos es la que se encuentra reconocida y protegida por la ley, el resto puede dar pie a ilícitos penales o civiles como la difamación y reparaciones por daños y perjuicios.

21 SSTCE 51/1985 y 223/1992 ARAGÓN REYES, Manuel, *Op. Cit*., p. 29.

22 Artículo 57 de la CRBV.

23 SSTCE 51/1985 y 223/1992 ARAGÓN REYES, Manuel, *Op. Cit*., p. 29.

24 Por ello se considera que los hechos (noticias) están excluidos de este derecho, así como que sólo ampara estrictamente opiniones como juicios morales, excluyendo las afirmaciones sobre datos de la realidad comprobables objetivamente. ARAGÓN REYES, Manuel, *Op. Cit*., p. 33.

como instrumentos de diversión y entretenimiento; y c) el rechazo a manifestaciones, expresiones o campañas de carácter discriminatorio, que atentan directamente contra el derecho al honor y la reputación.

De allí que toda persona, independientemente de su conducta tiene derecho a ser protegido de cualquier ataque injusto, tanto el aspecto objetivo como subjetivo de este derecho, en razón de la dignidad humana (artículos 60, 241, 444 y 446 del CP, el artículo 1.196 del CC, el artículo 11 de la Convención Americana de Derechos Humanos, el artículo 17 del Pacto de Derechos Civiles y Políticos y el artículo 12 de la Declaración Universal de Derechos Humanos), por lo que ante una intromisión en el honor e intimidad de la persona para que no se considere que existe una violación, debe haber un consentimiento del afectado, o se requiere que la información cumpla con la condición de veracidad y que se desarrolle en el ámbito del interés general, o que se está en el ejercicio legítimo del derecho a informar, o que se efectúe una investigación por razón de un delito y finalmente porque se esté en el ejercicio legítimo del derecho de corrección de los padres, tutores o de quienes hagan sus veces respecto de sus hijos menores[25].

En lo referente a la titularidad en cuanto al derecho al honor respecto a las personas colectivas o morales, se les ha reconocido su protección, estimando que el honor no es sólo el "honor espiritual", sino también el "honor mercantil", "el honor comercial" o el "honor profesional", ante lo cual puede ser titular de ese derecho y obtener tutela judicial ante cualquier vulneración[26]. Así la titularidad de los derechos fundamentales por las personas jurídicas no es sólo en protección del interés de las personas físicas que son su sustrato material o incluso de la

25 Incluso la Sala Constitucional en su sentencia N° 1.013 de 12 de junio de 2001, estableció que:

> *La información agraviante, es aquella que lesiona la dignidad, el honor, la reputación, la imagen, la vida privada o íntima, de las personas, exponiéndolas al desprecio público, que puede dañarlas moral o económicamente, y que resulta de una imputación que no se corresponde con la realidad, o que no atiende a la situación actual en que se encuentra una persona. Se trata de imputarle o endilgarle hechos o calificativos que no son congruentes con la situación fáctica o jurídica del agraviado. Ante tal información, nace en la ´víctima´ el derecho a que se rectifique, o a dar respuesta contraria a lo que se le imputa, y en ambos casos, el amparo constitucional podría ser la acción que concretaría la protección a los derechos que le otorga el artículo 58 comentado, si se niega la réplica o la rectificación*.

Igualmente la Sala Constitucional en su sentencia N° 1.074 de 19 de septiembre de 2000, señaló que:

> *Ahora bien, por otra parte el artículo 60 de la vigente Constitución otorga el derecho a la protección del honor y la reputación de las personas, protección que se hace concreta de varias maneras.*

26 ARAGÓN REYES, Manuel. "Derecho al honor de las personas jurídicas y sus posibles colisiones con el derecho de información". *Revista Jurídica de la Universidad Autónoma de Madrid*, N° 1, 1999, página 14.

protección de los fines para los que tales personas jurídicas fueron creadas, sino también en razón de la garantía de las condiciones de existencia e identidad de las mismas, por lo que salvo los derechos de estricta dimensión físico-personalista-personal que se interpretan restrictivamente para otorgar titularidad, los derechos fundamentales son susceptibles de titularidad por las personas colectivas, pero estas no actúan en defensa de un interés legítimo sino como titulares del derecho.

Así, la Sala Penal del Tribunal Supremo de Justicia en su sentencia N.° 240 del 25 de febrero de 2000, estableció que las personas jurídicas no tienen honor pero sí reputación. En tal sentido señaló que las personas jurídicas no tienen derecho subjetivo en el aspecto intrínseco por lo que no tienen honor, pero ello no implica que no puedan gozar de un aspecto extrínseco en cuanto a su relación con la sociedad y ello significa que sí poseen reputación. Por otra parte la Sala Constitucional también se ha pronunciado al respecto, en tal sentido se pueden el fallo N.° 1.136 del 5 de octubre de 2006, en el que señaló que:

> Esta Sala comparte igualmente el criterio del *a quo* en este aspecto, en cuanto a la reputación, ya que de ésta –con un valor económico- gozan las personas jurídicas de naturaleza mercantil, por lo que considera que a pesar de existir la violación al derecho a la reputación del accionante, no procede por la vía del amparo la inhibición del Presidente de la accionada, de actuar en el procedimiento contra las accionantes, ya que no consta de autos que se haya iniciado procedimiento alguno y en cualquier caso el planteamiento de dicha solicitud correspondería realizarse dentro del correspondiente procedimiento administrativo, y ASÍ SE DECIDE.

En este sentido tanto la Sala Penal como la Sala Constitucional, están de acuerdo en que las personas jurídicas gozan, por lo menos del derecho a la reputación, el cual puede ser defendido a través de la acción de amparo constitucional, no entendiéndolo como un derecho humano o una garantía procesal sino como un valor económico que debe ser protegido y en el caso de la Administración Pública como un valor de confianza y credibilidad que ha de ser preservado por parte de esta frente al administrado.

6. Acceso universal a Internet como derecho humano

Existen varias declaraciones internacionales dentro del marco de la Organización de Naciones Unidas que afirman como derecho humano el acceso a la "Sociedad de la Información", como acceso universal, entre las que están la Declaración de Ginebra de 2003, la Cumbre Mundial sobre la Sociedad de la Información o Compromiso de Túnez y su Declaración de Principios de 2005, los cuales se fundamentan especialmente en la libertad de expresión e información, en el derecho de recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.

En la Unión Europea el acceso a Internet se ha garantizando especialmente en el artículo 3 ordinal 1 de la Directiva 2002/22/CE, que exige la garantía a un acceso de calidad y a un precio asequible, lo cual se ha ido recogiendo en las diversas normas nacionales de comunicaciones. En América Latina, en el 2010 se presentó en México una propuesta de reforma de la Constitución para reconocer como artículo 4 ordinal 10 que "Toda persona tendrá derecho de contar con acceso a Internet, siendo este prioritario para el desarrollo nacional en los términos del artículo 25 de esta Constitución. El Estado determinará los mecanismos y formas para garantizarlo".

Independientemente de lo anterior, en todos los sistemas constitucionales hay normas jurídicas para apoyar las políticas conducentes a facilitar la sociedad de la información, del conocimiento, la alfabetización digital y el acceso a Internet, lo cual se empieza a conocer como *ius comunicationis* o *communication rights*, vinculado al artículo 19 de la Declaración Universal de los Derechos Humanos.

Esto demuestra la realidad de la penetración de internet y su carácter esencial para el desarrollo futuro de las naciones y el desarrollo personal de los individuos, mediante el acceso efectivo y funcional a la red a precios asequibles, lo cual se va a ir colocando como contenido de diversos derechos humanos, como el derecho de acceso a la información, a la educación y de acceso a la cultura, así como de otros aspectos jurídico constitucionales. Todo lo anterior debe ir vinculado con el garantizar la igualdad y prohibición de discriminación en el acceso a internet, ya que los que menos acceden son los sectores más necesitados y la falta de acceso puede agudizar la brecha social ya existente.

7. Libertades de expresión e información en Internet

En este mundo virtual se dan situaciones contra la protección clásica de la propiedad intelectual, ya que se habla de libertad en la red y movimientos del software libre, por lo que en los inicios de internet, se consideró al ciberespacio como el estado de libertad salvaje o natural, tal como se estableció en la conocida Declaración de Independencia del Ciberespacio de 1996[27] o la Propuesta de Declaración de los Derechos Humanos en el Ciberespacio de Gelman del mismo año[28], realizadas en el marco de la "primera guerra" por la libertad de expresión

27 Es un texto presentado en Davos, Suiza el 8 de febrero de 1996 por John Perry Barlow, fundador del *Electronic Frontier Foundation*, como respuesta a la aprobación en Estados Unidos de Norte Amérrica de la *Telecommunications Act*, tratándose de una reivindicación que critica las interferencias de los poderes políticos que afectan el mundo del internet y defiende la idea de un ciberespacio soberano.

28 Basado en la Declaración Universal de los Derechos Humanos de la Organización de Naciones Unidas, Robert B. Gelman elaboró su Declaración que propone una serie de artículos en los que se pretende elevar la calidad de vida en la red. La declaración consagra 24 artículos en los que se habla del derecho a iguales oportunidades para expresar y discutir las ideas más allá de

en internet, en la batalla jurídica contra la Ley de Decencia de las Comunicaciones de 1996 de EEUU (*Communications Decency Act*, CDA) que finalizó de manera favorable para la libertad de expresión ante el Tribunal Supremo federal en 1997 en el caso ACLU vs Reno. Esta sentencia trascendió las fronteras de aquel país, aplicándose a internet el estándar más amplio de protección en similitud a la prensa escrita, así como se enfatizó el efecto disuasorio que provoca perseguir conductas escasamente definidas, siendo que para esa fecha, en Europa o América Latina, ningún tribunal nacional ni supranacional había generado una sentencia tan importante sobre internet.

Las amenazas a la libertad en internet suelen proceder de la acción de los grandes productores de estos elementos en complicidad con los Estados que tienen capacidad real de acción, con lo cual ha surgido Linux (popular sistema operativo abierto a diferencia de Windows que es cerrado) a partir del cual se integró al Proyecto GNU de la *Free Software Foundation*, presidida por Richard Stallman, para un código abierto, *Open Source*, que se trata de un movimiento social creciente y activo, que se expresa incluso con partidos políticos, que son partidos piratas, que permiten a los usuarios descargar masivamente contenidos protegidos y multiplican los medios para facilitar tales descargas, por lo que en el ámbito del Derecho, se destaca la generalización de las licencias *creative commons* (diseñadas por Lessig), en las que los autores liberan más o menos el uso de sus creaciones.

Sería contrario a la libertad de expresión exigir una autorización previa para la presencia en la red o someterla a los requisitos del servicio público, dado que no se dan las limitaciones del espacio radioeléctrico que pueden justificar el sometimiento al régimen de autorización administrativa. Además cuando se alojan contenidos ilícitos que puedan atentar contra la privacidad, la propiedad intelectual, entre otros, aún no se ha definido si se puede atribuir responsabilidad jurídica al prestador de servicios como podía ser una red social (Facebook), un alojador de vídeos (Youtube), de comentarios (periódicos, blogs, foros), de contenidos (Wikipedia), servidor de enlaces (Google), etc., usualmente el

barreras sociales, religiosas, políticas, raciales o de otro tipo; el derecho a la privacidad, anonimidad y seguridad en la red; a impedir el envío abusivo de correo electrónico masivo o publicitario; a crear normas que permitan facilitar la interacción de los seres humanos en comunidades virtuales específicas; a la aplicación cabal de las leyes del mundo físico; a compensaciones legales por violaciones contra la libertad y los derechos del ciberciudadano; a rechazar cualquier intento de vigilancia sobre sus actividades en la red; a ser oído, equitativa y abiertamente, por un tribunal independiente e imparcial para la determinación de sus derechos y obligaciones, así como de cualquier cargo formulado contra ella; a acceder a niveles básicos de información a través de instituciones públicas y proveedores de servicios; entre otros. La formulación de los Derechos Humanos en el Ciberespacio implica la reafirmación del ser humano en un medio que comúnmente se considera frío por sus características fundamentadas sobre bases electrónicas.

prestador de servicios de internet no tiene un deber de vigilar los contenidos que transmite ni es responsable de los mismos si son ilícitos[29].

Aun no se ha establecido si en un futuro, se pueda crear en el ámbito mundial un órgano administrativo que vele por la propiedad intelectual, o una agencia de protección de datos, o un organismo regulador de las telecomunicaciones, que pueda decretar el cierre o bloqueo de acceso de una página en la red, ni se ha celebrado un convenio internacional que de dichas atribuciones a cada país y que actúen de forma coordinada con un órgano internacional, sobre todo al considerar que no todo es libertad de expresión e información en internet, siendo un criterio para identificarla el que exista un interés o relevancia pública de la información, así como la veracidad y la diligencia del informador y el derecho de réplica o rectificación.

II. Mecanismos procesales de protección de los derechos humanos ante la publicación digital de la sentencia

Cuando se produce la publicación de un fallo en internet, esa información y todo su contenido es público, salvo en los casos especiales que aunque en general la normativa permite el acceso a la información, en ciertos casos ésta se reserva, tal es el caso de el artículo 304 del Código Orgánico Procesal Penal; los artículos 70, 96 y 97 de la Ley Orgánica del Ministerio Público; los Ley artículos 22, 74, 155, 156, 158, 163, 164, 165, 166, 168 y 169 de la Orgánica de la Administración Pública; los artículos 7, 47 y 79 de la Ley Orgánica de la Contraloría General de la República; el artículo 102 de la Ley Orgánica de las Fuerzas Armadas Nacionales; los artículos 6 y 36 de la Ley Orgánica de la Procuraduría General de la República; artículo 59 de la Ley Orgánica de Procedimientos Administrativos; artículo 160 de la Ley Orgánica de Régimen Municipal; los artículos 24, 53 y 99 de la Ley Orgánica de Salvaguarda del Patrimonio Público; artículo 38 Ley Orgánica para la Ordenación del Territorio; los artículos 65, 157, 158 y 429 de la Ley Orgánica para la Protección del Niño, Niña y del Adolescente; el artículo 38 del Código Orgánico de Justicia Militar; el artículo 24 del Código de Procedimiento Civil; el artículo 5 de la Ley del Ejercicio del Periodismo en Venezuela; el artículo 3 del código de Ética del Periodista Venezolano y la Ley de Estadísticas, entre otras. Así para proteger de los anteriores derechos, esto se puede dar a través de diferentes acciones judiciales, entre las que se encuentran las que señalaremos a continuación.

En este sentido, también se puede observar lo establecido en la sentencia de la Sala Constitucional N.° 1.744 del 9 de agosto de 2007, en la que se señaló que:

29 En Estados Unidos de Norte América está la sentencia de 2006 del Tribunal Supremo de California en el caso Stephen J. Barrett et al. vs. Ilena Rosenthal, exime de responsabilidad al usuario individual que distribuye publicaciones en la red.

> *… la figura de la reserva legal viene dada por la consagración a nivel constitucional de determinadas materias que, debido a la importancia jurídica y política que tienen asignadas, sólo pueden ser reguladas mediante ley, desde el punto de vista formal, y ello excluye la posibilidad de que tales materias sean desarrolladas mediante reglamentos o cualquier otro instrumento normativo que no goce de dicho rango lega*l….
> *Este principio esencial del régimen constitucional venezolano, se encuentra contemplado en el artículo 156.32 de la Constitución de la República Bolivariana de Venezuela….*
> *… de esta primera garantía [reserva legal] se desprenden a su vez otras cuatro garantías estructurales. En tal sentido, se habla en primer lugar de una GARANTÍA CRIMINAL, la cual implica que el delito esté previamente establecido por la ley (nullum crimen sine lege); de una GARANTÍA PENAL, por la cual debe necesariamente ser la ley la que establezca la pena que corresponda al delito cometido (nulla poena sine lege); de una GARANTÍA JURISDICCIONAL, en virtud de la cual la comprobación del hecho punible y la ulterior imposición de la pena deben canalizarse a través de un procedimiento legalmente regulado, y materializarse en un acto final constituido por la sentencia; y por último, de una GARANTÍA DE EJECUCIÓN, por la que la ejecución de la pena debe sujetarse a una ley que regule la materia*.

De todo lo anterior se observa la importancia de encontrar el equilibrio entre el acceso a la información y publicidad, con los otros derechos constitucionales involucrados y que se pueden vulnerar a través de la publicación digital de una sentencia.

1. Habeas Data

Sobre el habeas data, se ha escrito y dicho mucho tanto en el ámbito nacional como internacional, pero se puede decir que como aspectos relevantes que se suele observar como una garantía y protección de los datos personales (también se ve por algunos como un derecho subjetivo), por ende, se puede decir que se trata de una acción constitucional o legal que tiene cualquier persona que figura en un registro o banco de datos, de acceder a tal registro para conocer qué información existe sobre su persona, y de solicitar la actualización, rectificación o la destrucción de esa información si le causara algún perjuicio, estando consagrado en el artículo 28 de la Constitución de la República Bolivariana de Venezuela, el cual prevé los siguientes derechos:

1) De acceder a la información y a los datos que sobre sí misma o sus bienes, consten en registros oficiales o privados (informáticos o no), a menos que la ley les niegue el acceso, lo que puede resultar de prohibiciones expresas derivadas de la protección de determinados

secretos de la vida privada, de la seguridad del país, de derechos de autor, entre otros.

2) A conocer la finalidad y uso que da el compilador a esos datos e informaciones.
3) El derecho de respuesta, lo que permite al individuo controlar la existencia y exactitud de la información recolectada sobre él.
4) La actualización de los datos e informaciones, a fin de que se corrija lo que resulta obsoleto o se transformó por el transcurso del tiempo.
5) La rectificación de los errores provenientes de datos o informaciones falsas o incompletas, sin reparar si los asuntos corresponden a errores dolosos o culposos de quien los guarda.
6) La destrucción de los datos erróneos, o que afecten ilegítimamente los derechos de las personas (como lo sería mediante ellos ingresar arbitrariamente en la vida privada, o íntima, de los individuos, recopilando datos o informaciones personales; o aquéllas que permitan obtener ilegítimamente un perfil del individuo, por ejemplo, que afecte el desarrollo de su personalidad). Este derecho, permite al reclamante optar entre la rectificación o la exclusión del dato erróneo.

Por lo tanto, se trata de derechos que giran alrededor de los datos recopilados sobre las personas o sobre sus bienes (materiales o inmateriales), por lo que requiere que ésta tenga un interés personal, legítimo y directo para ejercer la acción y reclamar los derechos vinculados a esta. Por ello, cualquier persona que tenga conocimiento que un determinado ente, sea público o privado, está utilizando la información allí compilada y que ésta pueda lesionar la esfera jurídica de éste, puede solicitar en primer lugar, el acceso a la referida información a los fines de conocer la finalidad y uso de la misma, inclusive si se trata de una sentencia en la que se haga referencia a las partes y terceros que pudieron o no haber participado en el proceso judicial o que se encuentre reservada previa demostración de interés legítimo de conocer dicha información. Así, si el ente niega el acceso a la información a la persona afectada, éste podrá ejercer acción de amparo constitucional para obtener la información y si ésta resulta errónea o inexacta la parte interesada deberá dirigir carta motivada al ente compilador de datos con miras a solicitar su rectificación, actualización o destrucción, siendo que en el caso que no se corrija, ello dará pie a la posibilidad de interponer el habeas data, no importando su forma de recolectar, almacenar o distribuir los mismos, permitiendo como consecuencia, la modificación de dicha información, en caso de ser la misma inexacta, discriminatoria o simplemente, invasiva de la esfera de intimidad personal o cualquier otro derecho relacionado, pudiéndose pedir su actualización o confidencialidad, si debieran

permanecer en tal estado (ej: datos estadísticos o sentencias judiciales). Aunque en principio esta acción es para personas individuales, no se considera descabellado pueda ser usada por una colectividad.

2. Demanda por intereses colectivos y difusos[30]

La materia de los intereses colectivos y difusos, supraindividuales o pluripersonales, conlleva a la ampliación de lo que se entiende por legitimación activa de las partes, lo cual, a su vez, permite que participen en juicio nuevos actores que son las personas naturales y las colectivas o morales que pueden intervenir para proteger no solamente sus derechos individuales, sino también los de una comunidad definible de personas o a un grupo indeterminado de ellas, sin llegar a ser una acción popular o *actio class* norteamericana, teniendo su definición en las sentencias de la Sala Constitucional N.° 656 del 30 de junio de 2000 y N.° 3312 del 2 de diciembre de 2003.

Esta acción cobra más sentido cuando se observa el artículo 143 constitucional que permite a los ciudadanos ser informados oportuna y verazmente por la Administración Pública, sobre el estado de las actuaciones en que estén directamente interesados, y a conocer las resoluciones definitivas que se adopten sobre el particular, teniendo acceso a los archivos y registros administrativos, sin perjuicio de los límites aceptables dentro de una sociedad democrática en materias relativas a seguridad interior y exterior, a investigación criminal y a la intimidad de la vida privada, de conformidad con la ley que regule la materia de clasificación de documentos de contenido confidencial o secreto, estando prohibida la censura alguna y sancionando a los funcionarios públicos que informen sobre asuntos bajo su responsabilidad, lo cual sería aplicable a los funcionarios del poder judicial respecto al contenido de las sentencias y demás documentos contenidos en el expediente judicial.

De lo anterior, se observa que las personas naturales, las morales y la colectividad podrían interponer esta acción, siendo que la protección de los intereses difusos no puede ser ilimitada, restringida o discriminada, siempre y cuando exista una relación de causalidad dada por el efecto reflejo de la objetividad en la subjetividad, donde el interés colectivo se traduzca en alguna afectación aunque fuere indirecta o refleja, pero nunca remota o de conveniencia, como en el simple interés, debiendo haber siempre una vinculación por razón de consumo, vecindad, habitabilidad, u otra equivalente o análoga, de lo contrario no habría legitimidad ni interés difuso o colectivo.

En relación a la legitimación pasiva, la misma corresponde a toda persona, individual o colectiva, que dispongan de registro o bases de datos de naturaleza

30 Sobre este punto se pude ver FERNÁNDEZ CABRERA**,** Sacha Rohán. "La legitimación procesal para actuar de la Defensoría del Pueblo (especial referencia a los derechos e intereses colectivos y difusos)". Libro Homenaje a Nectario Andrade Labarca. Editado por el Tribunal Supremo de Justicia. *Serie Libros Homenaje* N° 13. Julio de 2004.

pública o destinados a producir informes, donde pudiesen quedar excluidos aquellos de simple almacenaje de datos como archivos científicos, periodísticos, etc., no destinados a registrar de modo especial y particularizado datos sobre personas, destinados al conocimiento de terceros, pero ello, no es óbice de que proceda la acción para que los informes no se distribuyan de modo indiscriminado o al público en general, por lo que se podría interponer contra un registro que, sin estar abierto al público en general, informa a los socios cuando por la entidad o magnitud social o económica de la misma pudiese traer un perjuicio.

3. El derecho al olvido[31]

Este derecho ha sido vinculado o relacionado con el *habeas data* y la protección de los datos personales, por lo que se entiende como la facultad que tiene el individuo sobre datos personales para borrarlos, bloquearlos o suprimirlos, cuando contengan información personal que se considere obsoleta por el transcurso del tiempo o que de alguna manera afecte el libre desarrollo de alguno de los derechos fundamentales del sujeto titular del mismo.

Este derecho por lo tanto puede vincularse, coexistir o chocar en ocasiones con el *habeas data*, los derechos de la personalidad y la libertad de expresión, siendo un mecanismo de protección o garantía del derecho a la privacidad y protección de datos en el mundo virtual, mediante la solicitud de tutela de sus derechos de oposición y cancelación respecto a informaciones publicadas, ante la ausencia de criterios que permitan otorgar una prevalencia del derecho a la libertad de expresión e información sobre el derecho a la protección de datos. En tal sentido puede ser vinculado, visto o relacionado en diferentes aspectos y ámbitos, entre los cuales encontramos:

A) *En los informes comerciales*, cuando se trata de informes crediticios, así una primera norma en tratarlo lo fue la *Fair Credit Reporting Act* (Ley de Informes Crediticios), que fuera aprobada por el Congreso Federal Estados Unidos de Norte América en 1970, en el que se admite en ciertas situaciones la eliminación de la información antigua o caduca; también en España, existe la Ley de Protección de Datos Personales[32] que regula el derecho al olvido en materia de ficheros de morosos en el artículo 29 ordinal 4; en Argentina, esta

31 Para profundizar más sobre este derecho se puede consultar a FERNÁNDEZ CABRERA, Sacha Rohán. "Derecho al olvido". *Revista Venezolana de Legislación y Jurisprudencia* N° 6. Caracas-Venezuela, 2016.

32 Esta es la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, (LOPD), que tiene por objeto garantizar y proteger lo concerniente al tratamiento de los datos personales, las libertades públicas y los derecho fundamentales de las personas naturales, especialmente de su honor, intimidad, y privacidad personal y familiar, fundamentándose en el artículo 18 de la Constitución Española de 1978, con ella se pretende regular el tratamiento de datos y ficheros de carácter personal, independientemente del soporte, informático o no, en el

situación fue reconocida primero por la jurisprudencia en la sentencia "Falcionelli, Esteban P. v. Organización Veraz S.A. en amparo" de la Corte Nacional Civil, Sala G, en fallo del tribunal de Primera Instancia el 10 de mayo de 1996[33], a la que le siguieron varios fallos de la Cámara Comercial y luego la Ley de Protección de Datos Personales lo cristalizó en el artículo 26 de la ley 25.326, con lo cual luego de su expreso reconocimiento legal se afianzó en la jurisprudencia. El problema era que la gente contraía créditos, se endeudaba, luego no los paga, pasaban 20 años, el crédito estaba prescripto, el banco no podía reclamar la ejecución del crédito, pero la información contenida era más fuerte que una obligación natural, la persona no podía obtener otro crédito porque seguía figurando como deudora, teniendo dos opciones: 1) pagar la deuda prescrita (obligación natural) para que lo borraran del sistema y poder empezar desde cero, o 2) recurrir al derecho al olvido y eliminar la información negativa.

En Venezuela, la Defensoría del Pueblo interpuso una acción de nulidad en contra del artículo 192 del Decreto con Fuerza de Ley General de Bancos y otras Instituciones Financieras de 2001 y que se mantuvo inalterado con las sucesivas modificaciones hasta la ley dictada el 19 de agosto de 2010, que regulaba el Sistema de Información Central de Riesgos, siendo decidida por la Sala Constitucional mediante sentencia N.° 1.318 de 4 de agosto de 2011, estableciendo con carácter vinculante que toda normativa o sistema sobre datos personales que contenga información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables, debe garantizar: 1) el principio de la autonomía de la voluntad, 2) el principio de legalidad, 3) el principio de finalidad y calidad, 4) el principio de la temporalidad o conservación, 5) el principio de exactitud y de autodeterminación, 6) el principio previsión e integralidad, 7) el

cual sean tratados, quedando excluidos aquellos datos recogidos para uso doméstico, las materias clasificadas del estado y aquellos ficheros que recogen datos sobre terrorismo y otras formas de delincuencia organizada.

33 En esta sentencia se indicó que el dato caduco es el dato que por efecto del transcurso del tiempo, ha perdido virtualidad, ha devenido intrascendente a los efectos de cualquier efecto jurídico relativo a la ejecutabilidad, con lo cual, lo que se busca proteger con este derecho es el permitir la supresión del dato caduco que es el "derecho al olvido". Este, es el principio también a partir del cual ciertas informaciones deben ser eliminadas de los archivos transcurrido un determinado espacio de tiempo desde el momento en que acaeció el hecho a que se refieren, para evitar que el individuo quede prisionero de su pasado. Por ello, concluyó que de las constancias de lo actuado, surgía que la información producida por el Banco Central de la República Argentina conforme la cual se sindicaba al actor como deudor del ex Banco Agrario Argentino Limitado en la base de datos de entidades financieras liquidadas, recogió una situación patrimonial que al momento de su publicidad resultaba violatoria de lo dispuesto en el artículo 26, inciso 4 de la ley 25.326, por cuanto, conforme lo estipula dicha norma, sólo podían archivarse, registrarse o cederse los datos personales que fueran significativos para evaluar la solvencia económico financiera de los afectados durante los últimos cinco años, en tanto que la deuda que informara el demandado -conforme el mismo lo señaló en la ampliación del informe- correspondía a un juicio en el cual se dictó una sentencia en el año 1978, y que la última actuación fue la inhibición general de bienes decretada en 1985 y que consecuentemente, se informó que la ejecutoria se encontraba prescrita.

principio de seguridad y confidencialidad, 8) el principio de tutela, y 9) el principio de responsabilidad, entre otros aspectos que se desarrollaron y mencionaron y que se encuentra vinculado a los fallos N.° 1.419 de 10 de julio de 2007 y N.° 1.474 de 14 de noviembre de 2012[34].

B) El *derecho al olvido en internet o digital*, surge a raíz de la incidencia que tiene en la vida privada de las personas el internet, en la que se puede encontrar numerosa información de una persona, donde a menudo parte de la misma ha sido publicada por terceros, siendo que este medio tiene un carácter global, suele ser permanente la data y de fácil acceso, por lo que es relevante el tomar conciencia sobre las informaciones propias y de terceros que se dan, para evitar la pérdida de control de las mismas cuando se incorporan a la red; así como que el usuario cuente con mecanismos efectivos de defensa ante los riesgos que se puedan presentar, ante lo cual se pide la existencia de unos límites para garantizar los derechos, sobre todo cuando se trata de informaciones no reveladas ni difundidas por el afectado.

De allí que ante la notoria universalización del internet, que contiene una enorme capacidad de almacenaje de información y posee importantes motores de búsqueda de información que permiten localizar cualquier dato en cuestión de segundos, y con extrema facilidad, lo que hace difícil que quede en el olvido alguna información, lo cual le da un carácter de perennidad a la misma que genera nuevos desafíos para el derecho, en cuanto a determinar si una persona puede lograr borrar esa información del pasado. Normalmente la solicitud de reclamo para la eliminación de esos datos se dirigen contra el medio original que lo contiene ya sea la prensa, el sitio de internet, etc., en donde se encuentra publicado y también contra el buscador que suele ser indexado con datos publicados por los propios individuos y terceros, en páginas o diarios oficiales (como los tribunales) o medios de comunicación y referidos a materias tan sensibles como la publicación de deudas, indultos, condenas penales o administrativas, juicios civiles, la concesión de subvenciones, la existencia de adicciones, violencia infantil o doméstica, con identificación de los involucrados, puede traer consecuencias sociales importantes en todos los aspectos y ámbitos de la vida de un ser humano.

Por lo que se pretende no aparecer en buscadores o redes sociales, porque les plantea problemas personales y quieren evitar que siga manteniéndose esa información personal en la red informática y eliminar el rastro que han dejado durante todo el tiempo que han utilizado internet, como podría ser información sobre despidos laborales, enfermedades, relaciones amorosas, entre otras, lo

34 El Tribunal Supremo de Justicia de Venezuela también ha hecho referencia al derecho al olvido en un caso que se pretendía borrar una información de tipo penal en los archivos del Estado, en tal sentido se puede ver la sentencia de la Sala Político Administrativa N° 00409 de 2 de abril de 2008, que fue objeto de revisión ante la Sala Constitucional según sentencia N° 1.542 de 17 de octubre de 2008.

cual puede afectar su vida profesional, personal, sentimental, social y familiar, para evitar que se puedan generar daños personales importantes, buscando que éstos se eliminen una vez que cumplan su finalidad; pero en la red participan otros elementos como los motores de búsqueda, que además de generar una multiplicación sumamente extensa de la información, la dan sin ningún tipo de limitación o edición de la misma y la dotan de un carácter casi eterno en ese mundo virtual, sobre todo cuando se habla del *Big Data* o tecnología de procesado de millones de datos en tiempo real, junto con el "Internet de las cosas", que es el fenómeno creciente de conexión de todo con todo mediante sensores y que está disparando el volumen de información disponible[35].

Frente a esto, las personas no disponían de mecanismos efectivos para ejercer su "derecho al olvido digital", siendo que toda persona debería tener control y disposición de sus datos e información relativa a ella; mucho más cuando la difusión de cierta información puede tener un impacto muy negativo en la vida cotidiana, aunado a los posibles perjuicios que puede generar a una persona esa difusión masiva en internet, siendo excluidos de esto las personas de relevancia pública, pero los demás pueden reaccionar y pedir corregir la data, por eso surgió la necesidad de dotar a las personas de mecanismos reales y efectivos de garantía de sus derechos. Así se han dado diversas iniciativas por parte de los Estados para dotar a los ciudadanos de estos necesarios mecanismos de defensa y un control real sobre la información personal que se publica en la internet o la red, tal como ocurre en Alemania con un proyecto de ley que contempla controlar el acceso y uso de los empleadores a las informaciones publicadas en servicios de internet; el gobierno galo realizó una consulta pública para ciudadanos y empresas del sector tecnológico sobre la necesidad de regular el derecho al olvido en internet; la Comisión Europea en junio de 2014, indicó que revisaría la legislación de la Unión Europea sobre protección de datos, para otorgar a los usuarios de internet un control efectivo sobre sus datos personales y reflexionar sobre el derecho al olvido en el mundo virtual[36], el Tribunal de Justicia de la Unión Europea, estableció el 13 de mayo de 2014[37], que en Europa el buscador Google, tiene la obligación de eliminar de sus listas de resultados aquellos enlaces que violen ciertos derechos de un ciudadano, a petición de éste, cuando la información en la red sea considerada inexacta, inadecuada, irrelevante o excesiva, sin meterse con la fuente original de la noticia, sino instruyendo a Google desarrollar un mecanismo que permita obviar información

35 Tomado de http://www.lapatilla.com/site/2015/01/28/big-data-e-internet-de-las-cosas-nuevos-desafios-en-la-privacidad-personal/, consultado el 28 de enero de 2015.

36 Esta situación de los impulsos legales ha sido señalado por RALLO LOMBARTE, Artemi. "El derecho al olvido y su protección a partir de la protección de datos". Cuadernos de comunicación e innovación. *Revista de Pensamiento sobre Comunicación, Tecnología y sociedad* N° 85, Octrubre-Diciembre, 2010, páginas 104-108.

37 Leída en http://ep00.epimg.net/descargables/2014/05/13/5ba6db7a62470eb16ac8feb397cf936d.pdf, consultada el 15 de enero de 2015.

que amerite ser olvidada, ante lo cual se creó un consejo asesor de alto nivel, compuesto por 10 autoridades mundiales sobre los temas en discusión (derechos individuales, libertad de expresión, derecho al acceso a la información, etc), con el objeto de buscar una forma razonable de cumplir con el mandato de la corte, siendo una medida aplicable a los residentes de Europa, entre otros casos.

Debemos tener en cuenta que los buscadores no pueden borrar la información ya que no son ellos los que la hacen o almacenan, sino que crean la indexación del lugar en la red que se encuentra la información. Los vínculos de internet no desaparecen, por lo que si el buscador respectivo acepta la solicitud, el vínculo indicado será retirado de todas las versiones europeas, que es donde es posible actualmente ejercerlo, pero permanecerá en las versiones no europeas, por lo menos hasta que se logre judicialmente también que dicha eliminación sea en la totalidad de las páginas del buscador respectivo. Por lo tanto, las páginas seguirán siendo las mismas y serán referenciadas por el buscador respectivo para otras búsquedas, por lo que será casi imposible "olvidar" al sujeto que solicite la eliminación de la información a los buscadores, ya que siempre permanecerá en algún lugar dicha información y siempre de alguna manera se podrá acceder a ella.

El fallo del Tribunal de Justicia de la Unión Europea fue claro al establecer que los particulares pueden pedir el retiro de informaciones que les conciernan y que ya no son pertinentes, salvo las de "interés público a raíz de un rol público" de la persona, por lo que los políticos o las personas célebres no serían beneficiados con este fallo, lo cual podría traer a discusión si se trata o no de una discriminación y violación al derecho a la igualdad o por el contrario, en razón de ser personas públicas, todo lo vinculado con ellos es público y no pueden alegar este derecho a su favor, ya que renunciaron de manera tácita, en cierta forma a ello, al ser figuras públicas.

Se pueden presentar dificultades en los casos de homonimia, siendo que se solicite la eliminación de un dato o información alegando que es propio cuando no lo es, ya que la página señalada puede concernir a un homónimo, lo que será difícil de verificar por el buscador respectivo. Otro problema es el cómo determinar que una persona es "pública", por ende, no tiene derecho a solicitar que se borre la información contenida sobre ella, o si dejo de ser funcionario público, considerar si es pertinente que con posterioridad esa situación de dejar de ser servidor público, tenga derecho a que se borre la información respectiva. Igualmente es complicado el establecer al cabo de qué plazo una información pasa a no ser pertinente. También está la dificultad de atribución de responsabilidad jurídica, tanto civil, administrativa o penal, según se trate en la red, porque: 1) hay problemas para perseguir contenidos ilícitos para el derecho nacional, por estar ubicados fuera del ámbito territorial; 2) usualmente quien integra el contenido ilícito lo hace de forma anónima, por lo que conocer su número IP que identifica el ordenador desde el que se conecta –si es que se puede- tal vez no sea suficiente para conocer la identidad de la persona que ha

cometido el ilícito; y 3) la autoría y difusión colaborativa de los contenidos de la web 2.0 conlleva que sea casi imposible de determinar el responsable del contenido y de su difusión[38]. Por último, también se puede presentar la dificultad de establecer el cómo crear un equilibrio entre el derecho a la información y derecho al olvido.

Pareciera, que no va existir solución a este nuevo tipo de reputación electrónica con el reconocimiento de este derecho al olvido, siendo que al respecto se ha dicho que "Es un avance en la buena dirección, una primera etapa, pero no es una revolución, porque la e-reputación se juega en gran medida actualmente en las redes sociales. Además, las páginas que contienen esas informaciones se las arreglarán para reaparecer", según advirtió Albéric Guigou, cofundador de Reputation Squad; así como, en opinión de Olivier Andrieu, consultor independiente de internet, "el verdadero derecho al olvido es la supresión del contenido. Los motores pueden olvidar, pero la web no olvidará"[39].

Como ya hemos señalado, los medios informáticos potencian también los peligros respecto de los derechos de la personalidad, como lo son la intimidad, protección de datos, secreto de las comunicaciones, honor, reputación, integridad física y moral, los cuales quedan expuestos en gran medida al peligro. De allí, la importancia del surgimiento en los años ochenta del derecho a la protección de datos personales y el *habeas data*, los cuales intentan dar respuesta a los particulares ante los peligros informáticos y desde entonces se han ido constitucionalizando expresa o implícitamente también este tipo de derechos[40].

Del mismo modo, otros derechos como el del secreto de las comunicaciones adquieren nuevas dimensiones y generan complejas situaciones, ya que es difícil

38 En Europa, a partir de la Directiva 2000/31/CE sobre el comercio electrónico, el esquema general es que el prestador de servicios de internet no tiene un deber de vigilar los contenidos que transmite ni es responsable de los mismos si son ilícitos, pero sí tiene el deber de retirar o bloquear los contenidos cuando las autoridades le comunican la ilicitud. Del mismo modo, como principio, no hay responsabilidad por el contenido de los enlaces o de los resultados que ofrece un servicio de búsquedas (como Google). Sin embargo, la regulación no da respuesta a los problemas que hoy son los más habituales. El problema principal reside en determinar si cualquier sitio en la red que permite integrar contenidos de terceros usuarios (desde un foro clásico a Youtube) puede beneficiarse de las exenciones legales de responsabilidad.

39 Tomado de http://www.eluniversal.com/vida/140603/las-claves-del-derecho-al-olvido-impuesto-a-google, consultado el 14 de junio de 2014.

40 Asimismo, para la protección específica de estos derechos en Europa se ha constitucionalizado en el artículo 8 numeral 3 de la Carta de la Unión Europea, además de la existencia de autoridades administrativas independientes y específicas que incrementan día a día su importancia. Incluso a veces se reconocen nuevos derechos, como el caso del derecho fundamental frente al registro oculto en línea, en la sentencia del Tribunal Constitucional Federal alemán de 27 de febrero de 2008, que declaró inconstitucional y nula la Ley de Renania del Norte-Westfalia (Az: 1 BvR 370/07 y 595/07). Igualmente destaca, ante el carácter internacional de estos hechos que amenazan la privacidad, la "Propuesta Conjunta de Estándares Internacionales de Protección de Datos y Privacidad» de 2009 por parte de las autoridades de supervisión españolas (la Agencia Española de Protección de Datos) para reforzar el carácter universal de estos derechos.

el tratamiento de los llamados datos de tráfico que generan las comunicaciones de telefonía móvil y el rastro de la navegación en la red[41]. Lo cierto es que no está en modo alguno claro si estos datos de tráfico de comunicaciones ya finalizadas (llamadas realizadas, correos, navegación en la web, etc.) quedan bajo la garantía del secreto de las comunicaciones (reforzada por la intervención judicial) o simplemente amparados por las más débiles garantías del derecho a la intimidad[42]. La cuestión se enlaza también con el derecho al anonimato de los internautas, que en su caso puede estar protegido por la libertad de expresión. Con esto se observa que no es nada fácil dar una solución a este problema.

Visto que la solicitud del accionante en el derecho al olvido se referiría al petitorio de cambio, modificación, corrección y destrucción de los datos e informaciones que se encuentran recogidos sobre su persona en archivos públicos y privados, se podría pensar que efectivamente guarda relación con el derecho de autodeterminación informativa o *habeas data*[43].

Así, el *habeas data* como derecho se relaciona con la información sea esta automatizada o no, en cuanto a la facultad que tiene el individuo de controlar las informaciones (acceso a la información, rectificación, modificación, destrucción, actualización, entre otros) que de su persona consten en las base de datos o redes de información, por lo que se encuentra íntimamente relacionado o da el derecho a la autodeterminación informativa. Igualmente, es una garantía, medio, instrumento o mecanismo procesal en cuanto a que permite el acceso a los órganos de administración de justicia en protección de otros derechos fundamentales como la intimidad, el honor, la reputación, la vida privada, etc.,

41 Desde el ataque terrorista en Nueva York de 11 de septiembre de 2001, en Madrid el 11 de marzo de 2004 y en Londres el 7 de julio de 2005, surgen en todo el mundo normativas que obligan a la retención masiva de estos datos para la investigación por los cuerpos y agencias de seguridad, como sería el caso en la Unión Europea de la Directiva 2006/24/CE, así como la más importante Convención internacional sobre el Cibercrimen, de 2001, del ámbito del Consejo de Europa, que facilita la posibilidad de acceder a los diversos datos contra la comisión de delitos.

42 La primera opción parece ser la seguida en Europa al ver las sentencias del Tribunal Europeo de Derechos Humanos de 3 de abril de 2007 (caso Copland vs. Reino Unido, asunto 62617/00), de 16 de octubre de 2007 (caso Wieser y Bicos Beiligungen GMBH vs. Austria, asunto 74336/01); de 22 de mayo de 2008 (caso Iliya Stefanov vs. Bulgaria, asunto 65755/01) y de 10 de marzo de 2009 (caso Bykov vs. Rusia, asunto 4378/02).

43 Entendiendo que la autodeterminación informativa se refiere al derecho que posee la persona de decidir qué información personal ofrecer sobre sí misma y que acceso permite sobre la recopilación, recolección o almacenamiento de datos o informaciones de carácter personal que se encuentran en manos de un tercero y que pueden facilitar el que se penetre o conozca aspectos privados y personales del individuo, siendo que aisladamente podría parecer que no tienen ninguna importancia o significación relevante, pero que en conjunto o relacionados entre ellos y con otros datos si lo hacen, afectándose de esa manera los derechos fundamentales como el derecho a la intimidad, a la vida privada, al honor, a la reputación, entre otros. Por lo tanto, se posee un control –que no es ilimitado- sobre esos datos, así como de los archivos contentivos de la información que sobre la propia persona interesada existen o se poseen, en cuanto a su recolección, utilización, almacenamiento, transmisión, entre otros.

que se encuentran relacionados según las circunstancias y los hechos con el habeas data como derecho.

Pero se debe tener presente que el *habeas data* consagrado en el artículo 28 de la CRBV, supone un mecanismo procesal efectivo para propiciar la rectificación de los datos de la persona que se encuentren en registros públicos o privados, cuando no corresponden con la realidad, tratándose de una acción especialmente diseñada para garantizar el derecho constitucional a los datos o información, para acceder, conocer la finalidad, la destrucción, actualización o rectificación de los datos o información que haya sido almacenada con o sin el conocimiento del titular. Además, se debe tomar en cuenta que la jurisprudencia ha declarado improcedente este tipo de acción cuando existe una vía procesal distinta que pueda satisfacer la pretensión del actor, con lo que se observa su carácter residual o subsidiario, como lo sería un juicio contencioso administrativo (Sala Constitucional sentencia N° 2452/01.09.2003), de rectificación de partidas (Sala Constitucional sentencias N° 332/14.03.2001, N° 1306/19.07.2001) o la acción de amparo (Sala Constitucional sentencias N° 565/17.03.2003, N° 2303/21.08.2003, N° 920/15.05.2002 y N° 3001/02.12.2002), siendo que se precisa de una protección mucho más especial y particular para ejercer el *habeas data* (Sala Constitucional sentencia N° 2452/01.09.2003). Por ello, en esta acción, ante la ausencia de otra, se pretende la simple rectificación de un dato personal sin entrar a debatir jurídicamente la procedencia de fondo de dicho cambio, que sería parte de la materia que habría de ventilarse en otro tipo de procesos que van más allá de una simple corrección o rectificación[44].

En este sentido, visto que el actualmente llamado "derecho al olvido" se trata de la facultad que tiene el individuo sobre datos personales para borrarlos, bloquearlos o suprimirlos, cuando contengan información personal que se considere obsoleta por el transcurso del tiempo o que de alguna manera afecte el libre desarrollo de alguno de los derechos fundamentales del sujeto titular del mismo, pareciera entonces que fuese procedente este tipo de acción (*habeas data*) para proteger el derecho a la dignidad, a la intimidad, a la vida privada, a la reputación, al honor, a la imagen, a la salud mental, a la calidad de vida y aun proyecto de vida, a los fines de actualizar o rectificar, la información y la data, siendo que se trata en definitiva de lo mismo, con la única diferencia que el primero se limita al aspecto digital que se encuentra en internet o la red y al aspecto financiero, mientras que el segundo es más amplio.

44 Esta es la opinión de DOMÍGUEZ GUILLÉN, María Candelaria. "Algunas sentencias que declaran el cambio de sexo". *Op. Cit.* pp. 94-97, la cual compartimos plenamente.

III. Derechos y obligaciones que surgen de las partes, los terceros y el Estado ante la publicación del fallo por Internet

Las fuentes del Derecho informático afectan a las ramas tradicionales del Derecho, y en especial en referencia a ciertos aspectos del Derecho público en cuanto: 1) el flujo internacional de datos informatizados, 2) la libertad informática (defensa frente a eventuales agresiones) y 3) los delitos informáticos. En relación al Derecho privado estarían: 1) los contratos informáticos (hardware, software) y 2) la protección jurídica de los programas. No obstante, esto toca todas las demás áreas y materias del derecho aunque sea de forma tangencial.

Incluso hay una discusión de si este derecho es una nueva disciplina o es una serie de normas dispersas que engloba a varias disciplinas, lo cierto es que se relaciona con las ramas del Derecho que se encarga de observar el comportamiento en el ámbito informático que afecte a la sociedad; por eso se necesita una correcta implementación y regularlos adecuadamente a través del estudio y análisis jurídico para su aplicación correcta, con la finalidad de modernizar el Derecho según la forma en que avance la tecnología.

Algunas de las situaciones en las que se hace puede hacer uso indebido del Derecho informático son: 1) en la disposición de un bien, sin el consentimiento del propietario del mismo, realizada mediante equipos informáticos, 2) en el apoderamiento de información contenida en registros electrónicos; 3) en la destrucción o modificación de la información.

Pero también surge una cuestión respecto de la necesidad probatoria cuando se requiera la confidencialidad de un dato, deberá ser resuelta por el juez con base en los parámetros de la lógica y en especial por la merituación de la capacidad de producir daños a las personas en virtud de su difusión a terceros de los datos de que se trate. Resulta un hecho notorio, y por tanto, no debe en principio producirse prueba al respecto, que los datos relacionados con los pensamientos, modos de vida, sentimientos, creencias de los sujetos, pertenecen de modo indubitable a la intimidad de los sujetos, y por tanto, resultan susceptible de exigir la confidencialidad respecto del tratamiento de los mismos y su no difusión a terceros, salvo por causa debidamente autorizada en el ordenamiento jurídico.

Respecto del legitimado pasivo, carga a nuestro entender con el peso de fundamentar los datos por él almacenados, y no se exime de tal responsabilidad por la mera demostración que un tercero le acercó el dato. Esto, cuando se refieren los mismo a información sensible respecto de las personas. Estamos aquí frente a un supuesto de responsabilidad por el manejo de "cosas riesgosas", en razón de la aptitud que poseen tales datos relacionados con la esfera íntima de los sujetos, para provocar daños de magnitud contra los mismos, de ser distorsionados, o simplemente, informados de modo indiscriminado o fuera de contexto.

Así la persona o personas (partes o terceros) afectadas tienen el derecho de ejercer cualquiera de las acciones judiciales mencionadas anteriormente con la finalidad de proteger los derechos constitucionales, fundamentales y humanos mencionados anteriormente para solicitar que sean corregidos, modificados, borrados, omitidos o se guarde su debida reserva en cuanto acceso para proteger sus derechos, salvo en los casos particulares que se mencionó de las personas públicas. Del mismo modo, podrán solicitar que se tomen todas las medidas necesarias de protección de la información que se cargue en la red de internet para que ésta no sea alterada y mantenga su data inalterada, así como demandar cualquier daño o perjuicio de que haya podido ser objeto por la publicación de la misma.

Igualmente, tiene la obligación de que toda la información que suministren y que puede aparecer en la sentencia que se publique por la red, sea cierta y veraz o por lo menos que existan elementos probatorios que permitan considerarla de esa manera.

En cuando a la Administración Pública, tiene el deber de tomar todas las medidas de seguridad de infraestructura, hardware, software y demás aspectos relacionados y que se mencionaran a continuación para tratar de garantizar la inalterabilidad de la información de la data que se publica en internet, así como en caso de que se le solicite acceso a la información darla (en caso que este legitimada la persona por poseer algún derecho subjetivo), para obtener la información y si ésta resulta errónea o inexacta la parte interesada deberá dirigir una carta motivada al ente compilador de datos con miras a solicitar su rectificación, actualización o destrucción.

Por otra parte, en caso que la información suministrada fuese falsa la Administración Pública podrá ejercer las acciones administrativas, civiles y penales correspondientes en contra de quien la hubiese suministrado, ya se trate de una persona individual o colectiva.

IV. Medidas de seguridad informáticas

Para la publicación de las sentencias o cualquier expediente electrónico se han de tomar medidas de seguridad para su protección. Así, la seguridad informática, ciberseguridad o seguridad de tecnología de la información, es el área relacionada con la informática y la telemática enfocada en la protección de la infraestructura computacional y todo lo relacionado con esta, particularmente respecto a la información contenida en una computadora o circulante a través de las redes de computadoras, servidores, nueves, entre otras, para lo cual se utilizan una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información, para la protección del software (metadatos, archivos, bases de datos, entre otros), así como del hardware, redes de

computadoras y todo lo que pueda significar un riesgo si esta información confidencial o sensible o privilegiada llega a manos de otras personas.

Se suele establecer una diferencia entre la seguridad informática que se encarga de la seguridad en el medio informático en cuanto el diseño de las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable; y la seguridad de la información que se refiere a la información que se encuentra en diferentes medios o formas, y no solo en medios informáticos.

Lo que se busca es la seguridad en un ambiente de red identificando y eliminando vulnerabilidades, para salvaguardar la ventaja organizacional, incluyendo información y equipos físicos, tales como las computadoras, todo con la finalidad de minimizar los riesgos a la información o infraestructura informática, como el establecimiento de horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los equipos, los trabajadores y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.

Es importante tener presente que la seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran: 1) *la infraestructura computacional*: que es la usada para el almacenamiento y gestión de la información y para el funcionamiento mismo de la organización, velando por que los equipos funcionen adecuadamente y anticiparse a los fallos como robos, incendios, y cualquier otro factor que atente contra la infraestructura informática; 2) *los usuarios*: que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información, protegiendo el sistema para que en su uso no arriesgue la seguridad de la información y sea vulnerable; y 3) *la información*: que es el principal activo ya que se utiliza y reside en la infraestructura computacional que es empleada por los usuarios.

Además se debe tomar en cuenta que las amenazas no surgen únicamente de la programación y el funcionamiento de un dispositivo de almacenamiento, transmisión o proceso, sino que también hay otras circunstancias que pueden ser imprevisibles o inevitables, como las amenazas producidas por: 1) *los usuarios*: a veces por tener permisos sobredimensionados; 2) *los programas maliciosos*: destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema y que se instala en el ordenador, abriendo una puerta a intrusos o bien modificando los datos a través de un virus informático; 3) *los errores de programación*: que en general representan una amenaza informática para ser usados como exploits por los crakers, aunque en sí mismo es una amenaza; 4) *los intrusos*: que son personas que consiguen acceder a los datos o programas a los cuales no están autorizados como los crackers, defacers, hackers, sript kiddie o scrip boy, viruxers, entre otros; 5) *los siniestros*: como la mala manipulación o mala intención de un robo, un incendio, una inundación o cualquier

otra catástrofe; 6) *el personal técnico interno*: como los técnicos de sistemas, administradores de bases de datos, técnicos de desarrollo, entre otros que producen la vulnerabilidad o intervienen el sistema por motivos de disputas internas, problemas laborales, despidos, fines lucrativos, espionaje o cualquier otra razón; 7) *los fallos electrónicos o lógicos de los sistemas informáticos en general* y 8) *las catástrofes naturales*: como los terremotos, inundaciones, rayos, etc.

Estos ataques pueden ser contrarrestados o eliminados pero hay un tipo de ataque, más complejo de calcular y prever, que no afecta directamente a los ordenadores, sino a sus usuarios, pudiendo conseguir resultados similares a un ataque a través de la red, saltándose toda la infraestructura creada para combatir programas maliciosos, por medio de influencias psicológicas para lograr que los ataques a un servidor sean lo más sencillo posible, ya que el usuario estaría inconscientemente dando autorización para que dicha inducción se vea finiquitada hasta el punto de accesos de administrador.

Otros tipos de amenazas son el *phising* que puede llegar a robar la contraseña de un usuario de una red social y con ella realizar una suplantación de la identidad para un posterior acoso. Igualmente, se puede dar amenazas cuando nos conectamos a una red conectada a un entorno externo (internet) que da la posibilidad de que algún atacante pueda entrar en ella y hurtar información o alterar el funcionamiento de la red aunque este ataque se puede producir dentro de la misma red. Así están: 1) *las amenazas internas*: que pueden ser más serias que las externas, por razones como: a) la realizan usuarios o personal técnico que conocen la red y saben cómo es su funcionamiento, ubicación de la información, datos de interés y otros aspectos, poseyendo algún nivel de acceso a la red por las mismas necesidades de su trabajo y b) los sistemas de prevención de intrusos o *IPS*, y *firewalls* los cuales son mecanismos poco efectivos cuando se trata de amenazas internas por no estar orientados al tráfico interno usualmente; y 2) *las amenazas externas*: que son las que se originan fuera de la red.

En cuanto a las amenazas por el efecto que causan a quien recibe los ataques podría estarían: 1) el robo de información, 2) la destrucción de información, 3) la anulación del funcionamiento de los sistemas o efectos que tiendan a ello, 4) la suplantación de la identidad, publicidad de datos personales o confidenciales, cambio de información, venta de datos personales, etc. y 5) el robo de dinero, estafas.

Las amenazas por el medio utilizado se pueden clasificar por el *modus operandi* del atacante, si bien el efecto puede ser distinto para un mismo tipo de ataque encontrándose: 1) el virus informático o malware; 2) el *phishing*; 3) la ingeniería social; 4) la denegación de servicio y 5) el *spoofing* de DNS, de IP, de DHCP, entre otros.

Los ataques se pueden dar por: 1) *ataque por repetición*: cuando el pirata informático copia una secuencia de mensajes entre dos usuarios y envía tal

secuencia a uno o más usuarios, donde el sistema atacado procesa este comportamiento como mensajes legítimos y producen respuestas como pedidos redundantes; 2) *ataques de modificación de bits*: basadas en las respuestas predecibles de las estaciones receptoras, donde se modifican los bits de un mensaje para enviar un mensaje cifrado erróneo a la estación receptora, y éste se puede comparar entonces contra la respuesta predecible para obtener la clave a través de múltiples repeticiones; 3) *ataques de denegación de servicio* (DOS, Denial of Service):, que consiste en colapsar total o parcialmente a un servidor para que éste no pueda dar respuesta a los comandos (no para sacar de él información y 4) *ataques de diccionario*: dado en ciertos modelos de autenticación de datos que para ingresar al sistema la contraseña se mantiene en secreto, mientras que el nombre de usuario es enviado en forma de texto simple y es fácilmente interceptable, donde se obtienen distintos nombres de usuarios y con ellos, desde un ordenador, empieza a adivinar las contraseñas con base en palabras de diccionarios en distintos idiomas.

Se dice actualmente además de tener como objetivo de los ataques cambiar las plataformas tecnológicas, la nueva modalidad es manipular los certificados que contienen la información digital, lo cual es posible debido a que antes el área semántica era reservada para los humanos, pero ahora es el objeto de los ataques debido a la evolución de la Web 2.0 y las redes sociales, factores que llevaron al nacimiento de la generación 3.0. que otorga contenidos y significados de manera tal que pueden ser comprendidos por las computadoras, las cuales por medio de técnicas de inteligencia artificial son capaces de emular y mejorar la obtención de conocimiento, hasta el momento reservada a las personas, dotando de significado a las páginas Web, y de ahí el nombre de Web semántica o Sociedad del Conocimiento, como evolución de la ya pasada Sociedad de la Información. Por lo tanto las amenazas informáticas ya no son con la inclusión de troyanos en los sistemas o softwares espías, sino que los ataques se han profesionalizado y manipulan el significado del contenido virtual, usando la Web 3.0, provocando así la confusión del usuario y permitiendo la intrusión en los sistemas.

Para evitar estos ataques se recomienda: 1) mantener las soluciones activadas y actualizadas, 2) evitar realizar operaciones comerciales en computadoras de uso público o en redes abiertas, 3) verificar los archivos adjuntos de mensajes sospechosos y evitar su descarga en caso de duda y 5) DMS en el *Data Center*.

Este análisis de riesgo genera habitualmente un documento al cual se le conoce como matriz de riesgo que muestra los elementos identificados, la manera en que se relacionan y los cálculos realizados para lograr una correcta administración del riesgo y la gestión de los recursos de la organización para evitar el riesgo residual y el riesgo total así como también el tratamiento, evaluación y gestión, entre otras.

De allí que se deban asignar estratégicamente los recursos para cada equipo de seguridad y bienes que intervengan, basándose en el impacto potencial,

respecto a los diversos incidentes que se deben resolver, estableciendo prioridades, donde el sistema de gestión de incidentes necesita saber el valor de los sistemas de información que pueden ser potencialmente afectados por incidentes de seguridad, así se pueden distinguir: 1) confidencialidad de la información, la integridad (aplicaciones e información) y 2) la disponibilidad del sistema donde cada uno de estos valores es un sistema independiente del negocio.

Usualmente se busca asegurar los derechos de acceso a los datos y recursos con las herramientas de control y mecanismos de identificación que permiten saber que los operadores tienen sólo los permisos que se les dio, pero sin impedir el trabajo de los operadores, utilizando los firewalls que permiten crear una DMZ donde alojar los principales servidores y relacionándola con Internet sin la utilización de router.

Es indudable que el activo más importante que se posee es la información, por lo que debe existir métodos que la aseguren no solamente de manera física sobre los equipos en los cuales se almacena, sino además debe haber una seguridad lógica a través de la aplicación de *barreras y procedimientos* que resguardan el acceso a los datos y solo permitan acceder a ellos a las personas autorizadas para hacerlo, usando para ello un medio de protección o más como pudieran ser: 1) utilizar técnicas de desarrollo que cumplan con los criterios de seguridad del uso del software que se implante en los sistemas, usando estándares y con personal suficientemente capacitado y comprometido con la seguridad; 2) implantar medidas de seguridad físicas como sistemas contra incendios, vigilancia de los centros de procesos de datos, sistemas de protección contra inundaciones, protecciones eléctricas contra apagones y subidas o bajas de voltajes, sistemas de control de accesos, etc.; 3) codificar la información a través de la criptología, criptografía y criptociencia, en todos aquellos trayectos por los que circule la información que se quiere proteger y no solo en los más vulnerables; 4) usar contraseñas difíciles de averiguar que no puedan ser deducidas y que se cambien con la suficiente periodicidad, siendo complejas, utilizando en tal sentido certificados digitales; 5) vigilar las redes que transportan la información; 6) establecer redes perimetrales de seguridad o DMZ, que permiten generar reglas de acceso fuertes entre los usuarios y servidores no públicos y los equipos publicados; 7) emplear tecnologías repelentes o protectoras como los cortafuegos (firewall), sistemas de detección de intrusos, antispyware, antivirus, llaves de protección de software entre otros; 8) mantener los sistemas de información con las actualizaciones que más impacten en la seguridad; 9) efectuar copias de seguridad y sistemas de respaldo remoto que permiten mantener la información en dos ubicaciones de forma asíncrona y 10) controlar el acceso a la información por medio de permisos centralizados y mantenidos como el Active Directory, LDAP, listas de acceso, por medio de: a) restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos; b) asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión

minuciosa); c) asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido; d) asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro y que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos; e) organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas; f) actualizar constantemente las contraseñas de accesos a los sistemas de cómputo, como se ha indicado más arriba, e incluso utilizando programa que ayuden a los usuarios a la gestión de la gran cantidad de contraseñas que tienen gestionar en los entornos actuales, conocidos habitualmente como gestores de identidad; g) redundancia y descentralización; y h) candado inteligente: USB inalámbrico utilizado para brindarle seguridad a la computadora, que misma se bloquea cuando el usuario que tiene este aparato se aleja más de tres metros.

Por todo lo anterior es importante tener una buena política de copias de seguridad o *backups*, que incluyan copias completas (los datos son almacenados en su totalidad la primera vez) y copias de seguridad incrementales (solo se copian los ficheros creados o modificados desde la última copia de seguridad), elaborando un plan de copias en función del volumen de la información generada y la cantidad de equipos críticos que sea: 1) *continuo* de manera automática, continua, transparente y sin intervenir en las tareas que se encuentra realizando el usuario; 2) *seguro*, con un *softwares* de respaldo que incluya un cifrado de datos hecho localmente en el equipo antes del envío de la información; 3) *remoto*, en que los datos queden alojados en dependencias alejadas de la empresa y 4) con un *mantenimiento de versiones anteriores de los datos*, que permita la recuperación de versiones diarias, semanales y mensuales de los datos.

Debe buscarse la *protección física de acceso a las redes*, de los equipos de una red de área local y el *software* que reside en ellos, con medidas que impidan que usuarios no autorizados puedan acceder, las cuales van a depender del medio físico a proteger utilizando: 1) *redes cableadas*, como lo son las rosetas de conexión de los edificios que deben estar protegidas y vigiladas, evitando tener puntos de red conectados a los switches, listas de control de acceso por MAC addresses, servidores de DHCP por asignación reservada, etc.; 2) con *redes inalámbricas*, con el control físico y con medidas de contención de la emisión electromagnética para circunscribirla a aquellos lugares que se consideren apropiados y seguros, usar medidas de calidad con el uso del cifrado (WPA, WPA v.2, uso de certificados digitales, etc.), contraseñas compartidas y, también los filtros de direcciones MAC; 3) la *sanitización*, como proceso lógico y/o físico mediante el cual se elimina información considerada sensible o confidencial de un medio ya sea físico o magnético, con el objeto de desclasificarlo, reutilizar el medio o destruir el medio en el cual se encuentra; 4) el *uso de hardware confiable*, con dispositivos diseñados para ofrecer una serie de facilidades que permitan manejar de manera segura información crítica

aportando facilidades que mejoran la seguridad y dificultan los ataques; y 5) con la *recopilación y análisis de información de seguridad*, para mantener un sistema con mecanismos que monitoricen los distintos eventos e informaciones que estén relacionados con la seguridad del sistema con una visión centralizada para poderla analizar en una sola ubicación con sistemas de gestión de información de seguridad (**SIM** del inglés *Security information management*), encargados del almacenamiento a largo plazo, el análisis y la comunicación de los datos de seguridad; con sistemas de gestión de eventos de seguridad (**SEM** del inglés *Security Event Management*), encargados del monitoreo en tiempo real, correlación de eventos, notificaciones y vistas de la consola de la información de seguridad, y con sistemas de gestión de eventos e información de seguridad, los cuales agrupan las funcionalidades de los dos tipos de sistemas anteriores.

V. Blockchain

Dentro de los mecanismos de protección señalados anteriormente para evitar que se generen lesiones con la información y data que se encuentra en la sentencia digital o algún expediente digital, se indicó que se debería codificar la misma a través de la criptología, criptografía y criptociencia, en donde aparece e*l Blockchain* (o *cadena de bloques*), que es una de las más interesantes tecnologías en la actualidad, ganando mucho espacio en el mundo de la tecnología *teniendo la ventaja de que posee* la capacidad de hacer que los procesos sean más eficientes, transparentes y seguros, al tratarse de una base de datos distribuida que mantiene un listado de registros, o *bloques,* que está continuamente creciendo, aunado al hecho de que no se puede cambiar la información contenida dentro de un bloque, ya que cada bloque tiene una marca de tiempo y contiene un enlace a un bloque previo, por lo que los Blockchains se comportan innatamente como un inventario digital y público, por lo que es en realidad una forma de estructurar los datos.

Así, este avance de codificación consistente en bloques concatenados de transacciones que permite compartir un libro de contabilidad digital a través de una red de computadoras sin necesidad de una autoridad central, se trata de una base de datos del que todos los que participan en la red guardan una copia, por lo que nadie tiene el poder de manipular los registros y sus algoritmos matemáticos, es lo que preservan la integridad de todas ellas, aunado al hecho de que ninguna persona o compañía o Estado controla la entrada de datos o su integridad, no obstante, el conjunto de la cadena de bloques se verifica constantemente por cada computadora en la red, siendo que todos sus puntos tienen la misma información, por lo que los datos corruptos en el punto "1" no pueden formar parte del Blockchain al no coincidir con los datos equivalentes en los puntos "2" y "3", así su *leitmotiv* es el consenso y si todos esos puntos de la red validan una información es que es veraz, no hace falta un intermediario que lo confirme, por lo que es una forma de codificación de la información y su

funcionamiento es distribuido, un concepto informático algo abstracto que, fundamentalmente da seguridad, veracidad y desintermediación, ya que cuando damos nuestros datos en Internet.

De allí que permite registrar virtualmente cualquier valor que pueda ser expresado digitalmente: certificados de nacimiento, títulos de propiedad, votos, cuentas financieras, sentencias, etc., de forma más rápida, segura y transparente, al ser una base de datos distribuida que se modela, como una *cadena virtual* (electrónica) *de bloques o nodos*, enlazados uno detrás del otro con orden, y cada uno de ellos contiene la información, en la que dos partes pueden realizar una operación entre ellos sin intermediarios, registrarla en un bloque, y todo el mundo puede ver que se ha realizado esa transacción, pero, a la vez, el anonimato de quiénes son los que han intervenido, siendo que al tratarse de una base de datos de solo una escritura, el registro de una transacción no se puede cambiar, haciendo casi imposible cambiar registros históricos, ya que al ser una estructura distribuida, hay muchas copias de los datos, y, de hecho, cuantas más haya, más seguro es.

Por eso entre los usos y ventajas que trae esta tecnología no se limita a establecer un sistema financiero y sistemas criptomonetarios, sino que se puede emplear de otras maneras como la banca y las finanzas (para procesar transferencias y pagos, con la ausencia de intermediarios, reducir el tiempo de liquidación y reducir el costo de procesamiento de pagos globales, a la vez que ofrece una mayor transparencia), los servicios financieros, la salud, los medios de comunicación, el Estado y el gobierno (registro de títulos de la propiedad, identificación, vehículos, licencias, subvenciones, registros sanitarios, tributarios, seguridad pública, entre otros), la ciberseguridad (en las comunicaciones de datos que aseguran la fiabilidad de la fuente, como firma sin llave, reemplazar contraseñas), en los registros académicos, en las votaciones, en la venta y alquiler de vehículos, en el internet de las cosas, los contratos inteligentes o Smart contracts, las previsiones (investigaciones, análisis, consultorías o empresas basadas en la predicción de hechos), la música online, en el transporte y turismo, en el comercio de acciones, en el cuidado de la salud (firmas digitales, historiales médicos), en la fabricación e industria, en la caridad, en la defensa de los sistemas y equipos informáticos, en las ventas al por menor (minorista o *retail*), y para guardar información segura en Internet de forma distribuida.

Esto muestra los beneficios que se pueden llegar a obtener con la implementación de la tecnología blockchain en diferentes áreas de la cotidianeidad como el mundo empresarial, financiero, educativo, de gobierno, entre otros, por lo que en un futuro, probablemente la veamos en casi cualquier actividad que realice el ser humano de manera digital, por lo que aunque no todos estos proyectos se convertirán en empresas de éxito a largo plazo, indican una cosa el enorme potencial que ofrece la tecnología Blockchain, que en su nivel más fundamental es un gran avance en la informática y no es una casualidad ya que se basa en 20 años de investigación en la moneda criptográfica,

y 40 años de investigación en criptografía, por miles de investigadores de todo el mundo. Su potencial es tan considerable que los expertos del sector tecnológico y financiero lo consideran a la altura de las revoluciones tecnológicas que se produjeron con el ordenador personal en 1975 y el internet en 1993, sobre todo al considerar que cualquier ámbito de actividad que requiera registrar datos de forma segura y transparente es susceptible de incorporar las cadena de bloques en su seno.

Entre las ventajas de esta tecnología encontramos: 1) *intercambio sin intermediación de terceros:* el cual es posible entre dos partes sin la intermediación o supervisión de terceros, reduciendo riesgos considerablemente; 2) *fortaleza y fiabilidad:* este sistema puede resistir ataques maliciosos mucho mejor que otro, ya que carece de punto central débil, al utilizarse redes descentralizadas; 3) *datos de alta calidad:* los datos están disponibles ampliamente, son exactos, privados, completos y llegan siempre a tiempo, mejorando la integridad de los datos; 4) *usuarios más capacitados:* los usuarios pueden controlar todas sus transacciones e información; 5) *integridad del proceso:* los usuarios pueden tener la tranquilidad de que sus transacciones serán ejecutadas exactamente como marque el protocolo, sin necesidad de que supervisen terceros; 6) *transparencia e inmutabilidad:* cualquier modificación a Blockchains públicos puede ser vista abiertamente por cada parte, asegurando transparencia. Cada transacción es inmutable; no puede ser eliminada o modificada; 7) *simplificación del sistema contable:* al añadir cada transacción a una simple contabilidad pública, reducimos la complejidad de múltiples contabilidades; 8) *transacciones eficientes:* otorga mayor seguridad, rapidez y eficacia, lo cual la hace más productiva y permite que se reduzcan gastos generales y costes intermediarios innecesarios, al requerir menos seguimiento y control; 8) En internet, puede permitir que los *servidores de dominio pasasen del control de gobiernos y empresas a un control descentralizado*, pudiendo basarse de los PKI para la emisión de certificados digitales, a los KSI y 9) *servicios en la nube*: supondría el paso de un almacenamiento centralizado a uno descentralizado, lo cual ya ha sido implantado por empresas como Storj, en la que los usuarios con espacio libre en sus discos, pueden alquilarlo automáticamente, y los que lo necesitan almacenar sus archivos en los discos de otros mediante compensación.

Estos son solo algunos ejemplos de todo lo que se puede hacer con *blockchain*, donde el límite, como con cualquier tecnología novedosa, es la imaginación, tanto así, que Microsoft y muchas otras empresas grandes ya ofrecen alojar servicios de *blockchain* en sus nubes particulares, por lo que los avances tecnológicos pueden ser un terremoto de algunos modelos de negocio.

Conclusiones

En definitiva, los derechos humanos son la proyección jurídica de la dignidad de la persona y la condición de su desarrollo, lo cual a su vez subraya la dimensión individual de los mismos, los cuales deben ser protegidos por todos los Estados y naciones, vinculados estrechamente con la dignidad del ser humano y dentro de los cuales se encuentra una variedad y categoría de los mismos que se hallan especialmente vinculados como los derechos al libre desarrollo de la personalidad, de la personalidad, a la libertad, a la intimidad, a la vida privada y a la propia imagen, a la integridad psicofísica y moral, al honor y a la reputación.

Ante la universalización y globalización del internet y los accesos a la red, que contiene una enorme capacidad de almacenaje de información y posee importantes motores de búsqueda de información que permiten localizar cualquier dato en cuestión de segundos, y con gran facilidad, hace difícil que quede en el olvido cualquier información que se coloque allí, lo cual le da un carácter casi de perennidad a la misma que genera nuevos desafíos para el derecho, en cuanto a determinar si una persona puede lograr borrar esa información, de qué manera y ante quien, aunque usualmente la solicitud de reclamo para la eliminación de esos datos se dirigen contra el medio original que lo contiene, el sitio de internet, en donde se encuentra publicado o el motor de búsqueda que indica donde hallarla, debiéndose evaluar cada solicitud de forma individual, para buscar un equilibrio entre los derechos de privacidad de los usuarios y el derecho del público a conocer y distribuir información, examinando si los resultados incluyen información obsoleta sobre el solicitante, así como si existe interés público por esa información, como lo sería la ejemplo información sobre estafas financieras, negligencia profesional, condenas penales o comportamiento público de funcionarios del gobierno.

Así, surge el derecho a la protección de los datos personales, por lo que se entiende como la facultad que tiene el individuo sobre los mismos para borrarlos, bloquearlos o suprimirlos, cuando contengan información personal que se considere obsoleta, errónea, falsa o lesiva por el transcurso del tiempo o que de alguna manera afecte el libre desarrollo de alguno de los derechos fundamentales del sujeto titular del mismo, tratándose, a nuestro entender, de un derecho vinculado especialmente con el mundo informático.

De este modo, vemos que los particulares pueden pedir el retiro de informaciones que les conciernan y que ya no son pertinentes, como las sentencias y expedientes digitales, salvo en el caso que exista un interés público o se trate de una persona pública, como los políticos o las personas célebres, sin que ello signifique una discriminación y violación al derecho a la igualdad, ya que por el contrario, en razón de ser personas públicas, todo lo vinculado con ellos es público y no pueden alegar este derecho a su favor, ya que renunciaron de manera tácita, en cierta forma a ello, salvo en el caso de ciertos límites que afecten el núcleo esencial de algún derecho humano que les concierna.

No obstante, el reconocimiento de este derecho y la posibilidad de la eliminación de los datos, ello no significa que desaparezca completamente la data de la red, ya que aunque el buscador respectivo elimine el vínculo indicado, la información podría ser ubicada en algún buscador que no fuera objeto de la solicitud de retiro de la información o en alguna dirección de la red que posea la información que se quiere eliminar.

Igualmente se pueden presentar dificultades en los casos de homonimia, siendo que se solicite la eliminación de un dato o información alegando que es propio cuando no lo es, ya que la página señalada puede concernir a un homónimo, lo que será difícil de verificar por el buscador respectivo. También puede surgir la dificultad de determinar cuándo una persona es "pública" y por ende no tiene derecho a solicitar que se borre la información contenida sobre ella, o si dejo de ser funcionario público, si es pertinente que con esa posterioridad se borre la información respectiva. Del mismo modo, es complicado el establecer al cabo de qué plazo una información pasa a no ser pertinente y también es difícil establecer quién es el responsable. Finalmente, se puede presentar la dificultad de establecer un equilibrio entre el derecho a la información y los derechos de los individuos.

Por lo tanto, pareciera, que no va existir por ahora una solución fácil y absoluta a este nuevo tipo de reputación electrónica, aunque se trata de un avance en una primera etapa que involucra los buscadores y que posteriormente seguramente incluirá las redes sociales y páginas web en particular, para poder tratar de alcanzar el verdadero derecho al olvido que es la supresión del contenido.

Lo innegable es que la revolución tecnológica en la que estamos inmersos en el presente, junto con los continuos progresos en el campo de las ciencias informáticas, ha hecho posible, entre otras cosas, la creación, acceso y entrecruzamiento de enormes bancos de datos con todo tipo de informaciones, por lo que es el sustrato cultural del cual surge la necesidad de contar los ciudadanos con un medio de protección sobre lo que se almacene como información de su vida y los más diversos aspectos de su personalidad.

De esta manera en todos los estados democráticos o no, cada día es mayor el caudal de datos referentes a los habitantes del país que se almacena en bancos de datos estatales y privados, así como existen cada vez más posibilidades de acceder y cruzar datos de múltiples fuentes de almacenamiento, por lo que de este incremento en magnitud y calidad, surge la posibilidad de que tales datos sean incorrectamente asentados, procesados o difundidos, con el correspondiente menoscabo para la intimidad o imagen personal, ya sea de parte del sector público o privado, por lo que la intimidad ha sido erosionada por la revolución tecnológica, y en especial por el exponencial desarrollo que se viene experimentando la informática en los tiempos actuales.

De allí que se plantee un conflicto entre la "privacidad vs. información", que obliga buscar respuestas adecuadas en vistas a asegurar una convivencia armónica y el correcto uso de la información almacenada que esta tutelada por

las normas constitucionales, por lo que debe impedirse las intromisiones que perturben o se difundan de manera inadecuada los datos procesados mediante los modernos adelantos tecnológicos que pueden afectar a estos y hacer ilusorias las garantías constitucionales, por lo que está el habeas data, para proteger de los abusos e intromisiones que puedan afectarla y que nazcan de la manipulación de la información, resguardando la verdad, a la autodeterminación informativa, a la intimidad, a la privacidad, a la voz a la imagen, a los valores familiares, al honor, al patrimonio, entre otros, todo dentro de un marco protector de la libertad y de la dignidad humana, así como tomar todas las medidas de seguridad necesarias para proteger la data que se coloque en la red, como la publicación de un fallo digital.

La libertad a la información veraz no es un derecho absoluto, sino que hay que ponerlo en relación con otros derechos fundamentales, como lo es en este caso, el derecho fundamental a la protección de datos, la intimidad, secreto de las comunicaciones, imagen, honor, reputación, integridad física y moral, por ello ninguna persona que no tenga la condición de personaje público ni sea objeto de hecho noticioso de relevancia pública tiene que resignarse a soportar que sus datos de carácter personal circulen por la red de internet sin poder reaccionar ni corregir la inclusión ilegítima, errónea o caduca de los mismos en un sistema de comunicación mundial como es este. Además, las personas no están obligadas a someterse al ejercicio de las libertades de expresión e información de otras personas en referencia a ellas, sino que debe gozar de mecanismos y acciones que le permitan ejercer sus derechos que impidan el mantenimiento en la internet de esa información de carácter personal.

Sin embargo, tampoco es que el acceso a la información de estas personas sea ilimitada, sino que por el contrario tiene límites, cuando se trate de ese núcleo duro o esencial del derecho a la intimidad, honor, reputación, imagen, entre otros derechos a los que hicimos referencia anteriormente, en donde aunque se trate de personas socialmente expuestas y funcionarios públicos, tienen derecho a la protección de sus derechos humanos, al igual que requieren de protección si posteriormente dejan de tener esa condición en relación a los hechos que ocurran con posterioridad a dejar de serlo.

Responsabilidad de las personas jurídicas ante la comisión de delitos informáticos

Emy Noremy Rivero Núñez*

SUMARIO: Introducción. 1. Elementos de la responsabilidad penal de las personas jurídicas. 1.1. Personalidad jurídica. 1.2. Tesis en contra de la responsabilidad penal de las personas jurídicas. 1.3. Tesis a favor de la responsabilidad penal de las personas jurídicas. 1.4. Posición. 2. Tipos penales establecidos en la Ley Especial contra los Delitos Informáticos vinculados con la participación como sujeto activo de la persona jurídica. 3. Consecuencias de la responsabilidad penal de las personas jurídicas en el desarrollo de sus actividades. Conclusiones.

Resumen

La responsabilidad penal de las personas jurídicas, entendidas como sujetos de derechos y obligaciones, ha sido objeto de múltiples posiciones doctrinarias, unas a favor y otras en contra. En Venezuela se sigue la posición de que tienen responsabilidad penal, siempre que se den las condiciones fijadas por el legislador. La Ley Especial Contra los Delitos Informáticos prevé este tipo de responsabilidad bajo los parámetros que serán analizados en el siguiente estudio.

Palabras claves: Responsabilidad penal. Personas jurídicas. Delitos informáticos.

Recibido: 21/11/2019 • Aceptado: 19/12/2019

* Abogada Magna Cum Laude, egresada de la Universidad de Los Andes, Especialista en Derecho Procesal Penal por la Universidad Fermín Toro, Especialista en Ejercicio de la Función Fiscal por la Escuela Nacional de Fiscales, Especialista en Ciencias Penales y Criminológicas por la Universidad Experimental Rómulo Gallegos, Especialista en Derecho Probatorio en la Escuela Nacional de Fiscales y cursando el Doctorado en Derecho en la Universidad Católica Santa Rosa. Se desempeña como Fiscal Cuarta para actuar ante la Sala Plena, Constitucional y Salas de Casación del Tribunal Supremo de Justicia.

Abstract

The criminal liability of legal entities, understood as subjects of rights and obligations, has been analyzed from multiple doctrinal positions, some in favor and others against. In Venezuela the position that they have criminal liability is followed. This kind of liability occurs when the conditions established by the legislator are met. The Special Law Against Computer Crime provides this type of liability under the parameters that will be analyzed in the following study.

Keywords: Criminal Liability. Legal entities. Computer Crimes.

Introducción

Desde el nacimiento de las personas jurídicas, como sujetos de derechos y obligaciones, se ha planteado la discusión sobre la responsabilidad penal de su actuación, generándose dos posiciones contrarias, la primera de ellas, afirma que es imposible sancionar a la persona jurídica, por cuanto ésta no tiene voluntad. Conforme a esta posición, aunque la persona jurídica tiene una personalidad propia, diferente a la de las personas naturales que la conforman y que le permite realizar actividades en el mundo jurídico, no poseen voluntad autónoma, siendo éste el tradicional paradigma en virtud del cual se les negaba toda aptitud de responsabilidad penal, resumido en el apotegma *societas delinquere non potest* (las personas jurídicas no puede ser sujetos activos de delitos).

En segundo lugar, se encuentra la posición que asevera la necesidad de castigar a la persona jurídica, por cuanto su voluntad se deriva de la actuación de quienes efectúan sus propósitos, utilizando los activos de la empresa y generando una ganancia que va al patrimonio de la empresa. En esta visión de la dogmática del Derecho penal, se hace necesaria una revisión de los elementos que conforman el delito, los cuales han sido diseñados para la persona natural, pero que pueden ser adaptados a las personas jurídicas, no con identidad material sino funcional, surgiendo así la teoría de la responsabilidad objetiva, esto es, de una responsabilidad que no admite que el sujeto pueda eximirse de la misma observando un cierto tipo de comportamiento.

Así las cosas, es importante mencionar que en Venezuela se han dictado varias normas de carácter penal que establecen la responsabilidad penal de las personas jurídicas, siendo estas: la Ley Especial contra los Delitos Informáticos[1],

1 Publicada en la Gaceta Oficial Ordinaria No. 37.313 del 30 de octubre de 2001.

la Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo[2] y la Ley Penal del Ambiente[3].

En ese sentido, resulta relevante analizar la responsabilidad de las personas jurídicas ante la comisión de delitos informáticos, para lo cual se examinarán los elementos de la responsabilidad penal de las personas jurídicas, para luego describir los tipos penales establecidos en la Ley Especial contra los Delitos Informáticos vinculados con la participación como sujeto activo de las personas jurídicas, para finalmente determinar las consecuencias de la responsabilidad penal de las personas jurídicas en el desarrollo de sus actividades.

1. Elementos de la responsabilidad penal de las personas jurídicas

Para precisar los diversos elementos que configuran la responsabilidad de las personas jurídicas, es importante verificar los siguientes aspectos:

1.1. Personalidad jurídica

En ese sentido, es pertinente traer a colación la afirmación de Francisco Ferrara[4], las personas jurídicas pueden definirse como asociaciones o instituciones formadas para la consecución de un fin y reconocidas por la ordenación jurídica como sujetos de derecho.

De la cual se determina que las personas jurídicas pueden tener diversas formas, que su constitución es con una finalidad específica y que son amparadas por el ordenamiento jurídico, otorgándoles derechos y obligaciones, es decir, haciéndolas susceptibles de tener responsabilidad.

Por otra parte, María Domínguez[5] señala que la persona jurídica en sentido estricto o persona incorporal se traduce en la atribución de personalidad jurídica a entes distintos al ser humano. Es pues la consecución legal de la condición de sujeto de derecho a entes ideales.

De estas concepciones, se deriva que la persona jurídica no es una ficción pero tampoco es una persona real, sino que el ordenamiento jurídico le otorga derechos y garantías, en ese entender, serán personas jurídicas, todos aquellos entes susceptibles de ser sujetos de derechos.

En ese mismo sentido, el Código Civil[6] prevé la regulación, no solo de las personas naturales, sino de las personas jurídicas o morales, estableciendo en el artículo 19, que son sujetos de derechos y obligaciones, convirtiéndolas en sujetos

2 Publicada en la Gaceta Oficial Ordinaria No. 39.912 del 30 de abril de 2012.

3 Publicada en la Gaceta Oficial Ordinaria No. 39.913 del 02 de mayo de 2012.

4 Francisco FERRARA: *Teoría de las Personas Jurídicas*. Colección Grandes Maestro del Derecho Civil. Volumen 4. Editorial Jurídica Universitaria. México. 2008. P. 141.

5 María Candelaria DOMÍNGUEZ GUILLEN, *Derecho Civil I. Personas*, Ediciones Paredes Libros Jurídicos, año 2011.

6 Publicado en Gaceta Oficial Extraordinaria N° 2990 del 26 de julio de 1982.

de derecho y por ende en entes capaces de tener responsabilidad, de cualquier naturaleza, asimismo, efectúa una clasificación de las diversas formas de organización, desde las de Derecho público como son la Nación y las entidades políticas que la componen, las iglesias de cualquier religión, las universidades y por último señala las de Derecho privado como las asociaciones, fundaciones y corporaciones.

En ese mismo entender, siguiendo a Allan Brewer-Carias (2001, 4)[7], se determinará responsabilidad penal a "…las personas jurídicas de Derecho privado, que comprenden las asociaciones, entre las cuales se destacan las sociedades civiles y sociedades mercantiles, las corporaciones y las fundaciones lícitas". Conforme a ello, son susceptibles de imposición de sanciones, por la comisión de delitos previstos en la Ley, los entes de carácter privado.

Se trata, principalmente de las empresas que en el desarrollo de sus actividades empresariales, efectúan acciones que en general son lícitas, pero en el marco de evolución de sus facultades pueden cometer hechos que sean subsumibles en tipos penales, sea a objeto de obtener beneficios adicionales personales o para la propia empresa, como aminorar costos de producción u obtener mayores ganancias.

En ese sentido, como señala Feijoo[8], las organizaciones empresariales constituyen una realidad que debe ser tratada como un todo y no solo como un conjunto de sujetos, lo que conlleva a plantearse la necesidad de que le sea determinada responsabilidad jurídico penal por su accionar.

Conforme a esa afirmación, es el Estado, en el uso de su poder punitivo, el que establece cuáles conductas puedan atentar contra la sociedad y que deban ser penalmente sancionables, ello para prevenir la conculcación de bienes jurídicos protegidos, que puedan verse afectados por el accionar o funcionamiento de las empresas.

En ese particular, Missas[9] afirma que las organizaciones constituyen el eje de la economía y desarrollo de cualquier nación, lo que hace que influya en todos los ámbitos sociales y que su funcionamiento sea regulado desde distintas áreas del Derecho, a saber, civil, administrativo, mercantil, entre otros; siendo necesario que desde el Derecho penal, también sea establecida la responsabilidad penal de la persona jurídica, cuando sus acciones violenten algún bien jurídico tutelado.

7 Allan BREWER-CARIAS: Sobre las personas jurídicas en la Constitución de 1999: https://allanbrewercarias.com/.../473.-440.-SOBRE-LAS-PERSONAS-JURÍDICAS-EN [consulta: 2019. Julio 26]

8 B. FEIJO: "Autorregulación y Derecho Penal de la Empresa: ¿Una Cuestión de Responsabilidad Individual?". En: Arroyo Jiménez y Nieto Martín (directores.), *Autorregulación y Sanciones.* (1ra.ed.). Valladolid, España. Editorial Lex Nova. 2008.

9 Jorge MISSAS: "La responsabilidad penal de las personas jurídicas en Colombia, problemáticas sobre su aplicación desde la expedición del Código Penal". *Revista Criterio Jurídico.* Santiago de Cali. Colombia. 2017. p. 100.

De lo cual se deriva que le corresponderá al Estado verificar si hay necesidad o no de criminalizar ciertas conductas o actividades efectuadas por las corporaciones y si constituye el Derecho penal la última razón para reprochar o prevenir tal acción.

1.2. Tesis en contra de la responsabilidad penal de las personas jurídicas

Con la creación de las personas jurídicas y su tratamiento como sujetos de derechos, es decir, titulares de derechos y obligaciones, surge la posibilidad de que sean responsables penalmente de la comisión de delitos, generándose dos posiciones encontradas, una de ellas afirma que es imposible sancionar a la persona jurídica, por cuanto ésta no tiene voluntad. En esta visión de pensamiento Meier[10] afirma que apoya la tesis de Savigny, referente a que las personas jurídicas son meras "ficciones jurídicas", creadas por el Derecho para cubrir ciertas necesidades, intereses y fines de las personas naturales y que constituyen prolongaciones de estas.

En ese sentido, aunque la persona jurídica tiene una personalidad propia, diferente a la de las personas naturales que la conforman y que le permiten realizar actividades en el mundo jurídico, no poseen voluntad autónoma, siguiendo a Rosa Díaz[11] "por cuanto esta carece de voluntad y si no hay voluntad no hay acción penalmente relevante"; siendo este el tradicional paradigma en virtud del cual se les negaba toda aptitud de responsabilidad penal, resumido en el apotegma *societas delinquere non potest* (las personas jurídicas no puede ser sujetos activos de delitos).

1.3. Tesis a favor de la responsabilidad penal de las personas jurídicas

Por otra parte, se encuentra la posición que asevera la necesidad de castigar a la persona jurídica, por cuanto su voluntad se deriva de la actuación de quienes efectúan sus propósitos, utilizando los activos de la empresa y generando una ganancia que va al patrimonio de la empresa, de allí que Henrique Meier[12], afirme que la teoría de la realidad de Gierke, que vislumbra a la persona jurídica como una unidad capaz de intervenir en la vida jurídica en nombre propio, por cuanto es una persona real, conformada por personas naturales que actúan de

10 Henrique MEIER: "Las empresas y La Ley Penal del Ambiente". I Jornadas de Derecho Corporativo. Puerto La Cruz, Venezuela. https://dialnet.unirioja.es/descarga/artículo/3999478.pdf 2001[consulta: 2019. Julio 26].

11 Rosa María DIAZ: "La Responsabilidad Penal de las Personas Jurídicas". *Revista Ministerio Público* N° 5. Caracas, Venezuela. 2006. p.6.

12 H. MEIER: "Las empresas y La Ley Penal del Ambiente". ...*Op. Cit*., p. 5.

forma única y con una fuerza de voluntad común para conseguir lo fines de la organización que trasciende los intereses individuales.

Desde la doctrina del Derecho penal, se precisa una adecuación de los elementos del delito con la finalidad de adaptarlos a las personas jurídicas, para que puedan funcionar, naciendo la teoría de la responsabilidad objetiva, esto es, que no permite que el sujeto pueda eximirse de la misma observando un cierto tipo de comportamiento.

En ese sentido, se han establecido diversos sistemas de responsabilidad, a saber: a) Modelo de responsabilidad penal indirecta de la persona jurídica, que hace mención conforme señala Elienai González[13] (2013, p. 72) "imputa a la corporación el injusto y la culpabilidad a su representante" y b) Modelo de responsabilidad penal propia o directa de las personas jurídicas, que prevé que la persona jurídica debe ser tratada igual que la persona natural y que corresponde al Derecho penal tratarlas de forma idéntica.

En referencia a este punto, es preciso resaltar lo previsto en la Sentencia N.º C-320/98, emanada de la Sala Plena de la Corte Constitucional de Colombia[14] la cual dejó plasmada la necesidad de establecer la responsabilidad penal de las personas jurídicas, siendo uno de sus fundamentos el significado educativo de la pena, tanto de manera preventiva como sancionatoria, por cuanto la sanción penal impuesta a la persona jurídica, la expone a la censura social, y la muestra como autora del delito y no como una víctima de sus órganos de decisión, por lo que debe ser sancionada.

En ese sentido, si se tiene que a la persona jurídica le pueden ser reprochables penalmente las conductas que infrinjan bienes jurídicos, se genera la situación de cómo aplicar la pena a este ente, unas posibles soluciones nacen basadas en la finalidad preventiva de la pena y otras en la posición retributiva de la misma.

Como se ha expresado, la expectativa de la responsabilidad penal de las personas jurídicas ha suscitado numerosos debates tanto en el ámbito jurídico como empresarial, social, e inclusive, ético y moral.

A partir del aforismo *societas delinquere non potest*, prevaleciente en el pasado, hoy en día, se plantea el problema de las empresas, que en el desarrollo de sus actividades, ocasionan daños a las personas y comunidades, afectando sistemas de información, accediendo a ellos y modificando la data, entre otros, simplemente buscando lucrarse.

En pro del aforismo, esto es, de la irresponsabilidad de la persona jurídica, se han esgrimido diversos argumentos, como que la persona jurídica no tiene

13 Elienai GONZÁLEZ: "La responsabilidad penal de las personas jurídicas y sus implicaciones político criminales". *Revista del Ministerio Público. V Etapa*, Nº 3. Caracas, Venezuela. 2013. p.72.

14 Sala Plena de la Corte Constitucional de Colombia, sentencia N.º C-320/98, 30 de junio de 1998, donde resuelven las Objeciones presidenciales al proyecto de Ley 235/96 Senado-154/96 Cámara, "por el cual se establece el seguro ecológico, se modifica el Código Penal y se dictan otras disposiciones".

capacidad de obrar, por tanto no puede determinarse su culpabilidad, aunado a la imposibilidad de ser sujeto de una pena, ya que las sanciones de las que puede ser objeto siempre serán económicas, por lo cual serán impuestas en sede administrativa y nunca penal.

Tal vez, en épocas que parecen ya remotas, la solidez argumental del *societas delinquere non potest* era irrebatible. Sin embargo, en la época actual, sin abandonar el aforismo, ha surgido una especie de responsabilidad penal "lato sensu" de las personas jurídicas, denominada por Arteaga[15], (2007, p. 212) como una responsabilidad *sui generis*.

Si bien antes era inconcebible imputar, en sede penal, los daños producidos por la actividad de una persona jurídica, ese punto de vista ha variado. A favor de la variación, está la constatación de que, en muchos casos, no es suficiente imponer multas u otras sanciones administrativas.

En ese sentido, la cuantía de los perjuicios causados, la reiteración de prácticas nocivas, la indiferencia de los propietarios, personal directivo y gerencial, la ineficacia de las sanciones administrativas, el clamor de los afectados, la presión de organizaciones no gubernamentales, son factores que han obligado a los países a celebrar tratados y convenciones, a promulgar leyes que consagren normas sancionadoras de las conductas desplegadas, no solo por los operarios, a título individual, sino a la propia persona moral, por su autoría, instigación y participación en la realización de tales actividades, que afectan el orden económico, social, cultural, ambiental, entre otros.

1.4. Posición

Dentro de esa dinámica, la legislación patria en la Ley Especial contra los Delitos Informáticos[16], prevé en su artículo 5 la responsabilidad penal de las personas jurídicas, en los siguientes términos:

> Artículo 5. Responsabilidad de las personas jurídicas. Cuando los delitos previstos en esta Ley fuesen cometidos por los gerentes, administradores, directores o dependientes de una persona jurídica, actuando en su nombre o representación, éstos responderán de acuerdo con su participación culpable.
> La persona jurídica será sancionada en los términos previstos en esta ley, en los casos en que el hecho punible haya sido cometido por decisión de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en su interés exclusivo o preferente.

15 Alberto ARTEAGA SÁNCHEZ: *Derecho Penal Venezolano.* Caracas: Liber. 2007. p. 212.

16 Publicada en la Gaceta Oficial Ordinaria No. 37.313 del 30 de octubre de 2001.

Fijándose entonces como elementos de la responsabilidad penal de las personas jurídicas, conforme a lo previsto en la ley especial, los siguientes: decisión de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en su interés preferente.

Del cual se deriva, que la responsabilidad penal de las personas jurídicas, obedece a criterios de política criminal, es decir, a la necesidad del Estado de establecer parámetros claros para prevenir y sancionar delitos, en protección de los bienes jurídicos tutelados, ya que solo desde esta perspectiva se pueden establecer conductas que le sean imputables, y no desde una construcción válida del Derecho penal.

En ese sentido, la acción ejecutada será efectuada por la persona física, es decir por las personas capaces de comprometer a la empresa, que conforme a la redacción de la ley especial, también tienen responsabilidad, pero basta con que haya sido cometido por decisión de sus órganos, lo que compromete a la misma, siendo esto equiparado a la culpabilidad de la persona moral.

Siguiendo lo afirmado por Pérez[17] (2013, p. 108) referente a que la responsabilidad penal de las personas jurídicas no se basa en hechos propios, sino en acciones efectuadas por personas naturales específicas, de allí que la conducta no ha sido realizada por el ente moral, violentándose de esa manera el principio de culpabilidad.

Conforme a esta apreciación, será solo la persona física la que cometa o ejecute el hecho, pero el mismo será por disposición de la persona moral, siempre que de alguna manera esta se vea beneficiada.

Este sistema de atribución de responsabilidad, llamado de doble vía, (en este caso referido a la doble autoría) se circunscribe a los supuestos delitos que se cometan, por un lado, en nombre o por cuenta de la misma, y en su interés (entendido como el provecho directo, beneficio, o indirecto, ahorro de costos), por los gerentes, administradores o directores (la llamada responsabilidad del hecho personal por representación o tesis del reflejo) y, por otro, por los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en provecho de la persona jurídica, por sus dependientes o empleados.

Determinada la necesidad de que una persona física cometa el delito para atribuir la responsabilidad penal a la persona jurídica, se debe verificar el criterio subjetivo/personal establecido en el artículo 5 de la Ley Especial contra los Delitos Informáticos[18], esto es, qué personas físicas concretas son capaces para trasladar la responsabilidad. El referido artículo establece dos grupos de personas; así, de un lado, los delitos cometidos por los representantes legales y administradores y, de otro, los cometidos por los dependientes o personas sometidas a la autoridad de la persona jurídica.

17 Jacinto PÉREZ: *Sistema de atribución de responsabilidad penal a las personas jurídicas.* Universidad de Murcia. Murcia, España. 2013. p.108.

18 Publicada en la Gaceta Oficial Ordinaria No. 37.313 del 30 de octubre de 2001.

Conforme a lo antes señalado, será entonces la acción desplegada por las personas físicas, que puedan comprometer a la persona jurídica, las que traspasen su responsabilidad a la persona jurídica, siempre que se den los supuestos previstos en el referido artículo 5 de la ley especial.

2. Tipos penales establecidos en la Ley Especial contra los Delitos Informáticos vinculados con la participación como sujeto activo de la persona jurídica

La Ley Especial contra los Delitos Informáticos, publicada en fecha 30 de octubre de 2001, mediante Gaceta Oficial N° 37.313, establece los tipos penales que afectan o atentan contra los sistemas que utilicen tecnologías de información, las penas principales y accesorias a ser aplicables, las circunstancias que agravan las sanciones y como innovación la responsabilidad de las personas jurídicas.

Está estructurada en cuatro títulos, el primero de ellos, referente a las disposiciones generales, un segundo título, que consagra los delitos, subdividido a su vez en cinco capítulos, que prevén los diversos bienes jurídicos a ser protegidos por las conductas tipificadas; el tercer título referido a las disposiciones comunes y por último, el título cuatro, denominado de las disposiciones finales.

En el título primero, llamado disposiciones generales, puntualiza el objeto de la ley, en los siguientes términos:

> Artículo 1. Objeto de la Ley. La presente Ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los delitos cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta Ley.

Del cual se deduce que la intención de la norma es garantizar la protección a los sistemas que utilizan tecnologías de información y lograr la sanción de todos aquellos tipos penales que atenten contra los referidos sistemas o que se ejecuten usando como medio de comisión la tecnología.

Continúa la norma efectuando unas definiciones de términos básicos para la comprensión de su articulado, los tipos de sanciones a imponer, siendo clasificadas en principales y accesorias, las cuales podrán ser concurrentes o no, dependiendo de las circunstancias que rodeen el delito cometido y la responsabilidad de las personas jurídicas en la comisión de los tipos penales previstos en la presente ley.

En cuanto al título II denominado de los delitos, se configura en varios capítulos, cada uno denominado conforme al bien jurídico que protegen, así las cosas está estructurado de la siguiente manera:

Capítulo I **Contra los sistemas que utilizan tecnologías de información**	**Capítulo II** **Contra la propiedad**	**Capítulo III** **Contra la privacidad de las personas y de las comunicaciones**	**Capítulo IV** **Contra niños y adolescentes**	**Capítulo V** **Contra el orden económico**
Acceso indebido (Art.6)	Hurto (Art. 13)	Violación de la privacidad de la datao información de carácter personal (Art. 20	Difusión o exhibición de material pornográfico (Art. 23)	Apropiación de propiedad intelectual (Art. 25)
Sabotaje o daño a sistemas (Art.7)	Fraude (Art. 14)	Violación de la privacidad de las comunicaciones (Art. 21)	Exhibición pornográfica de niños o adolescentes (Art. 24)	Oferta engañosa (Art. 26)
Favorecimiento culposos del sabotaje o daño. (Art. 8)	Obtención indebida de bienes o servicios (Art. 15)	Revelación indebida de data o información de carácter personal (Art. 22)		
Acceso indebido o sabotaje a sistemas protegidos (Art. 9)	Manejo fraudulento de tarjetas inteligentes o instrumentos análogos (Art. 16)			
Posesión de equipos o prestación de servicios de sabotaje (Art. 10)	Apropiación de tarjetas inteligentes o instrumentos análogos (Art. 17)			
Espionaje informático (Art. 11)	Provisión indebida de bienes o servicios (Art. 18)			
Falsificación de documentos (Art. 12)	Posesión de equipo para falsificaciones (Art. 19)			

Fuente: La autora (2019).

En ese sentido, de la revisión de los delitos consagrados en el Capítulo I denominado contra los sistemas que utilizan tecnologías de información, al verificar los siete (07) tipos penales, pareciera que cualquiera de ellos le podría ser imputado a una persona jurídica, sin embargo, al contrastarlos con las circunstancias concurrentes para que surja la responsabilidad penal de las personas jurídicas, en los casos de los delitos de acceso indebido y favorecimiento culposo del sabotaje o daño, faltaría uno de los mismos, en el primer caso el interés exclusivo o preferente para la empresa y en el segundo caso, la decisión del órgano de efectuar la acción típica.

Asimismo, con respecto al resto de los delitos consagrados en este capítulo, parecieran ser los ideales para que sean ejecutados en favor de una persona jurídica, en especial el de espionaje informático, que reportaría en posicionamiento de la empresa al manejar la información de sus competidores comerciales, otorgándole ventajas en las negociaciones y acuerdo mercantiles.

En referencia a los siete (07) tipos penales previstos en el Capítulo II contra la propiedad, en principio cualquiera de ellos le podría ser imputable a la organización, ya que tienen por norte la protección del bien jurídico propiedad y como objetivo la obtención de un beneficio de cualquier naturaleza para la empresa.

Ahora bien, los tres (03) delitos pautados en el Capítulo III contra la privacidad de las personas y de las comunicaciones, pareciera que pueden ser determinantes de la responsabilidad penal de las personas morales, ya que le permiten poseer una información privilegiada, por ejemplo en el caso de lo previsto en el artículo 22, al dar a conocer alguna información reservada de sus competidores, puede generarse una baja del valor de mercado de esa empresa.

De la revisión de los dos (02) tipos penales descritos en el Capítulo IV contra niños y adolescentes, en principio pareciera ilógico que alguna empresa vaya a incurrir en la comisión de alguno de los delitos, pero dependerá de la organización y sus fines.

Por último, lo pautado en el Capítulo V contra el orden económico, que prevé dos (02) delitos, pueden ser perfectamente imputables a un ente corporativo, por cuanto de su análisis en ambos debe haber un provecho o beneficio para el sujeto activo.

Siendo que de los veintiún (21) tipos delictivos descritos en la Ley Especial contra Delitos Informáticos, en principio, por cualquiera de ellos puede ser responsable una persona jurídica, ya que su comisión se deriva de la persona natural o física que puede comprometer al ente corporativo o que dependen del mismo, siempre que se cumplan con los elementos previstos en el artículo 5 de la norma en estudio, es decir, cuando concurre que sea por decisión de sus órganos, en el ámbito de su actividad, con sus recursos o en su provecho.

El título III llamado Disposiciones Comunes, señala una serie de circunstancias que agravan las penas previstas en los delitos, siendo unas

genéricas y la otra específica para las personas jurídicas, pautada de la siguiente manera:

> Artículo 28. Agravante especial. La sanción aplicable a las personas jurídicas por los delitos cometidos en las condiciones señaladas en el artículo 5 de esta Ley, será únicamente de multa, pero por el doble del monto establecido para el referido delito.

Del cual se deduce que la sanción impuesta a la persona jurídica, será de índole patrimonial, lo que resulta lógico, en razón de la imposibilidad de privar de libertad a un ente moral o jurídico, previendo la aplicación de la multa, pero por el doble del monto previsto en el delito por el cual se determine su responsabilidad. Asimismo establece una serie de penas accesorias, la posibilidad de que el tribunal publique la sentencia condenatoria y por último la indemnización civil de la víctima de los tipos penales de contenido económico.

Revisados a grandes rasgos la disposiciones previstas en la Ley Especial contra los Delitos Informáticos (2001), se pudo observar que las personas jurídicas tienen responsabilidad penal, la cual es determinada si se dan de forma concurrente las circunstancias en las cuales se pueda establecer que se cometió el hecho por decisión de sus órganos, dentro de su actividad empresarial, con los recursos de la sociedad o en su interés preferente, así las cosas, pueden incurrir en diversos tipos penales y las sanciones aplicables son de multa por el doble del monto pautado en el delito, pero además de la imposición de penas accesorias, que se asemejan al cierre temporal de la empresa.

3. Consecuencias de la responsabilidad penal de las personas jurídicas en el desarrollo de sus actividades

Determinada la responsabilidad penal de la persona jurídica, por sentencia definitiva establecida por el Juez de Primera Instancia en funciones de Control o Juicio (dependiendo del momento procesal de la condena), la ley especial[19] ha establecido un conjunto de consecuencias, sanciones desde el punto de vista empresarial, que afectan su correcto funcionamiento, partiendo de que los delitos han sido cometidos en el seno de la persona jurídica o utilizándola como instrumento.

Conforme a ello, la ley establece las sanciones principales, las cuales son imponibles tanto a personas físicas como lo son la prisión y el arresto, y la multa, a la persona jurídica; en el plano económico, la multa es una sanción pecuniaria que puede perjudicar notablemente no solo el giro operacional de la empresa, sino también sus compromisos comerciales, laborales, tributarios; se considera importante destacar que la multa muchas veces no tiene una gran

19 Ley Especial Contra los Delitos Informáticos.

efectividad, ya que pierde importancia en algunas veces por la cuantía; al mismo tiempo, podría ser hasta injusta desde el punto de vista de afectación a su personal.

En ese orden de ideas, la ley establece sanciones accesorias a ser aplicadas conjuntamente con la sanción principal, las mismas están previstas en el artículo 29, siendo relevante señalar alguna de ellas, en primer término prevé el comiso de los objetos utilizados para la comisión de los delitos pautados en los artículo 10 y 19, relativos a posesión de equipos para sabotaje y falsificaciones, por cuanto en la investigación debieron ser incautados y sería ilógico su restitución al condenado.

En segundo término, la imposición de trabajo comunitario por tres años, en la comisión de los delitos de acceso indebido[20] y favorecimiento culposo al sabotaje[21], los cuales prevén penas inferiores a los ocho (08) años y no están consagrados en el catálogo de excepciones, siendo considerados delitos menos graves conforme a lo previsto en el Código Orgánico Procesal Penal[22], cuya pena principal impuesta podría ser incluso menor a la accesoria.

En tercer término prevé la inhabilitación para el desempeño de funciones públicas o el ejercicio de la profesión, estableciendo unas condiciones específicas, conforme a la redacción empleada, pareciera se refiere a las personas naturales.

En cuarto término, contiene la suspensión del permiso, registro o autorización para operar hasta por tres (03) años, luego de cumplida la pena principal, lo que a criterio de la autora, resulta un poco desproporcionado, porque podría llegar a constituir de manera indirecta la disolución de la empresa, es decir que deje de existir en el mundo jurídico, lo que puede equipararse a la pena de muerte, la cual está prohibida conforme a lo previsto en el artículo 43 de la Constitución de la República Bolivariana de Venezuela[23].

En ese sentido, valga acotar lo señalado por Frederich Desportes[24] cuando establece que aunque la disolución de la empresa pueda ser equiparada a la pena de muerte y se representa de forma tan dramática, ésta solo está prevista para los delitos más graves.

En el artículo 30 *ejusdem* se establece la facultad para el ente jurisdiccional de publicar o difundir la sentencia condenatoria, lo cual en el área empresarial, debe ser entendido como una sanción moral, ya que las empresas deben generar confianza en sus aliados y competidores, lo que a todas luces se traduce como una pérdida del buen nombre y por ende una baja en sus inversiones. Asimismo, se prevé la indemnización civil derivada de los delitos previstos contra la

20 Artículo 6 de la Ley Especial Contra los Delitos Informáticos.

21 Artículo 8 de la Ley Especial Contra los Delitos Informáticos.

22 Publicado en la Gaceta Oficial No. de 12 de junio de 2012, artículo 354

23 Publicada en la Gaceta Oficial Extraordinaria No. 5.908 del 19 de febrero de 2009.

24 Frederich Desportes, Las Penas Aplicables a las Personas Jurídicas. Disponible en https://www.unifr.ch/ddp1/derechopenal/anuario/an_1997_14.pdf

propiedad y contra el orden económico, por cuanto están revestidos de una afectación patrimonial a la víctima, cuyo monto será calculado por el juez respectivo.

Por último, se debe tener claro que todas estas sanciones pecuniarias, personales, y del propio funcionamiento en el tiempo de la actividad comercial, son medidas establecidas en el proceso penal venezolano, no solo para evitar la continuación de la participación del ente jurídico en la comisión de hechos punibles, sino que también se busca salvaguardar los bienes jurídicos tutelados por la ley especial.

Conclusiones

En referencia a la responsabilidad penal de las personas jurídicas, es evidente que ella obedece a criterios de política criminal del Estado, esto debido al surgimiento de fenómenos delictivos que incluyen, más allá de la persona natural, al ente colectivo con capacidad de ser sujeto de derecho, lo que resulta relevante no solo para el Derecho civil, sino también para el Derecho penal, lo que hace necesario su inclusión como sujeto de derecho con responsabilidad penal.

En ese sentido, el legislador venezolano al decidir su inclusión como sujeto activo en la comisión de delitos y por tanto, responsable penalmente, efectuó un traslado de la responsabilidad de la persona física a la persona jurídica, ya que la acción y por ende la culpabilidad siempre será efectuada por personas naturales.

Habida cuenta de lo anterior, en la Ley Especial contra Delitos Informáticos, como una norma innovadora para su época de publicación (año 2001), prevé la responsabilidad penal de las personas jurídicas, la cual dependerá de la acción de aquellas personas físicas que puedan comprometer la voluntad de la empresa, o que se encuentren bajo su dependencia, lo que debe redundar en un beneficio o preferencia para el ente colectivo o que se utilicen sus recursos.

Conforme a ello, la ley especial prevé veintiún tipos penales que en principio pareciera que pueden ser imputables a la persona jurídica, sin embargo, dependerá de cada caso específico el determinar la autoría del ente colectivo y por ende su responsabilidad penal, siendo lo más engorroso para el fiscal el poder atribuir los elementos subjetivos de la culpabilidad.

De llegar a determinarse la responsabilidad penal de la persona jurídica, más allá de la pena principal, que en este supuesto, siempre será una multa, lo que a todas luces es lógico, ya que la empresa no puede ser privada de su libertad, pero su sanción será pecuniaria con la circunstancia agravante de que será el doble del monto previsto en el tipo penal, aunado a la imposición de penas accesorias como el comiso de los objetos utilizados en la comisión del delito, no concederle en los tres años posteriores a la condena, los permisos o autorizaciones de funcionamiento, lo que va en detrimento de su funcionamiento.

Aún cuando la ley especial, en principio, no prevé la disolución de la empresa como pena principal o accesoria, podría esta sanción accesoria derivar en un cierre temporal o definitivo de la organización, sin que la norma establezca mecanismos de protección a los trabajadores u otros accionistas.

En conclusión, aun cuando doctrinariamente se mantiene la discusión sobre si es factible o no la responsabilidad penal de la persona jurídica, no es menos cierto, que el legislador patrio acogió la tesis de que era necesario, en virtud de los múltiples avances de la criminalidad y del riesgo de dejar impunes conductas lesivas a los bienes jurídicos protegidos, el establecer la responsabilidad penal a estos entes, siempre que se determinen las condiciones que permitan demostrar que su accionar fue producto del consenso de sus órganos de decisión, que fue con sus recursos y más importante en su beneficio.

Delitos informáticos como forma de entretenimiento: delitos contra niños y adolescentes, y contra el orden económico en la Ley Especial contra los Delitos Informáticos*

Gustavo Adolfo Amoni Reverón**

SUMARIO: Introducción. 1. Difusión o exhibición de material pornográfico (artículo 23 LECDI). 1.1 Sujetos. 1.2 Objetos. 1.3 Medio de comisión. 1.4 Parte objetiva del tipo penal. 1.5. Parte subjetiva del tipo penal. 1.6. Primera historia: Black Mirror. 2. Exhibición pornográfica de niños o adolescentes (artículo 24). 2.1 Sujetos. 2.2 Objetos. 2.3 Medio de comisión. 2.4 Parte objetiva del tipo penal. 2.5. Parte subjetiva del tipo penal. 2.6 Segunda historia. Exhibición pornográfica de niños o adolescentes: Dark Net (temporada 1, episodio 3). 3. Apropiación de propiedad intelectual (artículo 25); 3.1 Sujetos. 3.2 Objetos. 3.3 Medio de comisión. 3.4 Parte objetiva del tipo penal. 3.5. Parte subjetiva del tipo penal. 3.6 Tercera historia. Apropiación de propiedad intelectual: Suits (temporada 2, episodio 1). 4. Oferta engañosa (artículo 26). 4.1 Sujetos. 4.2 Objetos. 4.3 Medio de comisión. 4.4 Parte objetiva del tipo penal. 4.5. Parte subjetiva del tipo penal. 4.6 Cuarta historia. Oferta engañosa: Fyer, la fiesta más exclusiva que nunca sucedió. Conclusión.

Recibido: 29/1/2020 • Aceptado: 19/2/2020

* En este artículo se desarrollan por escrito las ideas expuestas en la conferencia "Delitos informáticos como forma de entretenimiento", impartida en la Universidad Católica "Santa Rosa" (Caracas), el 6 de diciembre de 2019, disponible en: https://youtu.be/iO_ciqxWitU

** Abogado *summa cum laude* de la Universidad de Carabobo, profesor de pregrado y postgrado de la Universidad Central de Venezuela, del Doctorado en Derecho de la Universidad Católica "Santa Rosa" y exdirector de la Escuela Nacional de la Magistratura de Venezuela, con más de 30 publicaciones en Argentina, Brasil, Colombia, Ecuador, España, México y Venezuela, en la mayoría de los cuales ha participado como ponente en congresos y foros sobre Derecho Informático.

Resumen

A partir de cuatro historias tomadas de programas de televisión se analiza el mismo número de los tipos penales informáticos previstos en los últimos dos capítulos de la Ley Especial Contra los Delitos Informáticos. Estos tipos penales tienen la particularidad de ser perpetrados por medios informáticos, salvo en ciertos casos de "apropiación de propiedad intelectual" que pueden verificarse de diferentes maneras sin intervención de tecnologías de información, pero que aún así pudieran estimarse formalmente delitos informáticos por el solo hecho de estar incluidos en la ley especial.

Palabras claves: Exhibición de material pornográfico. Pornografía infantil. Propiedad intelectual. Oferta engañosa. Delitos informáticos.

Abstract

Four stories from TV shows, allow us to analyze same number of cybercrimes from the last two sections of Venezuelan "Special Act against Cyber Crime". These crimes are committed by informatics means, except in some cases of "appropriation of intellectual property" that can be verified in different ways without using information technology. Nevertheless they are formally considered cybercrimes just because they are included in the special act.

Key words: Exhibition of pornographic material. Child pornography. Intellectual property. False advertising. Cybercrime.

Introducción

Los últimos dos capítulos de la Ley Especial Contra los Delitos Informáticos (LECDI)[1] están conformados por cuatro tipos penales. El Capítulo IV "De los Delitos Contra Niños, Niñas o Adolescentes" tipifica en el artículo 23, la "Difusión o exhibición de material pornográfico", por el que se sanciona la falta de previsiones para evitar el acceso a material pornográfico, u otro de contenido para adultos, por parte de niños y adolescentes, mientras que el artículo 24 prevé el tipo penal de "Exhibición pornográfica de niños o adolescentes", por el que se prevén penas para quien a estas víctimas especialmente vulnerables para fines pornográficos.

Se trata de dos normas que deben leerse de la mano con la Ley Orgánica para la Protección de Niños, Niñas y Adolescentes, a fin de evitar contradicciones

1 Gaceta Oficial de la República Bolivariana de Venezuela nro. 37.313 del 30 de octubre de 2001.

en la interpretación normativa, generando una aplicación armónica del ordenamiento de derecho especial en materia de niños y adolescentes, junto a otra especial también, en materia de delitos informáticos.

Por su parte, el capítulo V "De los Delitos Contra el Orden Económico", tipifica en el artículo 25 la apropiación de propiedad intelectual, la que deberá interpretarse a la luz de la Ley de Propiedad Intelectual. Con esta norma se pretende sancionar el tratamiento informático de obras del intelecto sin la debida autorización.

En el caso del artículo 26 se sanciona la oferta engañosa, imponiendo penas de prisión y multa a quien obtenga un provecho injusto mediante el engaño ajeno, perpetrado mediante las tecnologías de información y comunicación.

En suma, los capítulos IV y V de la LECDI prevén cuatro tipo penales que serán analizados, primero, dividiéndolos en sus elementos constitutivos, para aplicar luego el método de resolución de casos, según los elementos del delito, a partir de igual número historias tomadas de documentales y series de televisión, con el objeto de ilustrar, con casos dramatizados, estas normas de Derecho penal venezolanas que alcanzaron los 18 años de vigencia, lo que genera la necesidad de revisarlas y adaptarlas a las nuevas modalidades de actuación, mediante y en contra de, sistemas informáticos.

1. Difusión o exhibición de material pornográfico (artículo 23 LECDI)

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

El tipo penal transcrito prevé cinco acciones típicas correspondientes a igual cantidad de verbos rectores. Esta técnica legislativa se aplicó para el desarrollo de toda ley, por lo que en cada artículo se tipifican múltiples conductas, en este caso, cinco; no obstante, su análisis se efectuará por artículo, incluyendo los diversos verbos rectores al tratar la parte objetiva del tipo.

El desarrollo de la investigación seguirá el método propuesto por Santiago Mir Puig en el que identifica tres elementos de la estructura de todo tipo penal: la conducta típica, sus sujetos y sus objetos[2].

1.1. Sujetos

1.1.1. Activo: El artículo prevé responsabilidad penal para "Todo aquel que…" realice la acción típica. No hace falta que la persona tenga alguna

2 Santiago MIR PUIG, *Derecho Penal.* (7ª edición), España, Reppertor, 2004, p. 222.

característica o pertenezca a una categoría especial, puesto que hoy, gracias a Internet y al auge de las redes sociales, es fácil para cualquier persona compartir información de todo tipo con solo acceder a su computadora, teléfono inteligente, *tablet* o cualquier otro dispositivo electrónico con conexión a Internet y capacidad para recibir y transmitir datos.

1.1.2. Pasivo: Es calificado. El interesado directamente en que no se ejecute la acción típica para evitar lesiones a sus derechos es cualquier niño o adolescente, puesto que es a ellos a quienes se busca evitar el acceso a material pornográfico o reservado a adultos, ya que conforme a la Ley Orgánica para la Protección de Niños, Niñas y Adolescentes[3] (LOPNNA), tienen derecho a recibir, buscar y utilizar todo tipo de información que sea acorde a su edad, siempre teniendo presente su condición especifica de persona en desarrollo, lo que se garantiza con base en su interés superior.

También pudiera plantearse que el adulto, en su condición de padre, representante o responsable del niño o adolescente que accede al material reservado para aquel, sin saber el contenido de dicho material, pudiera ser víctima del delito puesto que se ve vulnerado en su derecho a educar al niño o adolescente según sus creencias, así como también en su deber de "… asegurar a los niños y adolescentes el ejercicio y disfrute pleno y efectivo de sus derechos y garantías"[4].

1.2. Objetos

1.2.1. Objeto material: Es la cosa o persona sobre la que recae la acción. En este caso, la exhibición, difusión, transmisión o venta recae sobre el material pornográfico o reservado a personas adultas. En otras palabras, lo que se exhibe, se difunde, se transmite o se vende es dicho material[5], que no requiere estar en formato electrónico, en todos los casos, para que se cumpla el fin del delito.

Así, la exhibición, difusión o transmisión de material reservado a adultos, para ser perpetradas por medios electrónicos, implican que dicho material se encuentre en formato electrónico; lo que no ocurre con la venta, ya que se puede vender, por medios electrónicos, material impreso o analógico para ser entregado por el vendedor y retirado por el comprador por medios tangibles.

3 Gaceta Oficial de la República Bolivariana de Venezuela nro. 6185 Extraordinario del 8 de junio de 2015.

4 LOPNNA.

5 En este sentido: Luis RODRÍGUEZ COLLAO, "Criterios de agravación de la pena en los delitos de producción, difusión y almacenamiento de pornografía infantil", *Revista de Derecho* (Valdivia), vol.26, no.1, jul. 2013, pp. 145-166 (p. 149)

1.2.2. Bien jurídico protegido: Es la cosa o valor que la ley protege, lo que pudiera ser, por una parte, el desarrollo del niño o adolescente según su edad, además de la educación de los hijos, de los representados, o de los niños o adolescentes de los cuales un adulto sea responsable.

También se ha planteado que en los delitos sexuales contra niños y adolescentes el bien jurídico protegido sería la indemnidad sexual, entendida como la exención de intervenciones en el desarrollo sexual de los niños o adolescentes[6], como sucedería si el niño o adolescente se expone a pornografía[7]; no obstante, este bien jurídico pudiera aplicarse al caso de la pornografía, mas no así en caso de otros materiales reservados a adultos por la naturaleza de su contenido vinculado a elementos de lenguaje, salud y violencia en los términos de la ley[8].

1.3. Medio de comisión

La norma prevé la perpetración de la conducta "… por cualquier medio que involucre el uso de tecnologías de información…" lo que remite la letra "a" del artículo 2 LECDI donde se definen tales tecnologías como la:

> Rama de la tecnología que se dedica al estudio, aplicación y procesamiento de datos, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, transmisión o recepción de información en forma automática, así como el desarrollo y uso del 'hardware', 'firmware', 'software', cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de datos.

Así, el medio de comisión no es genérico, como pudiera entenderse de la expresión "por cualquier medio", sino que es específico, ya que cualquiera de esos medios debe involucrar el procesamiento automático de datos, equipos o programas informáticos. De tal modo, si la exhibición, difusión, transmisión o venta de material reservado a adultos se verifica por medios tangibles o analógicos, esta norma sería inaplicable al caso concreto.

6 Norberto J. DE LA MATA BARRANCO, "Tratamiento legal de la edad del menor en la tutela penal de su correcto proceso de formación sexual", *Revista Electrónica de Ciencia Penal y Criminología*, 2019, pp. 1-70, p. 5.

7 Sobre la definición de pornografía, ver Liliana García, "La pornografía infantil en la era de las redes sociales", [video], disponible en: https://youtu.be/faht4v_KD-s

8 Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos, Gaceta Oficial de la República Bolivariana de Venezuela Nº 39.579 de fecha 22 de diciembre de 2010, reimpresa en la Gaceta Oficial de la República de Venezuela Nº 39.610 de fecha 7 de febrero de 2011.

1.4. Parte objetiva del tipo

Para que se configure el tipo penal de difusión o exhibición de material pornográfico, el sujeto activo debe exhibir, difundir, transmitir o vender, valiéndose de TI, material pornográfico o reservado a personas adultas, con la particularidad de omitir advertir al usuario sobre el contenido del material, para que restrinja el acceso a niños y adolescentes.

En este orden de ideas, exhibir significa "Manifestar, mostrar en público"[9]; difundir, "Propagar o divulgar conocimientos, noticias, actitudes, costumbres, modas, etc."; transmitir supone "Hacer llegar a alguien mensajes o noticias"; y vender, es el acuerdo por el cual una persona se compromete a entregar una cosa y la otra parte, a pagar cierto precio por ella[10].

Las tres primeras conductas no presentan particularidades destacables en entornos digitales, como lo prevé la norma, pero la situación difiere cuando se trata del contrato de compraventa electrónica: si es por videoconferencia, mensajería de datos, o cualquier sistema de intercambio de manifestaciones en tiempo real, se entendería como un contrato entre presentes, de lo contrario se trataría de un contrato entre ausentes o de formación sucesiva[11], lo que implicaría acudir al DLMDFE para precisar cuándo y dónde se perfecciona el contrato electrónico.

Lo expuesto es importante para determinar la perpetración del delito de venta de material reservado a adultos sin la debida advertencia para evitar el acceso a su contenido por parte de niños y adolescentes; el cual, no obstante, pudiera presentar formas inacabadas, como la tentativa o la frustración en caso de que se ofreciera en venta dicho material pero no se concretase la operación.

Ninguna de estas conductas es autónoma, en el entendido de que no configuran tipos penales por sí mismas, sino que requieren de una conducta complementaria: omitir realizar advertencias para que el usuario restrinja el acceso a su contenido, a niños y adolescentes, en cumplimiento de la LOPNNA y LRSRT[12].

Adicionalmente, es oportuno destacar que si la difusión, transmisión, exhibición o venta se produce en un entorno analógico o por medios tangibles, normalmente impresos, se aplicará los previsto en los artículos 74 y 235 LOPNNA, en concordancia con los términos fijados por la Sala Constitucional del Tribunal Supremo de Justicia en la sentencia número 359 del 6 de mayo de 2014 en la que se ordena "Eliminar toda imagen de carga o contenido sexual explícito o

9 https://dle.rae.es/exhibir

10 José M. LETE DEL RIO, *Derecho de Obligaciones*, Vol. III, tecnos, España, 1999, p. 31

11 Mariliana RICO CARRILLO, *Comercio electrónico, Internet y Derecho*, Legis, 2003, p. 109

12 Gaceta Oficial de la República Bolivariana de Venezuela, nro. 39.610, del 7 de febrero de 2011.

implícito de los anuncios publicitarios en los medios impresos de libre acceso a niñas, niños y adolescentes…".

También, debe indicarse que la explotación de la industria o el comercio de la pornografía es sancionado, a pesar de las advertencias debidas, si el sujeto activo actúa como parte integrante de un grupo de delincuencia organizada[13]; igualmente, si algún integrante de un grupo de delincuencia organizada vende, difunde o exhibe material pornográfico directamente a niños, niñas o adolescentes, incurre en el delito de difusión de material pornográfico tipificado en el artículo 47 *eiusdem*.

Para finalizar este tópico, es útil referir lo expresado por la Sala Constitucional en la misma sentencia aludida antes, en cuanto a las imágenes contenidas en los teléfonos inteligentes de particulares, que pueden ser transmitidas sin advertencia de su contenido aunque sea reservado para adultos:

> La Sala también debe indicar que escapa del control del Estado qué tipo de imágenes e información son transmitidas a través de los sistemas y equipos de telecomunicaciones de telefonía móviles por parte de los ciudadanos en casos en que no haya una contravención de normas legales, por lo que ante la situación de que sean los propios niños, niñas y adolescentes quienes transmiten la data considerada ofensiva, se debe reiterar que los padres, madres, representantes y tutores son quienes tienen la principal obligación de vigilancia de estos materiales respecto a sus hijos y representados, siendo a estos en todo caso a quien corresponde controlar el material que manejan y se encuentre disponible por medio de los teléfonos celulares, sin que ello menoscabe la corresponsabilidad que existe para el Estado y el resto de la colectividad en la protección de los niños, niñas y adolescentes, el cual, a través de sus diferentes órganos y entes, combate y combatirá todo lo que se encuentre vinculado a los delitos y en especial a la pornografía infantil.

La transmisión de imágenes reservadas para adultos puede ocurrir entre particulares, sin que esto quede excluido del tipo penal ya que no se exige que la transmisión sea pública. Un adulto puede recibir un video o imagen como mensaje de datos y sin saber cuál es su contenido, o creyendo que es apto para todo público, verlo con un niño o adolescente, exponiéndolo a contenido que pudiera perjudicarlo en el momento de desarrollo en el que se encuentra.

Si embargo, el derecho a la privacidad impide que el Estado vigile el contenido de cada mensaje que se envíe, correspondiendo a los padres, representantes y responsables evitar la exposición de niños y adolescentes a fotografías, videos u otras producciones visuales o audiovisuales, sin perjuicio de la eventual responsabilidad penal en que pudieran incurrir, previa denuncia.

13 Artículo 46 de la Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo, Gaceta Oficial de la República Bolivariana de Venezuela, nro. 39.912 del 30 de abril de 2012.

1.5. Parte subjetiva del tipo

Es un tipo penal doloso, pues se requiere la voluntad de exhibir, difundir, transmitir o vender material reservado a adultos, sin las debidas advertencias que permitan al usuario restringir el acceso de niños y adolescentes a tal material, sabiendo que lo hace "… sin ninguna causa de exclusión del comportamiento humano…"[14].

Deriva de lo anterior que cada comportamiento principal (exhibir, difundir, transmitir o vender) e incluso la omisión de las debidas advertencias al usuario, no pudieran producirse por culpa, sino solamente de modo doloso, ya que esto no está previsto expresamente; es decir, quien exhiba material reservado para adultos sin advertir previamente las reservas que deben hacerse de acuerdo con su contenido, debe tener consciencia de lo que está haciendo y debe querer llevarlo a cabo para que sea sancionado por tal norma, de lo contrario, la conducta no pudiera subsumirse en el tipo penal bajo análisis.

1.6. Primera historia. Delito de difusión o exhibición de material pornográfico: Black Mirror (temporada 1, episodio 2)[15]

Una sociedad conectada a Internet de modo total y permanente, cuyos integrantes viven en unos habitáculos[16], cuyas paredes están cubiertas de pantallas controlables por movimiento corporal sin necesidad de contacto, en las que se someten constantemente a publicidad. Si los habitantes cierran los ojos, un detector de reconocimiento facial emite una alarma e indica que la persona debe abrir los ojos para continuar viendo la publicidad.

Uno de los anuncios más recurrentes es el de "Wraith Babes" un portal de videos pornográficos[17], que se repite constantemente preguntando al usuario si quiere acceder a la transmisión, debiendo cumplir con un período obligatorio de visualización[18].

Durante la publicidad, se muestran mujeres en ropa interior, con poses sugestivas, acompañadas de frases como la siguiente "las chicas más sexis en las posiciones más obscenas".

A fin de determinar si se ha perpetrado el delito de difusión o exhibición de material pornográfico deben precisarse los hechos:

14 Santiago MIR PUIG, *Derecho Penal*, *op. cit*, p.62

15 Visto en Netflix en 2019.

16 Lo que recuerda los "Pisos Colmena" españoles: ttps://www.youtube.com/watch?v=2TKEZ0nQYrE

17 Entre 2015 y 2019, la pornografía o alguna expresión similar, no estuvo en la lista de las 10 palabras más buscadas en el ámbito global (trends.google.com).

18 Como sucede con algunos videos de Youtube.

La compañía de pornografía "Wraith Babes" difunde a los habitáculos de los habitantes publicidad sobre su actividad comercial. Esa publicidad es obligatoria y no se advierte que el contenido es solo para adultos.

Aplicando el método de resolución de casos penales se advierte que existe acción humana libre detrás de la emisión de la pauta publicitaria, que si bien no tiene contenido pornográfico en el sentido de no mostrar relaciones sexuales o genitales en forma lasciva, las poses sugestivas, la presencia en ropa interior, el maquillaje y los mensajes promueven el consumo audiovisual de pornografía, lo que lo convierte en material reservado a adultos.

La compañía que anuncia su producto lo hace queriendo difundirlo y estando consciente de que se trata de material para adultos. En este caso, no hay causales que excluyan la acción[19] de la sociedad de comercio, ya que la publicidad no se produjo por fuerza irresistible, movimientos reflejos o en estado de inconsciencia, sino por decisión de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en su interés exclusivo o preferente[20].

En segundo lugar debe revisarse la tipicidad. La empresa difundió material reservado a adultos sin advertir previamente que lo haría, impidiendo que los padres, representantes o responsables de los niños o adolescentes pudieran tomar las previsiones para evitar su acceso a tal publicidad.

En tercer lugar debe analizarse la antijuridicidad, donde no se advierten causas de justificación, pues la difusión del material pornográfico no se produjo en legítima defensa, estado de necesidad justificante, en ejercicio de un derecho[21] o cumplimiento de un deber.

En cuarto lugar, debe determinarse la "imputación personal del injusto penal" que se resumen en la capacidad de evitar el hecho y conocer su antijuridicidad[22], siendo posible que la incapacidad para evitar el hecho provenga de alguna causa de inimputabilidad como en los casos de niños y adolescentes menores de 14 años, alteraciones psíquicas, trastorno mental transitorio, intoxicaciones graves y alteración de la percepción[23].

Todos estos casos se refieren a personas naturales, pero en la situación ficticia que se está narrando, el autor es una persona jurídica que en Venezuela tiene responsabilidad penal *ex* artículo 5 LECDI[24], cuando actúe por decisión

19 Ver, a modo referencial, la sentencia nro. 93 emitida por la Sala de Casación Penal del Tribunal Supremo de Justicia el 11 de marzo de 2015.

20 Esto no se indica en el episodio que se comenta sino que se afirma como ejemplo del delito en cuestión.

21 En el episodio que se usa a modo ilustrativo no se cuestiona la legalidad del anuncio publicitario; no obstante, se está aplicando el artículo 23 como si esa situación hubiera ocurrido en Venezuela.

22 Santiago MIR PUIG, "Derecho Penal", *op, cit*., p. 529

23 Santiago MIR PUIG, "Derecho Penal", *op, cit*., p. 530

24 Sobre el tema: Emy Rivero, "Responsabilidad penal informática de las personas jurídicas», [video], disponible en: https://youtu.be/zTZjNFQ3WDg

de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en su interés exclusivo o preferente.

En consecuencia, si esto hubiera ocurrido en Venezuela, la sociedad mercantil "Wraith Babes" pudiera ser sancionada con multa de cuatrocientas a mil doscientas unidades tributarias conforme al artículo 23 LECDI en concordancia con el artículo 28, por el que se duplica la pena de multa prevista para personas naturales y se aclara que no procede la pena de prisión.

Además, se aplicará "necesariamente" como pena accesoria, la suspensión del permiso, registro o autorización para operar como productor audiovisual o para ofrecer material pornográfico por medios de comunicación, hasta por el período de tres (3) años después de cumplida o conmutada la sanción principal, ya que el delito se perpetró mediante una persona jurídica, sanción que pudiera significar el cierre definitivo de la empresa ante la falta de ingresos durante ese período, sin explicarse cómo se armonizaría esto con los pasivos laborales y otras deudas de la empresa[25].

2. Exhibición pornográfica de niños o adolescentes (artículo 24)

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

2.1. Sujetos

2.1.1. Activo: El tipo penal no diferencia categorías de sujetos sino que alude a "Toda persona…", por lo que cualquiera podrá perpetrar este delito que es de sujeto activo genérico.

2.1.2. Pasivo: El titular del bien jurídico tutelado o interesado directo en que se utilice su persona o imagen, es el niño o adolescente; no obstante, sus padres, representantes o responsables también pudieran considerados interesados indirectos, respecto de los primeros, que no requieren actuar mediante sus padres sino que pueden hacerlo por sí mismos.

2.2. Objetos

2.2.1. Material: La acción recae sobre la persona o imagen de un niño o adolescente, por tanto serán estos los objetos materiales. En el primer caso, se puede entender que se utiliza la persona de un niño o adolescente cuando se somete a captación de su imagen en vivo en el desarrollo de actividades

25 Al respecto: Emy Rivero, "Responsabilidad penal informática de las personas jurídicas», [video], disponible en: https://youtu.be/zTZjNFQ3WDg

sexuales, o de sus genitales u otras zonas erógenas del cuerpo humano adulto, para almacenarla y transmitirla por medios electrónicos.

Respecto del segundo supuesto, el agente utilizaría una imagen ya captada que no tenía intención exhibicionista o pornográfica y la utiliza para tales fines, incluso, a partir de la manipulación de imágenes mediante programas computacionales puede usar la imagen, por ejemplo, el rostro u otras partes del cuerpo de niños o adolescentes con tales fines, lo que encuadraría en el tipo penal.

En ambos casos se utilizan imágenes ya que su exhibición en directo, no requeriría el uso de tecnologías de información, de modo que esta pudiera ser una interpretación para justificar la diferenciación normativa.

2.2.2. Bien jurídico protegido: En el caso de la pornografía infantil, el bien jurídico protegido es la indemnidad sexual, entendida como se vio antes, en el sentido de permitir el desarrollo sexual de la persona conforme a su evolución etaria, considerando que los niños y adolescentes no están en capacidad de determinar libremente su vida sexual[26].

Respecto de la exhibición, serían la propia imagen, el honor, la privacidad e incluso los datos personales, puesto que nadie tiene derecho a difundir la imagen de la cara u otras partes del cuerpo de terceras personas, con fines sexuales sin su autorización, lo cual está totalmente prohibido en caso de niños y adolescentes, quienes están protegidos por el principio del interés superior.

2.3. Medio de comisión

Es informático. La norma prevé que debe perpetrarse "… por cualquier medio que involucre el uso de tecnologías de información…", de ahí que la utilización de niños o adolescentes, o de su imagen, con fines pornográficos sin valerse de medios informáticos no puede penarse con esta norma sino con el artículo 258 LOPNNA, que sanciona a quien se lucre de la actividad sexual de niños, niñas y adolescentes, sin importar el medio de comisión.

Además, es importante considerar que el numeral 15 del artículo 15 de la Ley Orgánica sobre el Derecho de las Mujeres a una Vida Libre de Violencia, que sería aplicable a niñas y adolescentes, prevé la "violencia mediática", mas no establece pena alguna por su perpetración.

26 Jelio Paredes Infanzón, "Análisis de la jurisprudencia en el delito de violación sexual de menores de edad en el Perú", trabajo de grado para maestría en Derecho Penal, Universidad Inca Garcilaso de la Vega, Perú, 2020, disponible en http://repositorio.uigv.edu.pe/bitstream/handle/20.500.11818/4869/TESIS_PAREDES%20INFANZON.pdf?sequence=1&isAllowed=y

2.4. Parte objetiva del tipo penal

La conducta exterior consiste en utilizar "… la persona o imagen de un niño, niña o adolescente…", por cualquier medio informático, con fines exhibicionistas o pornográficos.

El sujeto activo debe utilizar a un niño o adolescente, o su imagen, bien por la fuerza, mediante engaños o convenciéndolo, para exhibirlo sexualmente o generar contenido pornográfico, por medios informáticos, sin necesidad de que se genere ganancia alguna.

Si la actividad fuera ejecutada por el integrante de un grupo de delincuencia organizada, incluyendo su verificación por medios informáticos, se aplicará la LOCDOFT[27].

2.5. Parte subjetiva del tipo penal

El agente debe querer utilizar al niño o adolescente, o su imagen, con fines exhibicionistas o pornográficos, y estar consciente de lo que está haciendo. Si el sujeto no tiene esa intención y conocimiento, su conducta no encuadraría en la norma, ya que se está ante un tipo penal doloso mas no culposo.

2.6. Segunda historia. Exhibición pornográfica de niños o adolescentes: Dark Net (Temporada 1, episodio 3)[28]

Según se afirma en el documental, en la Isla Cebú, Filipinas, parte importante de la población utiliza a sus hijas, normalmente niñas, para desnudarse ante una cámara web y hasta llegan a realizar actos sexuales con ellas para que un tercero, normalmente extranjero, sacie sus ansias sexuales a cambio de dinero.

En ciertos casos, la propia familia convence a las niñas de que esa es su responsabilidad para que sus miembros puedan alimentarse. En entrevistas que les realizaron a algunas de estas víctimas de explotación sexual, declaran que lo hacen para mantener a su familia, seguras de que ese es su deber, dejando entrever que se trata de una actividad normal, aunque no se nota tranquilidad ni alegría, sino más bien vergüenza y tristeza en sus declaraciones.

En uno de los casos, ambos padres participaban en la explotación sexual. El padre (biológico y de crianza) le vendaba los ojos a la niña para proceder a tener relaciones sexuales con ella, transmitiendo la actividad por cámara web para que un extranjero se masturbara mientras veía la escena, previo pago a distancia.

Analizando este último caso, el primer elemento del delito, como es la acción, está presente. Aquí e el agente no actuó por fuerza irresistible, movimientos

27 Artículos 48 y 49, ajustándolos a las particularidades según cada caso concreto.
28 Visto en Netflix en septiembre de 2019.

reflejos o en estado de inconsciencia. Él y su esposa, querían y sabían lo que hacían, reiteradamente, puesto que con el dinero obtenido llegaron a comprar un vehículo.

En segundo lugar, la conducta es típica puesto que los padres utilizaron a la persona de su hija para realizar una actividad sexual, transmitiéndola en vivo mediante una cámara web y un programa de videoconferencia; es decir, se valieron de medios informáticos para fines de pornografía infantil.

La conducta es también antijurídica. Los sujetos activos, padres de la víctima, no actuaron en legítima defensa, estado de necesidad justificante, en ejercicio de un derecho[29] o cumplimiento de un deber. En efecto, por mucha necesidad que tengan los padres para sobrevivir no justifica someter a su hija, una niña, a tener relaciones sexuales con su propio padre para obtener dinero, y no solo comer, sino incluso, comprar un vehículo.

Por último, el injusto penal es imputable a los padres, quienes pudieron evitar el hecho y conocer su antijuridicidad[30], pues ambos son mayores de edad, sin alteraciones psíquicas, trastorno mental transitorio, intoxicaciones graves y alteración de la percepción[31] alegadas ni evidenciadas en el documental.

En cuanto a la intervención, ambos responden como coautores por haber planificado y dividido en partes el plan, ejecutando cada uno lo necesario para la ejecución definitiva.

Por último, pudieran generarse otros delitos en concurso real, pero ello escapa de este análisis limitado a los delitos informáticos descritos desde el inicio.

3. Apropiación de propiedad intelectual (artículo 25)

> Quien sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un *software* u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias".

3.1. Sujetos

3.1.1. Activo. La expresión "Quien…", sin estar seguida de una delimitación del agente, hace que cualquier persona pueda perpetrar este delito. Por tanto, el sujeto es genérico o indeterminado.

29 En el episodio que se usa a modo de ejemplo no se cuestiona la legalidad del anuncio publicitario no obstante, se está aplicando el artículo 23 como si esa situación hubiera ocurrido en Venezuela.

30 Santiago MIR PUIG, "Derecho Penal", *op, cit*., p. 529

31 Santiago MIR PUIG, "Derecho Penal", *op, cit*., p. 530

3.1.2. Pasivo: Es especial o determinado. Debe ser el "propietario" de "…un *software* u otra obra del intelecto…". El tipo penal establece una característica especial en la víctima: debe ser el propietario. Aquí, debe atenderse a la normativa civil ordinaria o especial en materia de transmisión de propiedad, pues son muchas las formas de que esta se produce, en los ámbitos civil (Ej. compraventa civil, donación, transmisión *mortis causa*, etc.), mercantil (Ej. compraventa mercantil), administrativo (Ej. expropiación, nacionalización y comiso), e incluso penal (Ej. confiscación), por citar los casos más representativos.

Por tanto, una persona natural puede ser víctima del delito pero también puede serlo una persona jurídica, ya que ambas pueden ser titulares de derechos y deberes, concretamente, de ser propietarias.

3.2. Objetos

3.2.1. Material: La acción recae sobre el "… *software* u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información…".

Se trata de obras que si bien no están disponibles únicamente en formato digital deben haberse obtenido estando almacenadas en un sistema informático para que se produzca la conducta típica. Una canción, una pintura, un poema, un texto literario o científico pueden estar disponibles en papel u otro formato no informático pero solo será si la acción recae sobre su versión obtenida de un entorno digital lo que pena la norma.

3.2.2. Bien jurídico protegido: El tipo penal se encuentra en el capítulo "Delitos contra el orden económico" y es porque se protege la propiedad de bienes que por estar en un entorno digital pueden reproducirse, modificarse, copiarse, distribuirse o divulgarse con facilidad.

No se intenta proteger la creación intelectual sino los beneficios económicos que pudieran derivarse de tal elaboración, en principio humana, pero que a partir de la inteligencia artificial pudiera tener otro origen.

3.3. Medio de comisión

La reproducción, modificación, copia, distribución y divulgación de obras de creación intelectual obtenidas mediante acceso a sistemas informáticos pudiera efectuarse por cualquier medio, salvo en ciertos casos.

Si se trata de un programa de computación o *software* su reproducción, modificación o copia tendría que realizarse por medios informáticos, dada su naturaleza; mientras que la distribución y divulgación pudieran hacerse manualmente mediante su venta en disco compacto, blu ray, o cualquier otro dispositivo de almacenamiento. En tales casos se estaría distribuyendo o difundiendo la creación intelectual que fue obtenida mediante el acceso a cualquier

sistema que utilice tecnologías de información sin necesidad de usar dichas tecnologías para tal fin.

Otras creaciones intelectuales como una imagen o texto, pueden ser fotografiadas con una cámara analógica y luego fotocopiadas o reproducidas manualmente o mediante otros procedimientos mecánicos. Si esto se ejecuta accediendo visualmente a la pantalla, por ejemplo, de una computadora, la información se estaría obteniendo mediante el acceso visual a un *hardware* (la pantalla) que forma parte de un sistema informático, y en consecuencia se perpetraría el delito tipificado en el artículo 25 incluso sin valerse, como medio de comisión, de sistemas informáticos.

Resumiendo, en ciertos supuestos el medio de comisión es informático y en otros, genérico o indeterminado, siempre que el objeto material sea una creación intelectual obtenida de un sistema informático.

3.4. Parte objetiva del tipo

La conducta externa consiste en reproducir, modificar, copiar, distribuir o divulgar un *software* u otra obra del intelecto, sin autorización de su propietario, que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información.

La parte objetiva incluye cinco conductas típicas o verbos rectores. Veremos algunas de las acepciones que recoge el diccionario de la Real Academia Española al respecto:

a. Reproducir[32]: significa "Sacar copia de algo, como una imagen, un texto o una producción sonora" y "Hacer que se vea u oiga el contenido de un producto visual o sonoro"[33].

b. Modificar: es "Transformar o cambiar algo mudando alguna de sus características"[34].

c. Copiar: "Escribir en una parte lo que está escrito en otra", "Trasladar a un escrito lo que alguien dice de viva voz", "Reproducir textos, imágenes, sonidos u objetos", e "Imitar servilmente a un autor, a un artista, una obra o su estilo"[35].

d. Distribuir: "Entregar una mercancía a los vendedores y consumidores"[36]

e. Divulgar: "Publicar, extender, poner al alcance del público algo"[37]

32 Ley de Derechos de Autor: "Artículo 41. La reproducción consiste en la fijación material de la obra por cualquier forma o procedimiento que permita hacerla conocer al público u obtener copias de toda o parte de ella, y especialmente por imprenta, dibujo, grabado, fotografía, modelado o cualquier procedimiento de las artes gráficas, plásticas, registro mecánico, **electrónico**, fonográfico o audiovisual, inclusive el cinematográfico" (énfasis añadido).

33 https://dle.rae.es/?w=reproducir

34 https://dle.rae.es/modificar?m=form

35 https://dle.rae.es/copiar?m=form

36 https://dle.rae.es/distribuir?m=form

37 https://dle.rae.es/divulgar?m=form

Para diferenciar los verbos reproducir y copiar, que pueden ser similares entre sí, puede entenderse reproducir como ejecutar o poner en funcionamiento, usar una obra del intelecto sin autorización del dueño, lo que requiere su previa fijación material en un medio que permita hacerla conocer al público u obtener copias de toda o parte de ella, tal como lo prevé el artículo 41 de la Ley de Derechos de Autor.

Así, quien reproduzca o en otras palabras, use un software "pirata", por haber sido adquirido sin los permisos necesarios, perpetrará la conducta típica de apropiación de propiedad intelectual.

Esto pudiera generar algunos problemas. Si una empresa dota a las computadoras de los empleados de software sin autorización del propietario, el uso que estos hagan pudiera encuadrarse en esta norma, y por tanto sancionarse según sus previsiones.

En este supuesto habría que diferenciar si los empleados conocen o no si la empresa tiene autorización para tal fin. En caso de no saberlo, y no tienen por qué saberlo, la conducta sería atípica, puesto que se requiere dolo como se verá luego. Ahora bien, si lo saben y aún así lo reproducen (lo usan), según la letra de la ley estarían perpetrando este delito.

Esta reproducción también aplicaría para obras musicales, cinematográficas y del ingenio en general, en las que el propietario no hubiera autorizado su uso.

Conforme a lo expuesto, se reservaría el verbo copia para su multiplicación en otro u otros dispositivos de la obra intelectual.

Por otra parte, parece necesario diferenciar los verbos "distribuir y divulgar", entendiendo en el primer caso la entrega de la creación intelectual, de forma individual o grupal y sin permiso del dueño; y por "divulgar", su reproducción pública para que cualquiera acceda a la referida creación o su puesta al alcance del público, aún sin reproducirla.

En los cinco supuestos de este tipo penal es fundamental que la acción se ejecute sin autorización del dueño y que el objeto material haya sido obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información.

La falta de autorización del dueño supone que deba tratarse de propiedad privada, en el sentido de que la ausencia de dueño permite su uso libremente, mientras que la obtención de la creación mediante acceso informático puede ser autorizada o no. El sujeto puede haber tenido autorización para acceder a la creación o pudo haberlo hecho indebidamente, en ambos casos, se perpetraría la conducta típica.

3.5. Parte subjetiva del tipo

Se trata de un tipo penal doloso, que requiere por tanto voluntad o querer realizar la conducta típica y conocimiento de que se está llevando a cabo.

Aunado al dolo, en este tipo penal hay un elemento subjetivo, ya que la conducta típica debe tener lugar "…con el fin de obtener algún provecho económico…".

Cualquier reproducción, modificación, copia, distribución y divulgación, indebida, de obras intelectuales obtenidas por medios informáticos no es punible, solo lo será aquella que se verifique con la intención de obtener provecho económico porque lo que se protege es la propiedad; o sea, que el dueño o quien este autorice, sea quien se lucre por la creación intelectual que le pertenece.

3.6. Tercera historia. Apropiación de propiedad intelectual: Suits (temporada 2, episodio 1).

Una empleada de una compañía editorial tuvo una idea para escribir un libro. Se la comenta a su jefa, y ésta, como trabaja con varios escritores le da la idea a un escritor a quien se le acababa el tiempo para producir una nueva obra literaria. El autor la acepta y escribe la novela, por lo que la empleada amenaza con demandar por apropiación de propiedad intelectual.

Es de advertir que la empresa se encuentra en proceso de fusión y no le conviene verse involucrada en un caso como este.

En la serie, el abogado de la empresa negocia con la empleada y llegan a un acuerdo extrajudicial.

Analizando el caso, se advierte que hubo acción o comportamiento humano libre y consciente porque no se manifestó ni probó su ausencia a causa de fuerza irresistible, movimientos reflejos o estado de inconsciencia. En el episodio, la jefa libremente le transmitió la idea al escritor y este, por decisión propia, escribió la novela que finalmente publicó la empresa.

Al analizar la tipicidad, la parte objetiva del tipo sanciona a quien reproduzca, modifique, copie, distribuya o divulgue una obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información.

Al no haber una obra intelectual, no puede haber apropiación de dicha obra, ya que solo se trata de una idea, la cual, está en la mente de la empleada quien se la contó a su jefa y esta, a su vez, se la narró al escritor, por lo que no fue obtenida mediante "… el acceso a cualquier sistema que utilice tecnologías de información…".

Al faltar este elemento, la conducta no puede encuadrarse en el tipo penal del artículo 25 LECDI, pero tampoco en la Ley de Derechos de Autor, cuyos artículos 119 y 120 tipifican la comunicación pública o reproducción no autorizadas de obras de ingenio, por cualquier medio excepto el telemático que se sanciona en la LECDI, lo cual tampoco ocurrió.

4. Oferta engañosa (artículo 26).

> Toda persona que ofrezca, comercialice o provea de bienes o servicios, mediante el uso de tecnologías de información, y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta, de modo que pueda resultar algún perjuicio para los consumidores, será sancionada con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias, sin perjuicio de la comisión de un delito más grave.

Este tipo penal incluye seis conductas típicas mediante tres verbos rectores con dos elementos objetivos para cada caso, que serán examinados individualmente en la parte objetiva, mas de modo conjunto en los demás elementos, como se ha venido haciendo.

4.1. Sujetos

4.1.1. Activo: Es indeterminado por cuanto puede perpetrarlo "Toda persona…" sin especificar una característica específica en el agente, que puede ser comerciante o solo un vendedor ocasional.

4.1.2. Pasivo: Igualmente es indeterminado, puesto que serían "los consumidores…" y esta es cualquier persona que compre bienes o contrate la prestación de servicios. El consumidor no es una categoría especial de sujeto sino la posición en que se puede encontrar cualquier persona cuando paga por una cosa o experiencia lícita.

4.2. Objetos

4.2.1. Material: Las acciones típicas recaen sobre "… bienes o servicios…" de cualquier naturaleza, siempre que sean legales en el país. No pudiera condenarse a quien ofrezca drogas de cierta calidad y finalmente entregue unas de menor calidad ya que no se trata de un bien válidamente comercializable en el país, por el contrario, se trataría de un delito.

Siguiendo el razonamiento expuesto, si el servicio ofrecido fuera de abuso sexual de niños o adolescentes, tampoco pudiera haber oferta engañosa, puesto que se trataría de un acto criminal.

4.2.2. Bien jurídico protegido: Se ha afirmado que en España es el interés económico de los consumidores[38], en este caso, sería el interés

38 César Chaves Padrón. "El delito de publicidad engañosa en España: algunas consideraciones político criminales y relativas al bien jurídico protegido.", tesis docoral, Universitat de Valencia, España, 2015, p. 212 disponible en: http://roderic.uv.es/bitstream/handle/10550/50500/Tesis%20Doctoral_C%C3%A9sar%20Chaves%20Pedr%C3%B3n.pdf?sequence=1&isAllowed=y

económico de los consumidores electrónicos, puesto que en el artículo 26 LECDI solo se sanciona la oferta engañosa en el entorno digital. Así mismo, se ha considerado la información veraz[39], a lo que también habría que agregar, en el caso venezolano, el adjetivo "electrónico" debido a las razones expuestas.

En Argentina, se ha expresado que es la lealtad en las relaciones comerciales[40], lo que *mutatis mutandi* para Venezuela, sería la lealtad en las relaciones comerciales telemáticas; mientras que en Perú, se ha aseverado que es el bienestar de una población afectada por un hecho calamitoso[41], lo que no pudiéramos aplicar al caso venezolano.

Los bienes jurídicos identificados en España y Argentina pudieran aplicarse al caso venezolano, en especial el relativo a la información veraz, pero adaptado al artículo 117 constitucional que establece el derecho fundamental de "Todas las personas… a disponer de… una información adecuada y no engañosa sobre el contenido y características de los productos y servicios que consumen…".

La información digital veraz sobre bienes y servicios, o en términos constitucionales "adecuada y no engañosa" puede estimarse como el bien jurídico protegido por el artículo 26 LECDI.

4.3. Medio de comisión

Es informático. La ley criminaliza la acción típica "…mediante el uso de tecnologías de información…". Si la acción se ejecuta por medios analógicos, en papel o a viva voz, no pudiera sancionarse al agente por este delito de publicidad engañosa tipificado en el artículo 26 LECDI.

Esto incluye: publicidad por redes sociales, portales de Internet, mensajes de datos vía teléfonos inteligentes (Ej. WhatsApp o Telegram), mensajes de correo electrónico o cualquier otra forma de comunicación e información telemática.

En caso de realizar la conducta típica pero sin usar tecnologías de información, pudiera aplicarse, según el caso, el segundo numeral 4 del artículo

39 Belén MACÍAS ESPEJO. *El delito de publicidad engañosa*. Vol. 29. Dykinson, España, 2016. p. 86

40 María Bibiana Nieto. (s.f.). Publicidad engañosa [en línea] (Documento no publicado. Facultad de Derecho. Universidad Católica Argentina). Disponible en: http://bibliotecadigital.uca.edu.ar/repositorio/investigacion/publicidad-enganosa-mariabibiana-nieto.pdf. P. 9.

41 Cóndor Córdova y Shirley Massiel Kirschen Korellei. "Propuesta Legislativa de incorporación de la Publicidad Engañosa como Delito de Estafa–caso Pura Vida." (trabajo de grado para obtar al título de abogados), Universidad Nacional Pedro Ruiz Gallo, Perú, 2019, p. 26. Disponible en: http://repositorio.unprg.edu.pe/bitstream/handle/UNPRG/3315/BC-TES-2169.pdf?sequence=3&isAllowed=y

49 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de Precios Justos[42] por lo que la actuación no quedaría impune.

4.4. Parte objetiva del tipo

La conducta perceptible por los sentidos radica en ofrecer, comercializar o proveer de bienes o servicios, mediante el uso de tecnologías de información, haciendo alegaciones falsas o atribuyendo características inciertas a cualquier elemento de dicha oferta, de modo que pueda resultar algún perjuicio para los consumidores.

Los tres verbos rectores usados por el legislador son, *ofrecer* que significa "Comprometerse a dar, hacer o decir algo"[43]; *comercializar*, "Dar a un producto condiciones y vías de distribución para su venta" y "Poner a la venta un producto"[44]; así como *proveer*, que es "Suministrar o facilitar lo necesario o conveniente para un fin"[45], los que pudieran interpretarse del modo siguiente:

El hecho de ofrecer en venta permite sancionar al sujeto activo aunque no se concrete la venta, bastando una sola voluntad para que se verifique el tipo penal; e incluso, aunque no disponga del producto sino que sea un intermediario.

La comercialización implica un hacer por parte del sujeto activo, bien sea como proveedor al distribuidor, en condición de fabricante o importador; de distribuidor, vendiendo al mayor; o de vendedor al detal o al por menor, permanente o eventual.

Y por último, proveerá el producto quien efectivamente lo posea y pueda garantizar su entrega sin depender de otro.

En todos los supuestos deben hacerse alegaciones falsas o atribuirse características inciertas a cualquier elemento de dicha oferta. Se trata de elementos creíbles, que puedan confundir, engañar o sorprender en la buena fe a un consumidor razonable[46] puesto que los claramente fantasiosos o humorísticos no permitirían atribuirle la capacidad de sorprender en la buena fe a los compradores.

Para que la conducta sea sancionable debería mentirse u omitirse la verdad, en este último caso, conforme a las previsiones del ordenamiento jurídico ya que no hay obligación de publicitar un bien o servicio y afirmar que el de la competencia es más económico o de mejor calidad, pero lo que sí no puede hacer es afirmar que el costo es el menor del mercado cuando ello no fuera cierto, u omitir que contiene determinada sustancia (Ej. gluten o maní) cuando

42 Gaceta Oficial Número 6.202, Extraordinario, del 8 de noviembre de 2015.

43 https://dle.rae.es/?w=ofrecer

44 https://dle.rae.es/comercializar?m=form

45 https://dle.rae.es/proveer?m=form

46 "The FTC Deception Policy Statement defines a practice as deceptive if it is likely to misleadingly influence a reasonable consumer". Andrew Rhodes, y Chris M. Wilson. "False advertising." *The RAND Journal of Economics*, 49.2, 2018, pp. 348-369.

realmente sí lo contiene, puesto que en tales caso pudiera atentarse incluso contra la vida, lo que pudiera constituir otro delito o un concurso de delitos.

Adicionalmente, hay un elemento objetivo que debe estar presente: "… que pueda resultar algún perjuicio para los consumidores…". No bastan alegaciones falsas o atribuirle características inciertas a algún elemento de la oferta, sino que debe existir la posibilidad de que a partir de tales conductas pueda perjudicarse a los consumidores.

No se requiere el resultado dañoso sino que basta con la puesta en peligro del consumidor, de quienes dependan económicamente de él, o de sus bienes, ya que en los tres casos se les estaría perjudicando, bien mediante daño emergente o lucro cesante.

4.5. Parte subjetiva del tipo

Es un tipo doloso de acción u omisión, en los casos en que se omite una información que corresponda incluir por ley, por tanto, quien no quiera el resultado típico y desconozca que está realizando la conducta típica, no podrá ser condenado por este delito.

4.6. Cuarta historia. Oferta engañosa: Fyer, la fiesta más exclusiva que nunca sucedió[47]

Una compañía estadounidense promocionó en las redes sociales el festival hotelero, gastronómico y musical más importante del siglo. Influenciadores con miles y millones de seguidores le hicieron publicidad, logrando que las personas pagaran entre dos mil y doce mil dólares americanos por asistir.

Al llegar a las Bahamas, el traslado era en un autobús básico, la comida *gourmet* eran sánduches con queso, y el alojamiento "de lujo" eran carpas usadas para catástrofes climáticas, con colchones mojados por la lluvia.

Los grupos musicales que se presentarían cancelaron su participación por lo que solo había un *dj* reproduciendo música.

En este caso, independientemente de los otros delitos que pudieron perpetrarse y por los que fue condenado a prisión el organizador del evento, hay que precisarse si pudiera tratarse de un caso de oferta engañosa a la luz del artículo 26 LECDI.

En cuanto al primer elemento del delito, hubo acción libre de la empresa, por decisión de sus órganos, con sus recursos y en su propio interés de ofrecer un servicio con el que no podían cumplir. No hubo causa alguna que excluyera la acción, en efecto, en el documental hay declaraciones de los colaboradores del organizador manifestándole que desistiera sin que él aceptara las recomendaciones.

47 Visto en Netflix en octubre de 2019.

La tipicidad también se cumple ya que la empresa ofreció y comercializó servicios (traslado, alojamiento, alimentación y música) a los asistentes, mediante el uso de tecnologías de información, puesto que la publicidad se hizo mediante redes sociales, el portal de Internet de la empresa y por correo electrónico, alegando prestaciones que no podían cumplir (presentación de grupos musicales) o atribuyendo características inciertas a cualquier elemento de dicha oferta (servicios de lujo), perjudicando a los consumidores que pagaron por un servicio que no recibieron, y que de haber conocido la realidad, posiblemente no hubieran pagado la cantidad que se les cobró o ni siquiera hubiesen considerado asistir.

La conducta también es antijurídica porque no hay causas de justificación para actuar como lo hizo la empresa y el organizador del festival.

Por último, tanto la empresa como el director son imputables por tener la capacidad de decidir y conocer lo que estaban haciendo.

Conclusión

La televisión, como el cine, la literatura y el arte en general, ofrecen, además de entretenimiento, la oportunidad de reflexionar sobre diversas materias según el interés de cada quien, en este caso sobre el Derecho Penal desde una perspectiva informática o más ampliamente, de las tecnologías de información y comunicación.

Black Mirror, Dark Net, Suits, y Fyer sirvieron de ejemplo sobre cómo se pueden obtener casos que permitan analizar el ordenamiento jurídico a partir del conocimiento científico.

En ciertas ocasiones, la conducta desplegada por el agente pudo subsumirse en la previsión normativa, y aunque en otros no fue posible, todos permitieron el análisis estructural de los último cuatro tipos penales de la LECDI tal como se propuso desde el principio.

En el episodio de Black Mirror, se advirtió la perpetración del tipo penal "difusión o exhibición de material pornográfico", puesto que se transmitió por un medio de comunicación libre y masivo, material reservado para adultos sin advertir su contenido para tomar las precauciones necesarias a fin de proteger a los niños y adolescentes bajo su responsabilidad.

En el capítulo analizado de Dark Net, la "exhibición pornográfica de niños o adolescentes" quedó claramente ilustrada, al usar a una niña para transmitir su imagen teniendo relaciones sexuales, usando una cámara web, un programa de videoconferencia e Internet.

En Suits, pudo apreciarse lo que no es "apropiación de propiedad intelectual" para lo que debió seguirse el mismo análisis de la estructura de los tipos penales que se hubiera tenido que efectuar para llegar a una conclusión diferente, por lo que se pudieron poner de manifiesto los elementos de este tipo penal que a diferencia de la Ley Especial de Derecho de Autor, requiere un elemento subjetivo adicional: el ánimo de lucro.

Por lo que concierne al documental "Fyer, la fiesta más exclusiva que nunca sucedió", este muestra los perjuicios que puede ocasionar la oferta engañosa, aunque en el caso concreto el organizador de la actividad fue condenado por otros delitos por los daños sufridos por los inversionistas.

Para finalizar, es importante tener presente que los cuatro tipos penales referidos son delitos informáticos aunque no en todos los supuestos se prevé que deban ser perpetrados por medios informáticos, lo que lleva a concluir que el concepto de delito informático que informa la LECDI, no en todos los casos precisa de medio de comisión especial, puesto que en ciertas ocasiones pueden materializarse por cualquier medio, no solo informático, y aún así se consideran como tales por su ubicación en la LECDI, esto es, con base en una noción formal, aunque en estos casos siempre está presente el elemento informático constituido por el objeto material, que puede ser digital o, como en algunos de los tipos penales descritos, puede estar en otro formato siempre que originalmente se hubiera obtenido de medios digitales.

Algunas consideraciones sobre el uso de las redes sociales para la difusión y comercialización de la pornografía infantil en Venezuela

Liliana Del Valle García Ojeda*

SUMARIO: Introducción. 1. Nociones generales de la pornografía infantil. 2. Uso de las redes sociales para captar a los niños, niñas y adolescentes para difundir y comercializar pornografía infantil. 3. medios de difusión y comercialización de material pornográfico de los niños, niñas y adolescentes a través de las redes sociales. 4. Consecuencias penales del uso de las redes sociales para la difusión y comercialización del material pornográfico de los niños, niñas y adolescentes en Venezuela. Conclusiones.

Resumen

Las tecnologías de la Información y la Comunicación (TICS), pueden ser muy útiles pero también son herramientas usadas por las personas que realizan hechos delictivos, como por ejemplo la pornografía infantil, la cual se difunde y se comercializa a través de las diversas redes sociales, captando a los niños, niñas y adolescentes, por tal motivo el artículo científico desarrollará las consecuencias penales del uso de las redes sociales para la comisión de este delito.

Palabras clave: TICS. Pornografía Infantil. Difusión. Comercialización. Delito.

Recibido: 29/1/2020 • Aceptado: 12/2/2020

* Técnico Superior Universitario en Administración Tributaria con Mención Honorífica, egresada del Instituto Universitario de Tecnología de Administración Industrial (IUTA), Licenciada en Administración Mención Recursos Materiales y Financieros, egresada de la Universidad Nacional Experimental Simón Rodríguez (UNESR), Abogada, egresada de la Universidad José María Vargas (UJMV), Especialista en Ejercicio de la Función Fiscal por la Escuela Nacional de Fiscales del Ministerio Público, y cursando el Doctorado en Derecho en la Universidad Católica Santa Rosa. Se desempeña como Abogada Adjunto IV en la Fiscalía Tercera del Ministerio Público para actuar ante la Sala Plena, Constitucional y Salas de Casación del Tribunal Supremo de Justicia. Email: lilianavgarcia@hotmail.com

Abstract

Information and Communication Technologies (ICT) can be very useful, but these are also tools used by people who carry out criminal acts, such as child pornography, which is disseminated and marketed through social networks, capturing children and adolescents. For this reason, the scientific article will develop the criminal consequences of the use of social networks for the commission of this crime.

Keywords: TICS. Child pornography. Diffusion. Commercialization. Crime.

Introducción

El hombre se ha visto en la necesidad de adaptarse a cambios inesperados para poder formar parte de una sociedad moderna, por supuesto estos son producto de movimientos sociales, políticos y económicos que afectan directa e indirectamente su vida y que muchas veces no sabe cómo manejarlos y termina envuelto en algún tipo de hecho punible.

Al respecto, se puede mencionar el uso de las Tecnologías de la Información y la Comunicación (TICS), que con el transcurrir del tiempo han desplazado al hombre, en gran parte de su operacionalidad en las distintas actividades que realiza a nivel laboral, social, personal y familiar.

El instrumento fundamental de las TICS es el internet, que juega un papel importante para mejorar sustancialmente la comunicación y la información de los seres humanos, haciendo así la vida más fácil, pero a su vez convirtiéndose en un elemento peligroso para la planificación y ejecución de delitos mediante las diferentes redes sociales que en la actualidad tienen un rol fundamental en las relaciones interpersonales del hombre.

En ese sentido, resulta relevante analizar las consecuencias penales del uso de las redes sociales para la difusión y comercialización de la pornografía infantil en Venezuela, a objeto de buscar alternativas que permitan coadyuvar a la comisión de este hecho punible, siendo indispensable revisar lo contemplado en la Ley Orgánica Para la Protección de Niños, Niñas y Adolescentes y la Ley Especial contra los Delitos Informáticos.

Desde esta perspectiva, la presente investigación pretende desarrollar los siguientes objetivos: a) describir el uso de las redes sociales para captar a los niños, niñas y adolescentes para difundir y comercializar la pornografía infantil, b) establecer los medios de difusión y comercialización de material pornográfico de niños, niñas y adolescentes a través de las redes sociales y c) determinar las consecuencias penales del uso de las redes sociales para la difusión y comercialización del material pornográfico de los niños, niñas y adolescentes.

1. Nociones generales de la pornografía infantil

Es necesario antes de desarrollar el tema de la pornografía infantil, tener claro la definición general de pornografía, haciendo énfasis en la que plantea Cabanellas (2016), la pornografía la define como: "Tratado sobre la prostitución, obscenidad o salacidad en las obras literarias o artísticas, obra o escrito lascivo. Conjunto de dibujos, grabados o pinturas obscenos"[1].

Por su parte, las Naciones Unidas de los Derechos Humanos a través del Protocolo Facultativo de la Convención Sobre los Derechos del Niño Relativo a la Venta de Niños, la Prostitución Infantil y la Utilización de Niños en la Pornografía, en su artículo 2, literal c) define a la pornografía infantil como "toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales"[2].

Según Morales (2007), La pornografía infantil se puede clasificar de la siguiente manera[3]:

Según los materiales o contenidos:

a) Pornografía leve o suave: En este tipo de pornografía no hay actividad sexual explícita, pero implica imágenes desnudas "seductoras e insinuantes" de niños, niñas o personas con aspectos de niños, niñas ya adolescentes. Incluye exhibición de estos en distintas posturas eróticas, pero no su participación en ningún comportamiento sexual.
b) Pornografía dura o Fuerte: consiste en la exhibición de acceso carnal, actos sexuales explícitos o ambos, en los que participan niños, niñas, adolescentes o personas con indicios de ser menores de 18 años.

Según el fin:

a) Pornografías comercialmente producidas con fines de lucro.
b) Pornografías producidas para ser circuladas e intercambiadas.
c) Pornografía utilizada con otros fines delictivos (chantaje, trata, entre otros)
d) Pornografía producida para consumo exclusivamente personal, entre otros.

De acuerdo con lo antes expuesto, se puede entender que la pornografía infantil son todas aquellas actividades que se caracterizan por ser y tener un elemento representativo, gráfico y visual realizado con niños, niñas y adolescentes

1 Guillermo CABANELLAS DE TORRES: *Diccionario Jurídico* 18ª ed., Buenos Aires, 2006, p. 296.

2 Publicada según la Asamblea General, Resolución A/RES/54/263 DEL 25de mayo de 2000, entró en vigor el 18 de enero de 2002.

3 MORALES, D (2007) "La pornografía infantil en la legislación venezolana", *Estudio de Ciencias Penales y Criminológicas*, Universidad Católica Andrés Bello, 2.007, pp. 9-10.

con fines sexuales y que en muchas ocasiones existen personas que se dedican a convertir esta práctica en un negocio lucrativo, las cuales se encargan de captar a estas víctimas vulnerables mediante cualquier medio, específicamente a través de las redes sociales que son en la actualidad un boom en la juventud.

Ahora bien, el motivo por el cual el internet[4] y las redes sociales se han convertido en una alternativa de comunicación e intercambio de información entre los niños, niñas y adolescentes, es porque estas se asemejan y representan la convivencia juvenil personalmente que antes se hacía en la calle a través de los juegos de mesas y las prácticas de deportes al aire libre, no obstante también son indicativo de que corren riesgo, están expuesto al peligro y pueden ser captados para la práctica de la pornografía infantil[5].

Por otra parte, hay que considerar que la necesidad genuina de los adolescentes de interactuar virtualmente con otros jóvenes no es solo el factor indispensable para que se pueda dar la pornografía infantil, también hay que tomar en consideración el interés que tienen los individuos desde el punto de vista sexual en los niños, niñas y adolescentes, y que actúan con libertad en el mundo virtual para utilizar los canales y recursos no solo para captar nuevas víctimas sino también para difundir y comercializar videos, fotos entre otros con contenido pornográfico[6].

Es por ello, que la pornografía infantil cada día rompe los esquemas y las barreras de seguridad a nivel mundial, convirtiéndose así en un monstruo depredador sexual de niños, niñas y adolescentes de todos los países, sin importar raza, religión ni condición social, por tal motivo todas las naciones deben manejar una sola contienda en contra de este delito como lo es "la lucha contra la pornografía infantil", siendo necesario que se maneje el término universal correcto en los hechos que permitan identificar que se está en presencia de este delito.

En tal sentido, INTERPOL ha propuesto una lista de terminología adecuada para ser usada en los hechos relacionados con la pornografía infantil, y que

4 CHEN, Caterina: "Es el conjunto de tecnologías desarrolladas en la actualidad para una información y comunicación más eficiente, las cuales han modificado tanto la forma de acceder al conocimiento como las relaciones humanas". En "TIC (Tecnologías de la información y la comunicación)". Disponibles en: https://www.significados.com/tic/Consultado: [Consultado: 2019, septiembre 05].

5 Al respecto, la OEA en el informe relacionado a la explotación sexual comercial de niños, niñas y adolescentes e Internet del año 2010, manifiesta lo siguiente "En Internet los niños, las niñas y los adolescentes experimentan roles sociales y van actualizando la imagen que tienen de sí mismos. Internet es un espacio que hace las veces de "la calle" o la "placita", de este lugar público donde los adultos no dominan la interacción y donde los adolescentes sociabilizan y se definen a sí mismos en conjunto a su tribu, a su banda, a sus iguales." Disponible en: http://iin.oea.org/boletines/boletin7/noticias-novedades-esp/x-Informe-escnna.pdf [Consultado: 2019, septiembre 05].

6 LEMINEUR, Marie: El combate contra la pornografía infantil en Internet, Caso de Costa Rica. http://white.lim.ilo.org/ipec/documentos/pornografia.pdf diciembre 2006. [Consultada: 2019, septiembre, 05]

muchos países hacen uso de ella en sus diferentes normativas, específicamente aquellas que están destinadas a la protección de los niños, niñas y adolescentes.

A continuación se presenta el cuadro con las terminologías propuestas por INTERPOL[7]:

Términos a evitar o utilizar con precaución	**Recomendado**
Pornografía Infantil	Abuso Sexual de Menores
Turismo Sexual que Afecta a Menores	Explotación Sexual de Niños, Niñas y Adolescentes en Viajes y Turismo
Turistas Sexuales que Viajan para Abusos de Menores	Autores Itinerantes de Delitos Sexuales Contra Niños, Niñas y Adolescentes
Prostitución Infantil	Explotación de Niños, Niñas y Adolescentes a través de la Prostitución.
Niño Prostituto, Niño Trabajador del Sexo	Víctima de Explotación Sexual.
Consumidor o Cliente	Abusador, Autor de Delitos Sexuales Contra Niños, Niñas y Adolescentes.
Turismo Sexual Infantil por WebCam/ Abuso Sexual Infantil por WebCam	Abuso Sexual de Niños, Niñas y Adolescentes en Directo en Línea.

En relación con esto, Venezuela en la Ley Orgánica para la Protección del Niño y del Adolescente (1998), establece en su artículo 237 lo relacionado a la pornografía con niños o adolescentes y en la Ley Orgánica para la Protección de Niños, Niñas y Adolescentes (2015), hace mención de la explotación sexual de niños, niñas y adolescentes en su artículo 258 y en el artículo 259 y 260 se refiere al abuso sexual a niños, niñas y adolescentes, mientras que en la Ley Especial Contra los Delitos Informáticos (2001) en sus artículos 23 y 24 indican la terminología de material pornográfico, por último en la Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo (2011) en sus artículos 46, 47 ,48 y 49 se utiliza la palabra pornografía, difusión y elaboración de material pornográfico con niños, niñas o adolescentes.

7 www.interpol.int/es/Delitos/Delitos-contra-menores/Terminologia-apropiada. [Consultada: 2019, octubre 27]

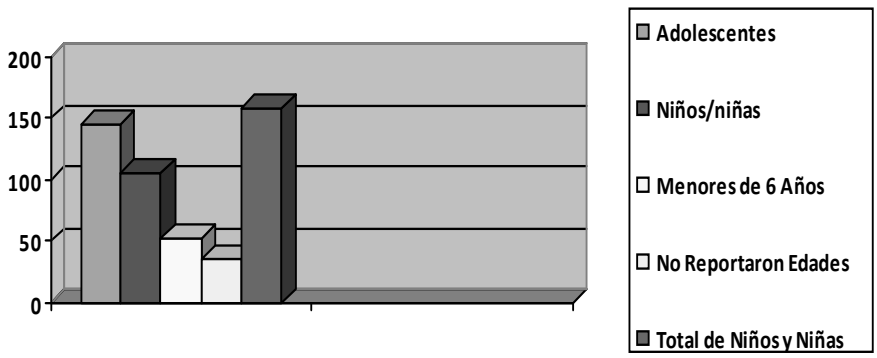
En función de lo antes expuesto, se puede visualizar que en estos instrumentos jurídicos venezolanos, la única ley que hace uso de la recomendación de INTERPOL es la Ley Orgánica para la Protección de Niños, Niñas y Adolescentes, mientras que las otras dos normas aún continúan haciendo uso de la palabra "pornografía", sin ser éste considerado como un factor para que este delito pierda su validez y conceptualización de hecho punible; de igual forma se observa que se omite el vocablo menores y se usa niños, niñas y adolescentes.

En definitiva, lo importante es destacar en esta investigación que en Venezuela el delito de pornografía infantil ha tomado una fuerza indescriptible en la sociedad, de acuerdo con las estadísticas presentadas en el informe "Somos Noticias" 2017, realizado por el Centro Comunitario de Aprendizaje (CECODAP), en relación con las muertes y otras formas de violencia contra niños, niñas y adolescentes en un contexto de emergencia humanitaria, estableciendo que el delito por violencia sexual presenta un total de 341 casos por violencia sexual por sexo. A continuación se presentan las cifras ofrecidas por CECODAP.

1. Rango de edad por violencia sexual

Violencia Sexual por Grupos de Edades Año 2017	
Rango de Edad	**Número de Víctimas**
0 meses a 6 años	53
7 a 11 años	106
12 a 17 años	146
No Reportaron Edades	36
Total:	**341**

Fuente: Registro Hemerográfico CECODAP



Fuente: Registro Hemerográfico CECODAP

Agredidos: 106+53=159

En función de lo que establece CECODAP[8] en su informe el análisis de los datos estadísticos proporcionados generaron la siguiente conclusión:

> La violencia sexual ocurre en las diferentes edades, contra adolescentes en la mayoría de los casos, pero también agrediendo a niñas y niños de corta edad. De 0 a 6 años se registran 53 casos, lo que interpela nuestra capacidad como sociedad para proteger a la niñez y para afirmar convicciones éticas tan esenciales como el respeto a la vida, la integridad personal y a la protección de la población más vulnerable. El abuso sexual es un crimen contra toda persona, pero en estos casos, es una actuación infame de quien se degrada como persona, al someter y violentar al otro, justo por su condición de debilidad e indefensión.

Fue necesario, plasmar en esta investigación las cifras de violencia sexual contra los niños, niñas y adolescentes por ser esta una forma generada por la explotación sexual (pornografía infantil), que se ha convertido en un medio comercial y laboral para aquellas personas capaces de hacerle daño a un ser inocente e indefenso como lo son los niños, niñas y adolescentes, quienes son víctimas fáciles para la comisión del delito de difusión y comercialización de material pornográfico infantil y de adolescentes, las cuales la sociedad y el Estado no han podido erradicar por completo este hecho punible.

Eso es lo que respecta a la violencia con sexo pero hay que considerar también la violencia que atenta la integridad física y psicológica, contra la dignidad de los niños, niñas y adolescentes cuando estos son forzados a realizar

8 CECODAP: Muerte y Otras Formas de Violencia Contra Niños, Niñas y Adolescentes en un Contexto de Emergencia Humanitaria. Informe Somos Noticia 2017. CECODAP.org.ve/ descargables/derechos NNA/Somos-Noticia-2017-2018. Pdf/www.unicef.org.

cualquier acto en contra de su propia voluntad, en tal sentido no solo se puede hablar de una violencia con sexo sino también de una violencia sin sexo[9].
La finalidad que tuvo el desarrollo de este primer epígrafe en este artículo fue mostrar de manera general los aspectos más relevantes que se deben tener en cuenta cuando se está en presencia del delito de pornografía infantil, siendo estos la explotación sexual de los niños, niñas y adolescentes, la difusión y comercialización de material pornográfico y que estos actos se realicen en contra de la voluntad de estas víctimas vulnerables.

2. Uso de las redes sociales para captar a los niños, niñas y adolescentes para difundir y comercializar pornografía infantil

La importancia que tiene en la investigación el desarrollo de este punto es darle los nombres tecnológicos a las acciones que realizan los victimarios para captar a las víctimas de la pornografía infantil, encontrando en primer lugar lo que se denomina como *Grooming,* siendo este definido por la Oficina de las Naciones Unidas Contra la Droga y el Delito (UNODC), en su guía denominada "Mini Guía de Seguridad en Internet (Todo lo que tienes que saber)" como:

> Las acciones que realiza un adulto utilizando engaños y mentiras que buscan ganarse la confianza de niños, niñas y adolescentes, haciendo uso de las tecnologías de información y comunicación. El *Grooming* es utilizado como un medio para cometer los delitos de violencia sexual, explotación y trata de personas[10]

9 Al respecto, la OEA en el informe relacionado con la explotación sexual comercial de niños, niñas y adolescentes e Internet del año 2010, manifiesta lo siguiente "La explotación sexual de niños, niñas y adolescentes es un ejercicio abusivo de poder, en el cual el niño se encuentra en situación de clara desigualdad: menor poder, menor fuerza, menor edad, etc. Las distintas modalidades de ESCNNA son parte de las aún más numerosas formas de violencia sexual contra los niños". *Op.cit*., pp. 20.

10 La Oficina de las Naciones Unidas Contra la Droga y el Delito (UNODC), en su guía denominada "Mini Guía de Seguridad en Internet (Todo lo que tienes que saber) también expresa lo siguiente: "Las personas que hacen Grooming suelen utilizar las redes sociales, chats, juegos en línea y foros para contactar y hacer amistad con sus víctimas. Los atrae con un perfil atractivo para brindar confianza. En sus conversaciones expresa los mismos gustos y emociones, y utiliza las mismas expresiones, lenguaje, emoticones (figuritas) para simpatizar con sus víctimas. Se presenta como el amigo (a) o novio (a) perfecto (a). Asimismo, establece las fases del Grooming:

Fase 1: Identifica y/o contacta a la víctima usando perfiles falsos, invitándole a ser su amigo (a).

Fase 2: Querrá asegurarse que el niño, niña y adolescente quiera hablar con él, le conversará sobre temas de su interés; le hablará de su situación familiar, relaciones sentimentales con el fin de crear un vínculo de amistad; hará preguntas sobre su edad y ubicación, e intentará conocer sus gustos para adaptarse a ellos. Su objetivo es ganarse su confianza.

Es decir, que las mentiras y los engaños que usan las personas que fomentan la pornografía infantil y la trata de personas para reclutar no solo a niños, niñas y adolescentes, sino también a los adultos se denomina *grooming;* al respecto, se puede mencionar como ejemplo las agencias de modelos que usan las redes sociales para atraer a los jóvenes que ellos consideran aptos para el negocio.

La autora de la investigación propuesta por experiencia profesional, opina que los niños, niñas y adolescentes por ser personas vulnerables y genuinas suelen enviar o recibir imágenes y vídeos de otros jóvenes con poca o sin ropa que generen suspicacias sexuales, a través de sus redes sociales, chat o correo electrónico, sin tener la malicia de pensar que no es una diversión, sino una invitación tácita de repetir esa conducta, en virtud que esta es una forma de captar su atención y jamás imaginan que la exposición de esas imágenes o vídeos con contenidos sexuales suelen generarles un grave daño a la privacidad e integridad de ellos y de sus familiares. Una vez que los niños, niñas y adolescentes caen en la trampa de enviar imágenes y vídeos (inclusive los que se hacen a través de la cámara de la computadora) no saben que pierden el control de ese material, pudiendo ser difundidos y comercializados por internet.

Por otra parte, la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), establece que existen otros dos medios que utilizan los victimarios de la pornografía infantil y que demuestran claramente que se está en presencia de este delito, entre los cuales se pueden mencionar el *Sexting* (mensajes sexuales) y el *Sextortion* (chantaje sexual)[11].

Fase 3: Obtiene contenido íntimo que le permitirá ejercer presión sobre su víctima.» Disponible En: https://www.unodc.org/documents/ropan/MINI_GUIA_DE_SEGURIDAD_EN_INTERNET_UNODC_ROPAN.pdf [Consultada: 2019, septiembre, 05]

11 La Oficina de las Naciones Unidas Contra la Droga y el Delito (UNODC), en su guía denominada "Mini Guía de Seguridad en Internet (Todo lo que tienes que saber), los define de la siguiente manera:

"El Sexting es el envío o recepción de contenido de tipo sexual (principalmente fotografías o vídeos) los cuales son producidos por quien los envía a través de las tecnologías de información y comunicación. El Sexting se puede dar de dos formas: de manera voluntaria y de manera involuntaria.

a) De manera voluntaria:

- Cuando a través de engaños envías fotografías y/o vídeos con poca o sin ropa, a personas que han ganado tu confianza pero no conoces en la vida real.

- Cuando en una relación sentimental o de amistad envías fotografías y/o vídeos con poca o sin ropa.

a) De manera involuntaria:

- Cuando durante una conversación a través de una cámara de computadora, esta puede capturar y/o grabar imágenes que pueden ser publicadas en Internet.

- Cuando a pesar de utilizar contraseñas y otros mecanismos de seguridad las fotografías y vídeos del celular o computadora puedan compartirse en Internet por robo, error, broma o extravío.

Se puede citar como ejemplo de lo anteriormente expuesto, lo que sucede entre los adolescentes cuando se toman una *selfie* con actitudes provocativas porque lo consideran normal y resulta que se lo comparten entre los amigos y uno de ellos es captador de niños, niñas y adolescentes para la pornografía infantil y la trata de niños, niñas y adolescentes.

De acuerdo con las investigaciones revisadas durante el proceso de desarrollo de este artículo científico, se pudo obtener como información que algunas personas utilizadas como captadores de niños, niñas y adolescentes para la pornografía infantil, consideran que no están cometiendo ningún tipo de delito, quizás por ignorancia o por desconocimiento de las leyes, además manifiestan que ellos no son los que directamente los comercializan, bien sea a través de material pornográfico por internet o por la trata de personas, lamentablemente están en un grave error, porque cualquier persona que realice las siguientes actividades con niños, niñas y adolescentes estaría inmerso en el delito de la pornografía infantil, según lo que afirmado por Sallent (2016) en su escrito denominado la pornografía infantil a través de las redes informáticas. Responsabilidad, tenencia y distribución dentro del Derecho Penal Argentino:

> 1. Los individuos que produzcan, financien, ofrezcan, publiquen o distribuyan mediante el internet o las diversas redes sociales material con información de contenido sexual con niños, niñas y adolescentes.
> 2. En el caso que personas adultas realicen acciones de producir, crear e incluso participar en actividades sexuales con niños, niñas y adolescentes.
> 3. Las personas que decidan financiar económicamente, comercializar, publicar la elaboración de material pornográfico de niños, niñas y adolescentes.
> 4. Ofrecer la plataforma digital que posibilite el acceso a material pornográfico e naturaleza pedófilos
> 5. Los individuos que reúnan a un grupo de niños, niñas y adolescentes para ingresar a una página pornográfica o a ver videos con imágenes pornográficas[12].

Según el planteamiento de Sallent, se puede detectar y determinar rápidamente a nivel mundial cuando un individuo o un grupo de personas se

- Cuando confías en alguien y pide fotografías comprometedoras para que le demuestre que confía en esa persona y es para otros fines.

El Sextortion es una forma de amenaza que sucede después que una persona ha logrado ganarse la confianza de alguien y obtiene imágenes o videos con contenido sexual. El chantaje se da cuando el agresor a cambio de no publicar las imágenes o videos, obliga a su víctima a realizar acciones que ponen en peligro su integridad, como relaciones sexuales involuntarias, producir pornografías infantiles u otras acciones que pueden poner en peligro la vida de la persona". *op.cit*.

12 SALLENT, F. (2016) "La pornografía infantil a través de las redes informáticas. Responsabilidad, tenencia y distribución dentro del Derecho Penal argentino", *Estudios de Derecho Penal*, Universidad Siglo 21, Argentina 2016, pp. 9.

encuentran inmersos en el delito de la pornografía infantil, en virtud que existen unas series de ítems característicos del referido hecho punible.

Asimismo, es importante destacar que Sallent también señala que existen diversos programas tales como E-Mule, E-Donkey, Ares, entre otros que posibilitan que los usuarios compartan contenido en una menor cantidad de tiempo (a diferencia de las comunes descargas "downloads" que se hacen directamente de una página web), que conllevan fácilmente a la comisión del delito de la pornografía infantil por parte de los agresores y autores intelectuales de este delito tan miserable.

Se puede concluir en este aparte de la investigación que desde el punto de vista tecnológico las acciones que enmarcan el delito de la pornografía infantil, universalmente tienen un nombre característico en el mundo virtual y a su vez se pudo describir de qué manera los partícipes de este hecho punible captan a los niños, niñas y adolescentes a través de las redes sociales, destacando en primer lugar que se ganan con mentiras y engaños la confianza de estos para poder hacer que caigan en la trampa y así volverlos víctimas.

3. Medios de difusión y comercialización de material pornográfico de los niños, niñas y adolescentes a través de las redes sociales

Un vez desarrollado el punto previo en esta investigación en relación con el avance de las TICS en la sociedad venezolana, ahora corresponde expresar la moda adoptada por los jóvenes a nivel mundial, el cual consiste en interactuar de manera constante y casi permanente durante varias horas del día en lo que se conoce como "el chateo" por las diferentes redes sociales, así como por internet mediante la cual se intercambia cualquier tipo de información y a su vez tienden a estar tentados a inventar y experimentar nuevas experiencias digitales como por ejemplo interactuar de manera voluntaria pero de forma manipulada la intimidad de su sexualidad, que dependiendo del interés de los que se comunican pueden estar incurriendo en la pornografía infantil.

Lo anteriormente expuesto es fundamentado por la autora de la presente investigación, en función de la experiencia adquirida en las inducciones y talleres que impartía en las diversas instituciones educativas del Área Metropolitana de Caracas relacionadas con el tema de los juegos del "*Shoking Game"*, "la Ballena Azul" y "Confiésate por Facebook", adoptados a través del internet y de las distintas redes sociales que ponen en riesgo la vida de los niños, niñas y adolescentes del país.

De igual forma, en el diario español "El País" en su artículo Pornografía Infantil: la cara oscura de internet, publicado en enero de este año, permitió afirmar que la pornografía infantil a través del internet y las redes sociales muestran como niños, niñas y adolescentes son abusados sexualmente, gracias a las facilidades que ofrecen las nuevas tecnologías para captar a estas víctimas

vulnerables para luego producir y distribuir el material pornográfico con fines lucrativos[13].

Asimismo, otro de los mecanismos más comunes donde se puede evidenciar que existe pornografía infantil, es cuando los jóvenes inician una relación amorosa y comienzan de manera natural a mostrar fotos o videos con posiciones, con poca ropa y actitudes insinuantes, luego por venganza o por considerar que es una gracia comienzan a difundir entre ellos el contenido pornográfico, siendo en primer lugar captadas por las personas que son captadoras de este tipo de material y comienzan a ofrecerlos a sus clientes y así comienza la difusión y comercialización[14].

Otra de las formas que se logra producir la pornografía infantil es en los casos donde la juventud en búsqueda de dinero y por tener una familia disfuncional asumen trabajar vendiendo su cuerpo y exponiéndolo a riesgos y estando conscientes que están laborando en un mercado sexual y que los videos y fotos pueden ser difundidos y comercializados para ese fin[15].

Al respecto, se puede indicar que cuando los niños, niñas y adolescentes suelen optar a participar en la pornografía infantil quizás por necesidad de dinero o por engaño, al principio suele ser para ellos una situación engorrosa e incómoda pero con el transcurrir del tiempo se convierten en captadores y victimarios de otros jóvenes, porque ya suelen disfrutar dicha práctica[16].

Ahora bien, en relación al nombre de las redes sociales que comúnmente suelen ser utilizadas para la realización de la pornografía infantil son: *el Facebook, Instagram, whatsapp,* entre otros, las cuales en la actualidad representan un *boom* en la vida cotidiana de la juventud y que al no ser controlado su uso suelen ser un arma mortal para los jóvenes y una herramienta potente a ser usada por las personas que cometen el referido hecho punible[17].

13 https://elpais.com/elpais/2018/11/15/planeta_futuro/1542292342_375507.html [Consultada:2019, noviembre 16]

14 Información obtenida en el Foro "18 años de delitos informáticos en Venezuela" celebrado en la Universidad Central de Venezuela, el 27 de septiembre de 2019, Caracas, Venezuela.

15 En el diario español "El País" en su artículo Pornografía Infantil: la cara oscura de Internet, publicado en enero de este año, señala lo establecido por la Convención sobre los Derechos del Niño, los expertos apuntan que la pobreza y el subdesarrollo son factores que propician que los menores se vean sometidos a trata, prostitución, pornografía… "Desde un punto de vista global, son niños y niñas en una situación de vulnerabilidad especial, proceden de familias desestructuradas en las que sus progenitores están separados, se cuenta con escasos recursos, hay problemas de alcoholismo… Son familias que no suponen el lugar protector que necesitan" *op.cit*.

16 |Barreiro, J (2015) "La pornografía y los efectos en el desarrollo psicológico de los niños de 10 a 12 años de la Escuela Fiscal n°. 28 "República Bolivariana de Venezuela" en la ciudad de Guayaquil", Estudio de Comunicación Social, Universidad de Guayaquil, 2.015, pp. 36. http://repositorio.ug.edu.ec/bitstream/redug/8297/1/Tesis%20Victor%20Barreiro.pdf

17 Información extraída del artículo ¿Venezuela se suma a los países que regulan la pornografía en Internet? Publicado en la página contrapunto.com "Por otro lado, las redes sociales como Twitter, Instagram y Facebook tienen una política con respecto a esta clase de publicaciones. La

De esta manera se logra visualizar en función de todo lo antes expuesto, cuáles son las redes sociales más conocidas y usadas por los niños, niñas y adolescentes para interactuar entre ellos y con el resto del mundo, pero que a su vez pueden ser interceptados y captados de manera maliciosa por las bandas de pornografía infantil para tomar otra víctima sin consideración a la dignidad humana y los derechos humanos de la juventud ni de cualquier otra persona.

Es evidente que el delito de la pornografía infantil transgrede de manera directa los derechos de los niños, niñas y adolescentes, las cuales el Estado debe garantizar en conjunto con la sociedad, mediante la aplicación de políticas y planes de prevención y coerción que permitan ofrecerles a estas víctimas vulnerables una estabilidad en todos y cada uno de sus aspectos, tal y como lo establece la Ley Orgánica para la Protección de Niños, Niñas y Adolescentes en su artículo 6[18].

Es por ello, que el desarrollo de este subtitulo en la investigación planteada y plasmada en este artículo científico, demuestra de manera clara y precisa los elementos característicos de la tecnología aplicada en la comisión de este hecho punible que ha traspasado todas las barreras a nivel mundial, destacando en primera instancia el uso del internet, y las redes sociales como Instagram y Twitter, que representan los recursos de comunicación muy importantes en el negocio de la pornografía infantil.

4. Las consecuencias penales del uso de las redes sociales para la difusión y comercialización de material pornográfico de los niños, niñas y adolescentes en Venezuela

El eje principal de la investigación propuesta busca en este aparte describir las consecuencias penales que se encuentran establecidas en las diferentes normativas que conforman el ordenamiento jurídico venezolano en relación al uso de las redes sociales para la difusión y comercialización del material pornográfico de los niños, niñas y adolescentes en el país.

Desde este contexto, es de vital importancia, destacar en este aspecto que fue a partir de 1999 con la nueva Constitución de la República Bolivariana de Venezuela, cuando el Estado venezolano se apodera del control y regulación de las telecomunicaciones, especialmente del internet, a los fines de permitirle a la sociedad venezolana el acceso universal a la información mediante la disponibilidad de servicios públicos tales como radio, televisión y redes informáticas, siendo necesario para cumplir con este objetivo la creación del Ministerio de Ciencia y Tecnología y el Centro Nacional de Tecnología de la

opción de denunciar contenido que incomode a otros usuarios es una constante polémica en las plataformas". Disponible En: https://contrapunto.com/tecnologia/venezuela-se-suma-a-los-paises-que-regulan-la-pornografia-en-internet/[Consultada: 2019, noviembre 16].

18 Publicada en Gaceta Oficial Extraordinaria Nº 6.185 del 8 de junio de 2.015.

Información, el cual tienen como misión " garantizar la participación de la sociedad en el uso del internet"[19].

En este sentido, tanto el internet como la pornografía infantil en Venezuela, el Estado venezolano se ha encargado de enmarcarlos en sus normativas legislativas con la finalidad de tener el fundamento legal de sancionar y penar a todas aquellas personas que incurran en este hecho punible, por tal motivo, se puede mencionar en primer lugar en el Código Penal, la Ley Orgánica para la Protección del Niño, Niña y Adolescente, la Ley Especial Contra los Delitos Informáticos y la Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo.

Ahora bien, en lo que respecta a la tipificación de la pornografía infantil, establecida en el Código Penal venezolano (2005), se debe considerar lo establecido en el Titulo VIII de los Delitos Contra las Buenas Costumbres y Buen Orden de las Familias, Capítulo I De la Violación, de la Seducción, de la Prostitución o Corrupción de Menores y de los Ultrajes al Pudor, en virtud que en él se tipifican una serie de delitos, cuya finalidad es proteger el bien jurídico de la integridad sexual de los niños, niñas y adolescentes[20].

En relación con la Ley Orgánica para la Protección de Niños, Niñas y Adolescentes (2015), en su Título III de la referida Ley, establece el Sistema de Protección del Niño y del Adolescente, el cual en su Capítulo IX regula las Infracciones a la Protección Debida, y en su Sección Segunda indica las Infracciones y Sanciones, haciendo referencia a tres disposiciones relativos a la pornografía infantil contenidos en los artículos: 235, suministro o entrega de material de difusión de imágenes o sonidos; 236, suministro y exhibición de material impreso, y 237 pornografía con niños y adolescentes[21].

Por su parte, la Ley Especial Contra los Delitos Informáticos en su Título II dirigido a los delitos contra los Sistemas que utilizan Tecnologías de Información, en su Capítulo IV relacionado con los delitos contra los Niños, Niñas y Adolescentes, en sus artículos 23 y 24, se establecen las penas que acarrea la difusión o exhibición de material pornográfico de los niños, niñas y adolescentes[22].

Asimismo, la Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo (2011), contempla en su Capítulo VI De los Delitos Contra la Indemnidad Sexual, específicamente en sus artículos 46, 47 ,48 y 49, donde se establecen las penalidades en relación a la pornografía, la difusión de material pornográfico, la utilización de niños, niñas y adolescentes en la pornografía infantil y la elaboración de material pornográfico infantil.

En relación con el internet, en el año 2001 se promulgaron las normativas en el país que lo regirán, siendo estas: la Ley de Mensajes de Datos y Firmas

19 https://ipysvenezuela.org/2018/09/27/internet-regulado-una-mirada-a-la-normativa-legal-de-los-derechos-digitales-en-venezuela/ [Consultada: 2019, noviembre 16]

20 Publicada en Gaceta Oficial Extraordinaria Nº 5.768 del 13 de abril de 2005.

21 Publicada en Gaceta Oficial Extraordinaria N° 6.185 del 08 de junio de 2015.

22 Publicada en Gaceta Oficial Extraordinaria Nº 37.313 del 30 de octubre de 2001

Electrónicas y la Ley Especial contra los Delitos Informáticos, teniendo como norte legislativo la regulación de la protección y fortalecimiento de la actividad comercial, empresarial, burocrática y de comunicaciones en el ámbito digital[23].

Lo anteriormente expuesto, se argumenta con lo planteado en la exposición de motivos de la Ley de Mensajes de Datos y Firmas Electrónicas, a través del cual se hace referencia de la imperiosa y "necesaria e inminente la regulación de las modalidades básicas de intercambio de información por medios electrónicos, a partir de las cuales han de desarrollarse las nuevas modalidades de transmisión y recepción de información, conocidas y por conocerse, a los fines de garantizar un marco jurídico mínimo indispensable que permita a los diversos agentes involucrados, desarrollarse y contribuir con el avance de las nuevas tecnologías en Venezuela"[24].

Finalmente y no por ser menos importante, se debe tener presente y no descuidar lo contemplado en la legislación internacional que sanciona este tipo de delito a nivel mundial y que los Estados que lo hayan suscrito y ratificado deben cumplir de manera obligatoria con los referidos tratados y pactos internacionales, entre las cuales se puede mencionar las siguientes:

1) Declaración Universal de los Derechos Humanos: Proclamada por la Asamblea General de las Naciones Unidas el 10 de diciembre de 1948.
2) Declaración de los derechos del Niño: Proclamada por la Asamblea General de las Naciones Unidas el 20 de noviembre de 1959.
3) Pacto Internacional de Derechos Civiles y Políticos (16 de diciembre de 1966).
4) Pacto Internacional de Derechos Económicos, Sociales y Culturales (16 de diciembre de 1966).
5) Pacto de San José de Costa Rica (22 de noviembre de 1969).
6) Convención sobre los Derechos del Niño (20 de noviembre de 1989), ratificada por Venezuela en fecha 29 de agosto de 1990, según Ley Aprobatoria publicada en Gaceta Oficial No 34.541.
7) Convención sobre la Eliminación de todas las formas de Discriminación Contra la Mujer: adoptada por la Asamblea General de las Naciones Unidas en Resolución 341180 del 18 de septiembre de 1979.
8) Convención Interamericana para prevenir, sancionar y erradicar la violencia contra la mujer, "Convención de Belém do Pará": adoptada por la Asamblea General de las Naciones Unidas el 9 de junio de 1994. (Ley Aprobatoria decretada por el extinto Congreso de la República de Venezuela, en fecha 24 de noviembre de 1994 y sancionada por el Presidente de la República , en fecha 16 de enero de 1995).

23 https://ipysvenezuela.org/2018/09/27/internet-regulado-una-mirada-a-la-normativa-legal-de-los-derechos-digitales-en-venezuela/ [Consultada: 2019, noviembre 16] *op.cit*.

24 Publicada en Gaceta Oficial Extraordinaria Nº 37.076 del 13 de diciembre de 2000

9) El convenio 182 sobre la erradicación de las peores formas de trabajo infantil de la OIT (1999).

10) Protocolo Facultativo de la Convención sobre los Derechos del Niño.

11) Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.

12) Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, adoptados por la Asamblea General de las Naciones Unidas el 15 de noviembre de 2000.

Es importante, manifestar que Venezuela en lo que respecta a la materia de protección de los niños, niñas y adolescentes no solo ha participado a nivel mundial en la fomentación del respeto al interés superior del niño, niña y adolescente, sino que además se ha suscrito y ha ratificado convenios y tratados internacionales con el compromiso no solo de hacer cumplir con lo establecido en ellos sino que también ha adaptado sus normativas jurídicas a la protección de estas víctimas vulnerables.

Desde esta perspectiva queda claro que en el territorio venezolano al igual que en otros países, la práctica de la pornografía infantil y el uso del internet deben estar tipificada en las normativas jurídicas internas de cada país, tal como se evidencia en el caso de Venezuela, donde se establecen las penas que se deben aplicar a todas aquellas personas que realizan la pornografía en especial con los niños, niñas y adolescentes.

Conclusión

De acuerdo con la experiencia profesional y social adquirida por la autora de la presente investigación, se puede establecer como reflexión negativa que la pornografía infantil se ha convertido en un delito que se ha manifestado en todos los países del mundo y mientras en esta oportunidad se está realizando una investigación orientada a abordar el tema a objeto de saber el modus operando del delito, las mafias en este momento se encuentran planificando y organizándose para buscar nuevas alternativas para traspasar muchas más fronteras, aumentando así el índice delictivo de la pornografía infantil y obteniendo grandes ganancias mediante el riesgo de las víctimas completamente vulnerables.

Al respecto, es lamentable admitir que Venezuela no escapa de esta cruel realidad, y el órgano titular de la acción penal, ha logrado detectar a través de las diversas investigaciones penales realizadas en conjunto con los demás órganos auxiliares de la investigación, las cuales gracias a ese trabajo en conjunto se ha podido identificar casos relacionados con la difusión y comercialización de pornografía infantil, pudiéndose mencionar un caso muy reciente y conocido por la sociedad venezolana por la rápida acción del cuerpo de seguridad llamado

Fuerzas de Acciones Especiales (FAES) que desmanteló una banda de pornografía infantil al norte de Barquisimeto el 25 de octubre de 2019.

En ese sentido, los órganos del Estado venezolano en conjunto con la sociedad deben desarrollar políticas que permitan garantizar el interés de los niños, niñas y adolescentes venezolanos, a objeto de mitigar la disipación de este ilícito y así salvar más vidas de la juventud venezolana.

Para ello, es necesario e indispensable que el Estado y la sociedad comprendan que los niños, niñas y adolescentes son "víctimas vulnerables" y están expuestos a muchos peligros que ponen en riesgo sus vidas, por tal motivo requieren mayor atención y se debe romper paradigmas y tabúes que aún existen en la comunidad venezolana en relación con la sexualidad y la mejor manera de disminuir el delito de la difusión y comercialización de material pornográfico infantil y adolescentes, es a través de la educación y realizando campañas por todos los medios de comunicación vinculados a este tema, a objeto de despertar a todas las familias venezolanas y así unir esfuerzos.

Tipos penales asociados con la protección del sistema integral de criptoactivos en Venezuela

Emilio Alberto Arévalo Rengel*

SUMARIO: 1. Introducción. 2. Aspectos generales del Decreto Constituyente sobre "El Sistema Integral de Criptoactivos". 3. Procedimiento penal aplicado para los delitos establecidos en el Decreto Constituyente sobre "El Sistema Integral de Criptoactivos". 4. Tipos penales establecidos en el Decreto Constituyente sobre "El Sistema Integral de Criptoactivos". 5. Conclusiones.

Resumen

El presente trabajo aborda el análisis de los nuevos tipos penales establecidos en el Decreto Constituyente sobre el Sistema Integral de Criptoactivos (2019), los cuales de manera expresa penalizan las acciones tipificadas, antijurídicas y culposas, previstas y sancionadas en dicha norma, instituyendo una responsabilidad de los sujetos activos indeterminados explícitamente en: cualquier persona que contraviene el bien jurídico protegido por la norma, que no es otro, que el propio "Sistema Integral de Criptoactivos".

Palabras clave: Delitos. Tipos penales. Responsabilidad penal. Sistema Integral de Criptoactivos venezolano.

Recibido: 21/11/2020 • Aceptado: 9/1/2020

* Abogado egresado de la "Universidad Nacional Experimental de los Llanos Centrales Rómulo Gallegos"; Especialista en Ejercicio de la Función Fiscal egresado de la Escuela Nacional de Fiscales y cursando actualmente el Doctorado en Derecho en la Universidad Católica Santa Rosa, asimismo, ha realizado los diplomados en Docencia Universitaria dictado por la UPEL y por ENEMP, Derechos Humanos, Responsabilidad Penal del Adolescente y Derechos Humanos Laborales dictados por la Escuela de Derechos Humanos de la Defensoría del Pueblo y Procesal Penal dictado por CJUPRO. En su trayectoria profesional se ha desempeñado en el libre ejercicio, actualmente labora en el Ministerio Público como Abogado Adjunto V, adscrito a la Fiscalía Quinta ante el TSJ, con competencia para actuar ante la Sala Plena, Salas de Casación y Constitucional del Tribunal Supremo de Justicia. Es fundador-presidente de la Organización No Gubernamental "ASOCAPROFE-DH", ONG constituida para la dedicación exclusiva en la formación, educación, proyección y protección de los Derecho Humanos.

Abstract

This work analyses new penal crimes established in the Constituent Decree on the Integral System of Criptoassets (2019), which expressly penalize unlawful and guilty actions, foreseen and sanctioned in said norm, instituting the liability of the active subjects, explicitly undetermined in any person, who contravenes the legal good protected by the norm, which is the "Integral Cryptoactive System" itself.

Keywords: Types or Criminal Offenses. Criminal Liability. Venezuelan Integral System of Criptoassets.

1. Introducción

Con la entrada en vigencia del Decreto Constituyente sobre el Sistema Integral de Criptoactivos[1], emanado de la Asamblea Nacional Constituyente[2], entra en operaciones funcionales el Sistema Integral de Criptoactivos, el cual está estructurado operativamente para regular, organizar y normar en el territorio nacional, todo los relacionado con el intercambio digital de activos y monedas virtuales que utiliza criptografía para controlar, proteger y resguardar las operaciones en criptoactivos, como expresión organizativa y de avanzada de la soberanía económica nacional, denotando un avance significativo en la tecnológica para el desarrollo y fortalecimiento financiero y monetario de la República.

Es conveniente precisar, que este proceso de mejoramiento de las tecnologías y sus usos en materia monetaria para su intercambio comercial, contempla y afianza un marco regulador y normativo para la protección, inspección y fiscalización del sistema, estableciendo un procedimiento administrativo y cinco tipos penales aplicables a los transgresores del bien tutelado o protegido de la norma.

Sobre la base del contexto jurídico antes señalado, se aborda el análisis de los nuevos tipos penales establecidos en el mencionado Decreto Constituyente, los cuales de manera expresa, penalizan las acciones tipificadas, antijurídicas y culposas, previstas y sancionadas en dicha norma, instituyendo una responsabilidad de los sujetos activos, indeterminados explícitamente en: cualquier persona, la cual contraviene el bien jurídico protegido por la norma, que no es otro, que el propio "Sistema Integral de Criptoactivos"; castigando con prisión,

1 Publicada en la Gaceta de la República Bolivariana de Venezuela N° 41.575, extraordinaria, de fecha 30 de enero de 2019.

2 Publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 6323, extraordinaria, de fecha 08 de agosto de 2017.

en los cinco tipos penales contemplados en la ley, los cuales presupuestan una pena de prisión que oscilar entre un mínimo de un año hasta el máximo de cinco años de condena, por estar incurso en el hecho antijurídico preceptuado, adicionando una multa equivalente, fluctuante entre 50 y 150 criptoactivos soberanos.

2. Aspectos generales del Decreto constituyente sobre "El Sistema Integral de Criptoactivos"

La República Bolivariana de Venezuela, consagra en su texto constitucional[3], como garantía al pueblo un interés público y fundamental en las tecnologías para el desarrollo económico, social y político, el cual será trascendental para la seguridad y soberanía nacional, tal como lo instituye el artículo 110, de la carta magna, que seguidamente se reproduce:

> Artículo 110. CRBV. El Estado reconocerá el interés público de la ciencia, las 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. (…).

En ese sentido estratégico, el gobierno instauró una política monetaria con diferentes matices, motivando a las nuevas tecnologías financieras que utilizan la criptografía para la protección de sus documentos, datos y usuarios, en tal contexto reproduce el activo digital que utiliza la criptografía y sus registros para constituir los criptoactivos, estableciendo como premisa para la soberanía económica un desarrollo integral entre lo productivo y lo social, para lo cual despliega y crea un Sistema Integral de Criptoactivos[4], como expresión organizativa y funcional de soberanía económica, tal como lo establece, en el objeto, del artículo 1, en el Capítulo I, relacionado a con los Aspectos Generales, del Decreto Constituyente sobre el Sistema Integral de Criptoactivos, (2019), en lo sucesivo (DCSIC).:

> Objeto
> Artículo 1. El objeto de este Decreto Constituyente, es crear y definir el marco regulador aplicable al Sistema Integral de Criptoactivos, como expresión

3 Constitución de la República Bolivariana de Venezuela, Gaceta Oficial N° 5.908, extraordinario del 19 de febrero de 2009.

4 (DCSIC), artículo 6. Conformación. El Sistema Integral de Criptoactivos está conformado por el conjunto de principios, normas y procedimientos, aplicados a las personas naturales y jurídicas, instituciones u organizaciones públicas y privadas, así como Consejos Comunales, Comunas y demás formas organizadas del Poder Popular que en su conjunto interactúan para el objetivo superior de garantizar la incorporación de los criptoactivos y las tecnologías asociadas en la República Bolivariana de Venezuela.

> organizativa y funcional de soberanía económica, con el firme propósito de avanzar, de forma armónica en el desarrollo productivo y social de la República Bolivariana de Venezuela.

En razón de lo expresado por el constituyentista, en la norma que precede, el desarrollo social del Estado venezolano, tiene como propósito el avance productivo de la nación y el fortalecimiento de la soberanía económica, la cual desarrolla un apalancamiento tecnológico con la creación y puesta en marcha del Sistema Integral de Criptoactivos. En consecuencia, con el objeto de la norma, la misma establece la disposición tácita de la condición de ley de orden público, el cual se representa para el mantenimiento tutelado de la tranquilidad y la paz social como se reseña seguidamente:

> Orden Público
> Artículo 2. Las disposiciones de este Decreto Constituyente son de orden público y prevalecerán en su aplicación sobre las contenidas en otras leyes, incluso de su mismo rango, cuando regulen ámbitos relacionados con el objeto de ésta, en cuanto contradijeren o colidieren con su aplicación.

Es conveniente expresar que, la condición de ley de orden público, establecida mediante la disposición del Decreto Constituyente sobre el Sistema Integral de Criptoactivos, instituye la prevalencia de esta norma sobre las demás disposiciones legales del ordenamiento jurídico nacional, inclusive determina explícitamente que el presente basamento legal, está sobre las leyes estructuradas con rango similar a la de presente decreto ley, como garantía fundamental de la seguridad pública y social.

Precisado lo anterior, cabe subrayar el ámbito de aplicación del Decreto Constituyente sobre el Sistema Integral de Criptoactivos, el cual se configura en dos grandes grupos, precisando el primero de ellos en los bienes, servicios, valores o actividades y funcionamiento, y el segundo grupo en compra, venta uso, distribución y demás actividades conexas de los criptoactivos, como seguidamente expresa la norma:

> Ámbito de aplicación
> Artículo 3. Este Decreto Constituyente tiene como ámbito de aplicación los bienes, servicios, valores o actividades relacionados con la constitución, emisión, organización, funcionamiento y uso de criptoactivos y criptoactivos soberanos, dentro del territorio nacional, así como la compra, venta, uso, distribución e intercambio de cualquier producto o servicio derivado de ellos y demás actividades que le sean conexas.

Condiciona de manera expresa el Decreto Constituyente, (16) principios para la operatividad y funcionabilidad, todos ellos, reguladores y orientadores

de las actividades de los criptoactivos y criptoactivos soberanos, bajo un carácter liberador, como seguidamente se corresponde:

> Principios
>
> Artículo 4. Este Decreto Constituyente tiene un carácter liberador para el pueblo venezolano y está basado en principios de:
>
> 1. Inclusión.
> 2. Promoción e innovación financiera
> 3. Cooperación interinstitucional.
> 4. Universalidad.
> 5. Protección a los usuarios y usuarias.
> 6. Bien común.
> 7. Corresponsabilidad.
> 8. Preservación de la estabilidad financiera.
> 9. Prevención de operaciones ilícitas.
> 10. Seguridad tecnológica y simplificación de trámites administrativos.
> 11. Integridad.
> 12. Soberanía.
> 13. Inmunidad.
> 14. Concurrencia.
> 15. Transparencia.
> 16. Responsabilidad social y ética pública.
>
> Prevaleciendo la armónica coordinación entre los organismos del Estado para garantizar su cabal ejecución.

Llama poderosamente la atención, en lo que respecta a los principios rectores de las actividades reguladas por el Decreto Constituyente sobre el Sistema Integral de Criptoactivos, lo relativo al "principio de la preservación de la estabilidad financiera", por lo que comporta su realización plena por parte de los sujetos e instituciones llamadas a resguardar, salvaguardar y proteger el sistema financiero nacional. Por otra parte, en lo que respecta al principio "prevención de operaciones ilícitas" el cual soporta la prevención de acciones delictivas establecidas en los tipos penales representados en esta norma.

En este sentido, el Sistema Integral de Criptoactivos, está concebido en su conjunto con sus: principios, normas y dos procedimientos uno de inspección y otro de fiscalización de las actividades propias del sector de criptoactivos, aplicados a las personas naturales y jurídicas, instituciones u organizaciones públicas o privadas, que interactúan en las actividades encriptados en blockchain, con el firme objetivo de garantizar la incorporación y los usos de los criptoactivos y criptoactivos soberanos a las tecnologías de los sistemas financieros asociadas y conexas de la República Bolivariana de Venezuela.

De manera general el Sistema Integral de Criptoactivos, realizará mediante el uso de los medios técnicos más idóneos, para inspeccionar y fiscalizar las actividades propias del sector de criptoactivos (procedimiento administrativo de inspección).

Adicionalmente, deberá determinarse mediante la fiscalización la verdad de los hechos, que permitan conocer la conformidad o incumplimiento de los deberes establecidos por este Decreto Constituyente, los responsables, el grado de responsabilidad y de ser procedente, el daño causado. Denunciando ante el Ministerio Público, "Modos de Proceder", los hechos delictivos, para el inicio de la investigación penal conducente, derivada de la responsabilidad de los sujetos comprometidos con el hecho penal denunciado.

La conformación de un órgano rector del Sistema Integral de Criptoactivos, el cual está a cargo de la Superintendencia Nacional de Criptoactivos y Actividades Conexas (SUNACRIP), funcionando como rectora de: 1) la Tesorería de Criptoactivos de Venezuela, S.A.; 2) las casas de cambio; 3) las personas naturales y jurídicas tanto públicas como privadas; 4) el Poder Popular Organizado vinculado directa o indirectamente con la materia de criptoactivos.

La disposición de un procedimiento administrativo, el cual haciendo uso de los medios técnicos adecuados inspeccionará las actividades propias del sector de criptoactivos, para el cumplimiento de los deberes establecidos por el Decreto Constituyente sobre el Sistema Integral de Criptoactivos (2019), estableciendo los responsables y el grado de responsabilidad, su procedencia y el daño causado. Para tales efectos, podrá adoptar y ejecutar en un mismo acto medidas preventivas, destinadas a impedir que se continúen quebrantando las normas que regulan la materia de delitos financieros e informáticos.

Son las medidas preventivas contempladas en el Decreto Constituyente sobre el Sistema Integral de Criptoactivos: el decomiso; la suspensión de licencias, permisos o autorizaciones emitidas por la Superintendencia Nacional de Criptoactivos y Actividades Conexas (SUNACRIP); cualquier otra prevista en el ordenamiento jurídico para impedir la vulneración de los derechos de los ciudadanos.

En consecuencia, el Decreto Constituyente sobre el Sistema Integral de Criptoactivos (2019), establece la configuración de diez normas sancionatorias incorporando cinco artículos que instituyen pena de prisión y cinco que comportan infracción pecuniaria, tomando en consideración que de las diez disposiciones sancionatorias solo cuatro, de ellas, contemplan tanto una multa exigida en moneda virtual como una pena privativa de la libertad, para el tipo penal tipificado, en la presente norma reguladora de la actividad integral de los criptoactivos, en la República.

Es imperativo señalar, que los tipos penales sancionados y previstos en el Decreto Constituyente sobre el Sistema Integral de Criptoactivos (2019), son de orden público y prevalecen sobre las aplicaciones contenidas en otras leyes, incluso las de su mismo rango normativo, como se fundamenta en su propio texto normativo.

En su aplicación territorial instituye un ámbito de aplicación, el cual regula el uso novedoso pero supervisado de los criptoactivos y criptoactivos soberanos, para el adelanto tecnológico en lo que comporta el uso de la criptografía y de

sus bases de datos por blockchain, como un novedoso modelo monetario para la estabilidad del sistema financiero, económico y productivo de la nación. Concluye el Decreto Constituyente, sobre sus aspectos generales, configurando su base actuación sobre los principios rectores, determinados para la consecución del mejoramiento progresivo de las operaciones financieras tanto dentro de la República como en las relaciones encriptadas bajo la modalidad de criptoperaciones[5], realizadas fuera del territorio con operadores nacionales.

El estudio de los cinco tipos penales establecidos en Decreto Constituyente sobre el Sistema Integral de Criptoactivos, comporta un análisis previo de algunos conceptos propios del Derecho penal, bajo ese esquema afirma Muñoz[6], que el Derecho penal existe por la configuración previa del tipo penal, que sanciona la conducta antijurídica culposa tipificada por el Poder Legislativo. En ese contexto, establece el maestro Chiossone[7]:

> *La iniciación del proceso penal tiene por base la existencia de una acción u omisión prevista expresamente por la ley como delito o falta, o lo que es lo mismo, la existencia de un hecho que corresponda a un tipo legal expresamente previsto por la ley. Hemos dicho en alguna oportunidad que la acción humana, cuando es transgresora de un orden público, perfila una forma o tipo real (hecho) que hemos denominado tipo-transgresión, el cual, para que sea punible, debe corresponder exactamente en sus elementos esenciales al tipo-lega, o sea a la descripción legal, (...).*

Conforme a lo afirmado por el maestro Chiossone, la transgresión del sujeto activo mediante la ejecución de la acción u omisión subsumida en lo preceptuado en el tipo penal, comporta la realización de las premisas objetivas y subjetivas, las cuales tipifican la realización del hecho antijurídico de la expresión propia de la voluntad culposa, que ofende a la víctima y quebranta el bien protegido por la norma, afectando directamente el orden público, acarreando la activación inmediata del proceso penal en contra de los confrontados contra la ley.

En ese contexto, establece Grisanti Aveledo[8], sobre la tipicidad como parte integral del delito y explicando su concepto sobre los tipos penales y como deben estos subsumirse dentro de los elementos esenciales del delito, a saber:

> *Tipicidad. Es un elemento del delito que implica una relación de perfecta adecuación, de total conformidad, entre un acto de la vida real y un tipo*

5 Operaciones relacionadas con la funcionabilidad de las actividades relacionadas y conexas con los criptoactivos, actuando bajo la modalidad del blockchain.

6 MUÑOS CONDE, Francisco (2008). Teoría General del Delito pág. 1. "*Desde el punto de vista jurídico, delito es toda conducta que el legislador sanciona con una pena. Esto es una consecuencia del principio nullum crimen sine lege, que rige el moderno derecho penal*".

7 CHIOSSONE, Tulio (1972). *Manual de Derecho Procesal Penal*. Facultad de Derecho Universidad Central de Venezuela. Pág. 125.

8 *Manual de Derecho Penal*. Parte especial. Vigésima cuarta edición 2009.

> *penal. Entendemos por tipo penal o legal, cada una de las descripciones incriminantes de la ley penal. La tipicidad es, en otros términos, la adaptabilidad de un acto a un tipo legal.*

Precisado lo anterior, establecen los autores Piva y Pinto[9] sobre los tipos penales descritos en las normas, se consideran delitos, las acciones u omisiones antijurídicas realizadas por los sujetos activos, las cuales se encuentren previstas y sancionadas en las leyes sustantivas.

Con ese marco referencial introductorio, la entrada en vigencia del "Decreto Constituyente sobre el Sistema Integral de Criptoactivos, en lo sucesivo "DCSIC", se incorporan al compendio punitivo del Estado Venezolano unos nuevos tipos penales, los cuales preservan y protegen como bien jurídico tutelado al Sistema Integral de Criptoactivos, y como este, nuevo sistema es conexo y agregado directamente al sistema financiero nacional requiere la protección del Estado venezolano.

En consecuencia, las operaciones en criptoactivos pueden ser generadas o generadoras de situaciones de ilegalidad o ilicitud, tal y como lo apunta en el resumen de su artículo Valenzuela (2015):

> *Las monedas virtuales son un fenómeno reciente nacido en virtud del progreso constante de la tecnología y el aumento del acceso a Internet hacia el público. Actualmente, son utilizadas para realizar transacciones en todo el mundo, algunas veces de forma lícita, otras veces no. (p 155).*

Es ese contexto destacado anteriormente, las operaciones de criptoactivos y las denominadas monedas virtuales, operan en redes financieras y mercantiles asociadas al control de la criptografía, como formato de almacenamiento de la red informática "cadena de bloques blockchain" constituida y operada por usuarios indeterminados o anónimos, tanto por los criptoactivos como por sus monedas virtuales, todos copartícipes con diversos activos encriptados[10].

Habida cuenta de lo anterior, las operaciones criptográficas pueden generar o financiar conductas delictivas contrarias al orden social mundial, por su capacidad para vulnerar y transgredir el orden público interno de las naciones, ya que, la operación de los criptoactivos sucede con o sin ninguna regulación externa al propio sistema, lo cual es considerado por el propio sistema como su fortaleza operativa, pero denotando inconvenientes a la hora de establecerse las medidas regulatorias propias de cada Estado en defensa de su autonomía funcional y operativa del sistema financiero, soportado por plataformas informáticas encriptadas en la modalidad del blockchain.

9 GRISANTI, A. Hernando. (2009). *Manual de Derecho Penal.* Parte especial. Vigésima Cuarta Edición. Caracas, Venezuela. Pág. 107.

10 Activos inscriptados: activos operacionalizados bajo la modalidad de la red informática del blockchain, para la criptografía de la sistematización como método de seguridad en la red financiera y comercial para los criptoactivos y sus operaciones derivadas y conexas.

A manera de conclusión sobre este primer análisis, el Decreto Constituyente sobre el Sistema Integral de Criptoactivos, establece como aspectos generales normativos, en lo que comporta como su objetivo funcional, coadyuvar al desarrollo del sistema financiero y monetario nacional para la protección integral de la soberanía económica; para ello, instituye la protección del Sistema Integral de Criptoactivos, para el apalancamiento del sistema nacional financiero.

3. Procedimiento penal aplicado para los delitos establecidos en el Decreto Constituyente sobre "El Sistema Integral de Criptoactivos"

Si bien el Decreto Constituyente sobre el Sistema Integral de Criptoactivos, establece un procedimiento administrativo de inspección y fiscalización, para que la Superintendencia (SUNACRIP[11]), pueda imponer multas y demás sanciones derivadas del incumplimiento de las obligaciones determinadas para los operadores y usuarios como protección del sistema[12], existe la posibilidad real y efectiva de detectar ilícitos técnicos de orden operacional y administrativos, para conocer de las infracciones y delitos mediante las revisiones o fiscalizaciones administrativas, en tal sentido, con respecto a los tipos penales, el decreto no explica explícitamente el procedimiento a seguirse para el juzgamiento de los delitos, el cual debería ser el procedimiento ordinario establecido en el Código Orgánico Procesal Penal (2012), siendo éste el procedimiento adecuado garantista y defensor de los derechos fundamentales para el juzgamiento de los ciudadanos confrontados con las normas penales preconstituidas a sus efectos directos.

Al respecto, el constituyentista instituyó para proteger el Sistema Integral de Criptoactivos, el mencionado Decreto Constituyente, determinando competencias para la superintendencia, entre las cuales destaca la facultad de actuar como órgano auxiliar del sistema de justicia[13] y de instituir el procedimiento de oficio o instancia de parte o de terceros[14] para instruir el expediente como órgano actuante en la primera etapa del proceso penal respectivo para el juzgamiento de los delitos contemplados en el Capítulo V De las Infracciones y Sanciones, las cuales representan tipos penales con establecimiento de prisión por penas que oscilan de 1 a 5 años, más multas equivalentes de 50 a 150

11 (SUNACRIP). Superintendencia Nacional de Criptoactivos y Actividades Conexas.

12 Artículo 20 Atribuciones del Superintendente. Numeral 9 Imponer las multas y demás sanciones que se deriven del incumplimiento de obligaciones relacionadas con las competencias de la (SUNACRIP).

13 Artículo 11. Competencias de la Superintendencia. Numeral 14. Actuar como órgano auxiliar del sistema de justicia en relación a la materia de criptoactivos y actividades conexas.

14 Artículo11. Competencias de la Superintendencia. Numeral 15. Instituir el procedimiento de oficio o a instancia de terceros y aplicar las sanciones a que hubiere lugar a quienes ejerzan la minería sin la autorización requerida o incumplan con las formalidades establecidas en este Decreto Constituyente, relacionadas con el Sistema Integral de Criptoactivos.

criptoactivos soberanos, tal y como se analizó en el tema correspondiente al estudio de los tipos penales establecidos en la referida norma.

Para continuar el análisis del marco legal, de lo que comporta el juzgamiento de los ciudadanos confrontados con este Decreto Constituyente, el cual establece nuevos tipos penales, hay que precisar, los siguientes aspectos: la Constitución de la República Bolivariana de Venezuela[15], consagra y ostenta la concepción de un Estado democrático y social de Derecho y de justicia, que propugna valores superiores, garantizando derechos y fomentando los deberes ciudadanos, en ese sentido garantista, se establece como el proceso es la base fundamental de la realización de la justicia, tanto para los ciudadanos venezolano y extranjeros sometidos a los procesos judiciales en el territorio nacional, en ese contexto jurídico, instituye la carta fundamental en su artículo 257 constitucional.

> Artículo 257 CRBV. Proceso Judicial. El proceso constituye un instrumento fundamental para la realización de la justicia. Las leyes procesales establecerán la simplificación, uniformidad y eficacia de los trámites y adoptarán un procedimiento breve, oral y público. No se sacrificará la justicia por la omisión de formalidades esenciales.

En concordancia expresa con lo sustentado anteriormente, establece el Código Orgánico Procesal Penal[16], en el artículo 1, la protección expresa, para que todo ciudadano confrontado con una ley, la cual establezca pena de prisión que coarte su libertad, debe ser sometido previamente a un juicio penal, en el cual se le deben proteger y consagrar todos sus derechos y garantías procesales, como seguidamente se señala:

> Artículo 1. COPP. Juicio Previo y Debido Proceso. Nadie podrá ser condenado sin un juicio previo, oral y público, realizado sin dilaciones indebidas, sin formalismos ni reposiciones inútiles, ante un juez o tribunal imparcial, conforme a las disposiciones de este Código y con salvaguarda de todos los derechos y garantías del debido proceso, consagrados en la Constitución de la República Bolivariana de Venezuela, las leyes, los tratados, convenios y acuerdos internacionales suscritos y ratificados por la República.

En correspondencia con lo citado, preceptúa el Código Orgánico Procesal Penal en el artículo 13[17], que lo fundamental del proceso es establecer la verdad de los hechos, obtenidos por el sistema de justicia, a través del proceso mediante la aplicación del derecho para la realización plena de la justicia.

15 Gaceta Oficial N° 5.908, extraordinario del 19 de febrero de 2009.

16 Gaceta Oficial N°6.078 extraordinaria, del 15 de junio de 2012.

17 COPP. Artículo 13. Finalidad del Proceso. El proceso debe establecer la verdad de los hechos por las vías jurídicas, y la justicia en la aplicación del derecho, y a esta finalidad deberá atenerse el juez o jueza al adoptar su decisión.

Como parte del aporte del presente trabajo es definir la vía procesal para el juzgamiento de los delitos cometidos por ciudadanos confrontados con los tipos penales previstos y sancionados en el Decreto Constituyente sobre el Sistema Integral de los Criptoactivos, se consultó lo referido por doctrinario nacional Rivera Morales[18],

> (…) La Constitución, las garantías y el proceso penal, parte de la idea que el sistema penal no tiene como objetivo final llevar al ciudadano a la cárcel, sino que es un sistema de defensa ante el ius puniendi estatal: no se le puede seguir juicio penal por cualquier hecho, sino por aquellos tipificados previamente como delito, y así mismo, no se le puede seguir juicio penal de cualquier manera, sino según las formalidades pautadas en la ley adjetiva y respetando las garantías propias del debido proceso.

En función de lo destacado anteriormente y reafirmando lo alegado de manera precisa, Rivera Morales[19], establece que el proceso penal se le aplica al sujeto activo derivando en una consecuencia jurídica, la cual acarrea una pena privativa de libertad, siendo en Venezuela por excelencia el procedimiento ordinario, el previsto para juzgar a los ciudadanos confrontados con la ley penal, el instituido en el COPP, tomando como excepcionales a los procedimientos especiales y demás leyes, las cuales contemplen un procedimiento especial. Seguidamente asevera Rivera Morales, lo siguiente:

> En el proceso penal se aplica la ley penal en cuanto al tipo (hechos constitutivos y consecuencias jurídica) y la ley procesal, en cuanto al procedimiento y la organización judicial. Esto supone que los operadores jurídicos (Ministerio Público, defensores, juzgadores) para la aplicación de la ley penal deben realizar interpretaciones del sentido y alcance, cuando ello se deduzca claramente de la literalidad de la norma.

Precisando todo lo anteriormente referido tanto en la Constitución de la República Bolivariana de Venezuela como por la doctrina, al citarse al profesor Rivera Morales, es determinante para establecer el procedimiento en Venezuela para el juzgamiento de los delitos de acción pública cometidos por los ciudadanos confrontados con las leyes que establecen penas privativas de libertad y consecuente prisión de los sentenciados, por lo general es el procedimiento ordinario del Código Orgánico Procesal Penal.

La norma adjetiva penal, preceptúa como procedimiento especial en el Libro Tercero, Título II, del procedimiento para el juzgamiento de los delitos menos graves, en el artículo 354, conceptualizando el término como los delitos de acción pública previstos en la ley, cuyas penas en su límite máximo no excedan de 8

18 Rodrigo RIVERA MORALES. *Manual de Derecho Procesal Penal*. "El garantismo de Rodrigo Rivera Morales a manera de prologo". (2012).

19 Rodrigo RIVERA MORALES. *Manual de Derecho Procesal Penal* (2012. Pág. 82.

años de privación de libertad, como fórmula acogida para descongestionar los centros penitenciarios, debido al interés social por considerarse de penalidades leve.

En ese contexto adjetivo, entran los 5 tipos penales previstos y sancionados en el Decreto Constituyente sobre el Sistema Integral de Criptoactivos (2019), ya que los mismos fluctúan de un mínimo de prisión de 1 año hasta el máximo 5 años de presidio, para los sujetos activos confrontados con la norma penal, consecuentemente con la normativa procedimental también los tipos penales del Decreto Constituyente tipifican delitos de acción pública, para los tipos tipificados. De conformidad con lo referido anterior, el artículo 354, en su parágrafo *infine*, establece los 14 delitos excluidos del presente procedimiento especial para el juzgamiento de los delitos menos graves, seguidamente cuadro contentivo de los delitos exceptuados.

N°	**Delitos exceptuados artículo 354 del COPP**		
01	Delito de Homicidio Intencional	08	**Delitos contra el Sistema Financiero y Delitos Conexos**
02	Delito de Violación	09	Delitos con Multiplicidad de Víctimas
03	Delitos que atenten contra la libertad, integridad e identidad sexual de los niños, niñas y adolescentes	10	Delitos Delincuencia Organizada
04	Delito de Secuestro	11	Delitos por Violaciones a los Derechos Humanos
05	Delitos de Corrupción	12	Delitos de Lesa Humanidad
06	Delitos contra el Patrimonio Público y la Administración Pública	13	Delitos contra la Independencia y Seguridad de la Nación
07	Delitos de Tráfico de Drogas de Mayor Cuantía	14	Crímenes de Guerra
08	Delitos de Legitimación de Capitales		

En el catálogo de los delitos el legislador, exceptúa el delito contra el sistema financiero o delitos conexos, del procedimiento de delitos menos graves, al estar esté relacionado con el sistema integral de criptoactivos, como a continuación se señala:

> *Artículo 354. COPP. Procedencia. El presente procedimiento será aplicable para el juzgamiento de los delitos menos graves.*
> A los efectos de este procedimiento, se entiende por delitos menos graves, los delitos de acción pública previstos en la ley, cuyas penas en su límite máximo no excedan de ocho años de privación de libertad.
> Se exceptúa de este juzgamiento, independientemente de la pena, cuando se trate de los delitos siguientes: homicidio intencional, violación; delitos que atenten contra la libertad, integridad e identidad sexual de los niños, niñas y adolescentes; secuestro, corrupción, delitos contra el patrimonio público y la administración pública; tráfico de drogas de mayor cuantía, legitimación de capitales, contra el sistema financiero y delitos conexos, delitos con multiplicidad de víctimas, delincuencia organizada, violaciones a los derechos humanos, lesa humanidad, delitos contra la independencia y seguridad de la nación y crímenes de guerra.

Habida cuenta de lo referido anteriormente y de manera concluyente, existen unas excepciones para aplicar el procedimiento especial para los delitos menos graves, no importando si su penalidad no excede los ocho años de prisión, siendo que los cinco tipos penales previstos y sancionados en el Decreto Constituyente sobre el Sistema Integral de Criptoactivos, oscilan en el rango de prisión de 1 a 5 años, pero estando excluidos del procedimiento especial para los delitos menos graves, lo cual comporta directamente su juzgamiento por el procedimiento ordinario del COPP, al respecto afirma Ruiz, Juan[20]. En ese contexto, afirma Rivera Morales[21], que lo exceptuado en la norma adjetiva penal en su artículo 354 del COPP, representa la afirmación de la gravedad del delito y su impacto directo sobre la sociedad, lo cual hace procedente para el juzgamiento de ciudadanos confrontados con los tipos penales previstos y sancionados en el decreto, será por el procedimiento ordinario.

4. Tipos penales establecidos en el Decreto Constituyente sobre "El Sistema Integral de Criptoactivos (2019"

El Decreto Constituyente sobre el Sistema Integral de Criptoactivos (2019), establece cinco tipos penales para la protección integral y expresa del Sistema de Criptoactivos en Venezuela, comportando los aspectos fundamentales objetivos y subjetivos de la norma, para el tutelaje efectivo del sistema como

20 Ruiz Blanco, Juan Eliezer. (2013). (…) Al respecto, define la norma como delitos menos graves aquellos cuyas penas en su límite máximo, no exceden de ocho años de privación de libertad. Se exceptuarán del presente procedimiento los delitos que se indican en el último aparte de esta norma, independientemente de la cuantía de la pena. Páginas 663 - 664.

21 Rivera Morales, Rodrigo (2013). Por lo general, la doctrina respecto a la conceptualización de la gravedad del delito lo relaciona con la asignación de penas más severas. No obstante, la gravedad del delito debe examinarse partiendo del perjuicio o daño ocasionado a la colectividad (…).

bien protegido por la ley, observando como característica fundamental del Derecho penal, de sus derivadas tipicidades y antijuricidades de la sanción propia de las figuras delictivas previstas y sancionadas en las normas punitivas, para lo cual, se establece seguidamente análisis de los tipos penales contemplados en el Decreto Constituyente:

De los delitos contra el Acceso Indebido
al Sistema Integral de Criptoactivos

Artículo 43.

- Quien:
- Sin la debida autorización o excediendo la que hubiere obtenido:
  1. Acceda.
  2. Intercepte.
  3. Interfiera.
  4. O use un sistema que utilice tecnologías de información relacionados con el Sistema Integral de Criptoactivos.

Será penado con prisión de uno (01) a tres (03) años y multa equivalente de cincuenta (50) a cien (100) Criptoactivos soberanos.

1. Acción típica : a) sin la debida autorización; b) o excediendo la que hubiere obtenido.
2. Verbos: a) acceder, b) interceptar, c) interferir d) o use un sistema.
3. Sujeto Activo: Indefinido o Indiferente. (Cualquier persona imputable).
4. Sujeto pasivo: a) el Sistema Integral de Criptoactivos.
5. Culpabilidad: Delito doloso.
6. Naturaleza de la acción: Delito de acción pública.
7. Prisión: de uno 1 a tres 3 años.
8. Multa: equivalente de 50 a 100 criptoactivos soberanos.

Del análisis a este tipo penal establecido por el constituyentista, para proteger el Sistema Integral de Criptoactivos, como bien tutelado o protegido por la norma, en lo que respecta al delito por acceso indebido, comporta una acción de ingresar al sistema de manera y forma indebida, violentado la seguridad del propio sistema, configurando una acción similar a hackear[22] el sistema sin la permisión convenida, conformando la acción típica dolosa establece que el sujeto activo, accederá, interceptará, interferirá o usará un sistema, sin la debida autorización para hacerlo o excediendo la autorización otorgada, desplegada la acción típica, el mismo estará incurriendo en el delito de acceso indebido, penalizado con prisión de 1 a 3 años, más una multa equivalente que oscila de 50 a 100 criptoactivos soberanos. Es conveniente destacar que el tipo penal del acceso indebido también está contemplado en similar redacción en la Ley Especial contra los Delitos Informáticos (2001)[23], haciendo la correspondiente salvedad que la diferencia

22 Hackear: se utiliza para conocer información general sobre el sistema y la tecnología empleada, propiciando una vulneración al sistema de seguridad interna del sistema.

23 Ley Especial contra los Delitos Informáticos (2001), artículo 6.

fundamental radica en el bien protegido directo en ambas normar siendo en el Decreto Constituyente, el propio Sistema Integral de Criptoactivos.

Del Sabotaje o Daño al
Sistema Integral de Criptoactivos

Artículo 44.

- Quien
- Con intención:
  1. Destruya.
  2. Dañe.
  3. Modifique.
  4. O realice cualquier acto que altere el funcionamiento.
  5. O inutilice un sistema que aplique tecnologías de información o cualquiera de los componentes que lo conforman, relacionados con el Sistema Integral de Criptoactivos.

Será penado con prisión de uno (01) a tres (03) años y multa equivalente de cien (100) a ciento cincuenta (150) Criptoactivos soberanos.

- Incurrirá en la misma pena quien:
  1. Destruya.
  2. Dañe.
  3. Modifique.
  4. O inutilice.
- La data o la información contenida en cualquier sistema que emplee tecnologías de información o en cualquiera de sus componentes.

1. Acción típica : a) con intención, b) realice cualquier acto que altere el funcionamiento, c) inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman.
2. Verbos: a) destruya, b) dañe, c) modifique.
3. Sujeto Activo: Indefinido o Indiferente. (Cualquier persona imputable).
4. Sujeto Pasivo: a) el Sistema Integral de Criptoactivos.
5. Culpabilidad: Delito doloso. (Intencionalidad).
6. Naturaleza de la acción: Delito de acción pública.
7. Penalidad: de uno 1 a tres 3 años.
8. Multa: equivalente de 100 a 150 criptoactivos soberanos.

En lo que comporta a este tipo penal establecido por el constituyentista para proteger el Sistema Integral de Criptoactivos, el mismo procura resguardar al propio sistema de todas aquellas conductas dolosas dirigidas a eliminar o modificar funciones operativas o datos propios generados o resguardados por el Sistema de Criptoactivos, sin autorización previa o expresa, para objeto de obstaculizar o eliminar su correcto funcionamiento, dañando el hardware, el software o demás componentes propios o conexos del sistema, en ese contexto normativo, el sujeto activo debe realizar una labor de sabotaje informático o daño directo al sistema interno, destruyendo, dañando o modificando, maliciosamente al mismo, produciendo la consecuencia jurídica presupuestada

en la norma, lo cual comporta una pena de prisión de 1 a 3 años más una multa que oscila entre los 100 a 150 criptoactivos soberanos.

Posesión de Equipos o Prestación
de Servicios de Sabotaje

Artículo 46.

- Quien:
  1. Importe.
  2. Fabrique.
  3. Distribuya.
  4. Venda o utilice:
     1. Equipos.
     2. Dispositivos o programas.
  5 realice algún tipo de financiamiento al:
     1. Terrorismo.
     2. Narcotráfico.
     3. O legitimación de capitales.
- Con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información;
- O el que ofrezca o preste servicios destinados a cumplir los mismos fines relacionados con el Sistema Integral de Criptoactivos.

Será penado con prisión de uno (01) a tres (03) años y multa equivalente de cincuenta (50) a cien (100) Criptoactivos soberanos.

1. Acción típica: a) realizar algún tipo de financiamiento al terrorismo, narcotráfico y legitimación de capitales, b) con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información, c) ofrezca o preste servicios destinados a cumplir los mismos fines relacionados con el Sistema Integral de Criptoactivos.
2. Verbos: a) importe, b) fabrique, c) distribuya, d) venda, e) o utilice, f) realice algún financiamiento.
3. Sujeto Activo: Indefinido o Indiferente. (Cualquier persona imputable).
4. Sujeto Pasivo: a) El Sistema Integral de Criptoactivos y b) la salud, seguridad y economía universal
5. Culpabilidad: Delito Doloso. (Intencionalidad).
6. Naturaleza de la acción: Delito de acción pública.
7. Penalidad: de uno 01 a tres 03 años.
8. Multa: equivalente de 50 a 100 criptoactivos soberanos.

El Decreto Constituyente sobre el Sistema Integral de Criptoactivos, determinó en este tipo penal para la protección del mismo, en lo que comporta la acción típica dolosa sobre una posesión de equipos o la prestación de servicios de sabotajes, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías u ofrezca o preste servicios destinados a cumplir los mismos fines relacionados con el Sistema Integral de Criptoactivos,

con la intención de realizar algún tipo de financiamiento determinado a apoyar organizaciones o movimientos subversivos y contrarios al orden mundial, como lo son: el terrorismo, el narcotráfico o la legitimación de capitales, será penado con prisión de 1 a 3 años más una multa equivalente de 50 a 100 criptoactivos soberanos.

Responsabilidad
del funcionario o funcionaria

Artículo 49.

- El funcionario público o funcionaria pública.
  1. Que obstaculice o detenga
  2. Sin causa justificada por la Superintendencia Nacional de Criptoactivos y Actividades Conexas (SUNACRIP).
  3. La materialización de operaciones relacionadas con criptoactivos.

Será sancionado con prisión de tres (03) a cinco (05) años.

1. Acción típica: a) sin causa justificada por la Superintendencia Nacional de Criptoactivos y actividades conexas (SUNACRIP), b) la materialización de operaciones relacionadas con criptoactivos.
2. Verbos: a) obstaculizar, b) detener.
3. Sujeto Activo: los funcionarios públicos.
4. Sujeto Pasivo: el Sistema Integral de Criptoactivos.
5. Culpabilidad: Delito doloso. (Intencionalidad)
6. Naturaleza de la acción: Delito de acción pública.
7. Penalidad: de tres 3 a cinco 5 años.

El estudio jurídico de este tipo penal, determinado por el constituyentista para proteger el Sistema Integral de Criptoactivos, tiene su relevante importancia, incorporando el delito cometido por funcionario público como sujeto activo, en la comisión del tipo delictivo, desplegando voluntariamente la acción típica dolosa de obstaculizar o detener, la materialización de las operaciones relacionadas directamente con criptoactivos, sin causa justificada o autorización previa por la Superintendencia Nacional de Criptoactivos y actividades conexas (SUNACRIP), contempla este tipo penal una prisión de 1 a 3 años, sin establecerse multa al respecto.

Instrumentos Falsos

Artículo 50.

- Quien.
- Intencionalmente.
- Haga uso de:
  1. Instrumentos digitales.
  2. O documentales relacionados con el Sistema Integral de Criptoactivos.
- Cuyos datos:
  1. Sean falsos.

2. O estén alterados.

- De modo que pueda resultar en perjuicio de los particulares.

Será sancionado con prisión de tres (03) a cinco (05) años y multa equivalente de cincuenta (50) a cien (100) Criptoactivos soberanos.

1. Acción típica: a) hacer uso de instrumentos digitales o documentos relacionados con el Sistema Integral de Criptoactivos, b) cuyos datos sean falsos, c) o estén alterados.
2. Verbos: a) hacer uso, b) falsificación de datos, c) alteración.
3. Sujeto Activo: Indefinido o indiferente. (Cualquier persona imputable).
4. Sujeto Pasivo: a) el Sistema Integral de Criptoactivos.
5. Culpabilidad: Delito doloso. (Intencionalidad)
6. Naturaleza de la acción: Delito de acción pública.
7. Penalidad: de tres 3 a cinco 5 años.
8. Multa: equivalente de 50 a 100 criptoactivos soberanos.

El tipo penal establecido por el constituyentista para proteger el Sistema Integral de Criptoactivos contra instrumentos falsos y sus usos maliciosos, comporta una acción típica dolosa en la que el sujeto activo indeterminado, realiza la acción de hacer uso de instrumentos digitales o documentos relacionados con el Sistema Integral de Criptoactivos, cuyos datos sean falso o estén alterados, en perjuicio directo de particulares como sujetos pasivos del tipo delictual, estableciendo prisión de 3 a 5 años más una multa equivalente de 50 a 100 criptoactivos soberanos, es conveniente destacar que este tipo penal acarrea junto con el artículo 49 del Decreto Constituyente sobre el Sistema Integral de Criptoactivos, las penas de mayor cuantía, estableciéndose en tope de una máximo de 5 años de prisión.

Agravante o Incremento de la Sanción

Artículo 45.

- Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad:
  1. Cuando los hechos allí previstos o sus efectos recaigan sobre cualesquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas.
  2. O que contenga información personal o patrimonial de personas naturales o jurídicas.

Comporta como escenario agravante para los sujetos activos en el artículo 45 del Decreto Constituyente sobre el Sistema Integral de Criptoactivos, el cual establece como situaciones de incremento de las penas para los tipos penales contemplados en el artículo 43, con respecto a los delitos contra: 1) el acceso indebido al Sistema Integral de Criptoactivos y del artículo 44, 2) sabotaje o daño al Sistema Integral de Criptoactivos; todos del Decreto Constituyente sobre el Sistema Integral de Criptoactivos; un incremento en las penas que

oscila de una tercera parte hasta la mitad de la pena, a los sujetos imputados en los artículo anteriormente señalados, cuando los hechos recaigan sobre cualesquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas.

Al cierre sobre la finalidad, del Decreto Constituyente sobre el Sistema Integral de Criptoactivos es la protección general del propio sistema, estableciendo 5 nuevos tipos penales concebidos por el constituyentista para la protección del Sistema Integral de Criptoactivos, los cuales previenen y sancionan; en primer lugar, el acceso indebido al sistema, en un segundo tipo, el sabotaje o daño al sistema; en un tercer delito, se contempla la prestación de equipos y servicios para sabotajes internos y externos al sistema; como también en un cuarto tipo penal, se provee y condena la responsabilidad del funcionario público que obstaculice o detenga el sistema sin justificación; y en el último y quinto tipo penal, se condena el uso de instrumentos falsos para perjudicar usuarios directos e indirectos del Sistema.

La noción de lo expresado anteriormente comporta el robustecimiento y fortalecimiento del Sistema Financiero Nacional y sus demás sistemas conexos, lo cual redunda en la tutela del Estado democrático y social de derecho y de justicia que propugna y consagra la Constitución de la República Bolivariana de Venezuela.

5. Conclusiones

Es concluyente precisar que si bien el Decreto Constituyente sobre el Sistema Integral de los Criptoactivos no establece claramente el procedimiento para juzgar los delitos previstos y sancionados en la ley, el ordenamiento jurídico nacional contempla el procedimiento ordinario en el Código Orgánico procesal Penal como el viaducto jurídico procesal para establecer la responsabilidad de los ciudadanos confrontados con los tipos penales que protegen el bien tutelado directamente, que no es otro que el Sistema Integral de Criptoactivos, el cual es análogo con el Sistema Financiero Nacional, sobre el cual se sustenta y fortalece el Estado democrático y social de derecho y de justicia que consagra y ostenta la República Bolivariana de Venezuela.

También es preciso concluir que los tipos penales establecidos en el Decreto Constituyente sobre el Sistema Integral de Criptoactivos (2019), son similares a los preceptuados en la Ley Especial contra los Delitos Informáticos (2001), significando su diferencia estructural, solo a lo que respecta al bien jurídico tutelado por la norma, siendo en el Decreto Constituyente, el Sistema Integral de Criptoactivos.

Tecnología, proceso judicial y derechos fundamentales*

Mariel Alejandra Suárez**

SUMARIO: I. Introducción – Objetivos. II. De la modernización de los procesos. III. Del impacto de la tecnología en los derechos fundamentales del hombre. IV. Del expediente digital – tramitación digital completa y uso cero de papel. Como objetivos a lograr: a) La denuncia telemática. b) Participación telemática de los sujetos procesales. c) La presencia telemática de los sujetos procesales en casos de cooperación judicial. d) De la presentación telemática de escritos. e) De las comunicaciones y notificaciones telemáticas. f) Otras formas de comunicación procesal telemática posible. g) De la firma digital. h) Automatización de tareas sencillas – sistemas predictivos – experiencia en la ciudad de Buenos Aires. i) De la telematización de las medidas investigativas. j) De la modernización de la etapa de Ejecución Penal. k) Del control de medidas de protección de personas y de coerción personal morigeradas a través de sistemas de georreferenciación satelitales. V. A modo de conclusión.

Resumen

Con el presente trabajo, me propuse identificar las practicas actuales del servicio de Justicia y como ha sido el proceso de incorporación de las nuevas tecnologías a nivel nacional y a nivel provincial en la República Argentina.

Es dable señalar el sistema de Justicia en Argentina está compuesto por un Poder Judicial Nacional, que cuenta con sus propias normas procesales, y distintos Poderes

Recibido: 5/2/2020 • Aceptado: 25/2/2020

* Trabajo presentado para el Congreso de Derecho Procesal Telemático celebrado en la sede de la Escuela Nacional de la Magistratura de la República Bolivariana de Venezuela, 28 y 29 de noviembre de 2018.

** Abogada egresada de la Universidad de Buenos Aires (2001), Especialista en Derecho Penal (UBA 2011), Jueza Penal en la Provincia del Chubut (Argentina) desde el año 2009 hasta la fecha, Docente Universitaria UNPSJB desde 2010 al 2014, Especialista en Derecho Tributario ECAE (2009); Diplomada en Ciencias Sociales con mención en Constructivismo y Educación (2014), mail oficial masuarez@juschubut.gov.ar.

Judiciales Provinciales, que a su vez también cuentan con sus normas procesales, lo que responde estrictamente al carácter federal del Estado argentino.

A través de la experiencia personal en relación con esas prácticas, intentaré formular algunas propuestas que producirán una mejora en la prestación del servicio, impactando en todos los procesos judiciales en sus distintas etapas.

Palabras clave: Proceso. Derechos. Modernización.

Abstract

On this research, I proposed to identify on the current practices of the service of Justice and how the incorporation of new technologies has been at national and provincial level in the Argentine Republic.

It is significant to mention that the Justice System in Argentina is composed of a National Judicial Power, which they have their own set of laws, and different Provincial Judicial Powers, which also have their own procedural rules, which act in response of the federal characteristic of the Argentine State.

Through personal experience in relation to these practices, I will try to formulate proposals that will produce an improvement in the provision of the service, impacting on all judicial processes in their different stages.

Keywords: Process. Rights. Modernization.

I. Introducción - Objetivos

La Revolución Tecnológica impone la utilización de sus herramientas en todos los ámbitos en los que el hombre desarrolla su vida en sociedad.

El servicio de Justicia, no debe, ni puede ser un ámbito ajeno a ese movimiento de modernización, porque ello tiene relación con un aspecto central del reconocimiento activo de los derechos de los justiciables, y en definitiva asegura de una manera más eficaz, la concretización de esos derechos.

Lo ideal es que el cambio de paradigma, no sea solo por el cambio en sí mismo, sino que responda al fin de maximizar los logros en los distintos servicios de justicia a favor del hombre, máxime en el caso de sujetos involucrados a procesos judiciales, pues éstos procuran la resolución de un conflicto.

Con este trabajo, intento compartir la experiencia percibida en mi país, en función de la implementación de las herramientas informáticas, digitales, telemáticas o tecnológicas, en los procesos judiciales, reforma que se efectuó primariamente en el proceso penal, enfocándome en los efectos que tuvo en el ámbito social, ético y económico, destacando los beneficios que puede traer

aparejado la incorporación de esas nuevas tecnologías, a todos los proceso judiciales como a todas las etapas del proceso.

Analizaré las herramientas utilizadas en la actualidad en Argentina, intentaré destacar los aspectos positivos y los negativos como resultado de la implementación, proponiendo un mejoramiento de las mismas, a partir de la experiencia local, para que en conjunto podamos cumplir el objetivo que entiendo nos une, el de afianzar la justicia.

II. De la modernización de los procesos

Después de más de un siglo de convivir con sistemas procesales inquisitivos, escritos y secretos, en Latinoamérica se han ido reformando los procesos judiciales en pos de instalar sistemas orales, públicos y de tipo acusatorio, donde las partes tienen bien definidas sus funciones, el Juez decide, el Fiscal investiga y las tareas administrativas del proceso están a cargo de un órgano burocrático, llamado en muchos casos Oficina Judicial.

El Proceso Penal ha sido el pionero en ésta área, por lo menos en Argentina. A partir de esa experiencia, la modernización del proceso intenta trasladarse a otras áreas[1].

La teoría general del proceso es la base de todos los procesos judiciales y, sus principios aplicables a todas las ramas del Derecho. Esta modernización de los procesos penales, se tradujo directamente en la reforma de sus códigos, incorporando normas constitucionales y convencionales como base fundamental de todo el procedimiento.

No fue algo que decididamente se hizo de un día para el otro, sino que comenzó con la incorporación de los tratados y convenciones internacionales a la legislación interna, constituyendo así Derecho Supremo de cada país, por lo que necesariamente sus principios se debieron volcar a legislaciones procesales y de fondo sin discriminación.

Fue un crecimiento desde lo macro (lo mundial) hacia lo micro (cada país), y por supuesto una incorporación aceptada por las distintas normas Fundamentales de cada Pueblo.

Podríamos decir entonces que en materia de concesión de derechos, de incorporación de derechos internacionales al derecho interno y en materia de modernización de la justicia, los pueblos latinoamericanos vienen andando el mismo camino.

Esta modernización de los procesos desde el aspecto práctico, en su mayoría, significó la incorporación de sistemas de informatización al servicio de la justicia, dando vida al expediente judicial, a la grabación de audiencias en soportes magnéticos con acceso directo a operadores del sistema y partes, a la publicidad

1 Política de Estado a Nivel Nacional "Justicia 2020" data en https://www.justicia 2020.gob.ar/ o http://www.jus.gob.ar/media/3139950/JUSTICIA%20VEINTEVEINTE.pdf, consultadas el 03/11/2018.

de los procesos, a la incorporación del expediente digital, a las comunicaciones digitales a través de cuentas oficiales o no de *email* con letrados y operadores, a la incorporación de sistemas de audiencia con videoconferencia (audiencias a la distancia) a través de distintos organismos judiciales, a la creación de oficinas judiciales (equipos de trabajo destinados a cumplir las tareas administrativas del proceso, como ser el manejo del calendario judicial, licencias del personal, etc.), la creación y mejoramiento de páginas *web* oficiales de los poderes judiciales en los que se fueron incluyendo información demandada por los ciudadanos en general y por las partes del proceso, el uso de equipos de *hardware* y *software* de los distintos operadores, la utilización de la firma digital, todo ello con el fin de que impacte de manera favorable en el servicio de justicia.

La demanda de información por parte de los ciudadanos, generó inexorablemente que se crearan páginas en las que se publicara información judicial analizada, respetando así los principios de publicidad de los procesos. Subyaciendo de lo dicho, dos acepciones del concepto publicidad, por un lado la publicidad de aquellos actos del tribunal para las partes del proceso garantizando el debido proceso legal y, por el otro lado la publicidad para los ciudadanos en general como garantía de control público esencial para el funcionamiento del Poder Judicial en una Sociedad Democrática, también relacionado estrictamente a la imparcialidad del Juez[2].

La publicidad como característica del sistema democrático de gobierno, es el más valioso instrumento de fiscalización popular sobre la obra de los magistrados, ya que en último término, es el pueblo el que juzga los actos de los jueces[3], y esto se ha tenido en cuenta también en los procesos de modernización de la justicia.

III. Del impacto de la tecnología en los derechos fundamentales del hombre

La preocupación central de los estados nacionales o provinciales, y concretamente del Poder Judicial de cada uno de ellos, es satisfacer la demanda de información que reclama el ciudadano sobre los actos de la justicia.

Con este fin, se crearon páginas *web* que tienden a transparentar la mayor cantidad actos de ese poder.

En las páginas se agregó información de localización y contacto de las distintas sedes y operadores de la justicia, incluso en algunos países se implemento el *chat* con funcionarios en forma directa[4] [fue el caso de nuestros hermanos

2 Norberto Bobio afirmaba "que la democracia es igualmente el gobierno del poder visible, o sea el poder que se ejerce o debería ejercerse siempre en público".

3 COUTURE, (1962) "Fundamentos del Derecho Procesal Civil", Buenos Aires.

4 MUNDACA, Julio, Dirección de Comunicación Poder Judicial Chile, realizada por Ricardo LILLO para *Revistas Judiciales* año 9 N° 16, página 80, el cual puede ser consultado en http://sistemasjudiciales.org/nota.mfw/397

chilenos, con un resultado satisfactorio y utilizando redes sociales ya existentes], se agregó jurisprudencia, doctrina, notas de interés, noticias judiciales con imágenes, grabaciones de audiencias realizadas, calendarios de audiencias, *links* de interés, entre otros agregados.

Sin embargo en ese camino, por satisfacer la necesidad de información, se descuidaron otros aspectos relacionados con los mecanismos de acceso a la justicia, con afectación directa de los derechos del hombre.

Convengamos en que el Estado está obligado a brindar un servicio de justica claro, sencillo, de fácil acceso, expedito, remoto, instantáneo, que garantice el debido proceso legal, que tutele efectivamente los derechos de las víctimas, que proteja eficazmente personas vulnerables, enfocado en el hombre y para el desarrollo de éste.

No basta con satisfacer la demanda de información.

La modernización es también una obligación del Estado que pasa por entender que debemos incorporar tecnología a los procesos judiciales y cumplir con los ejes de ésta, que facilitan la concreción de los derechos del hombre: la tramitación digital completa y la utilización cero de papel.

Que ello tiene impacto directo en todos los procesos judiciales y en todas las etapas, beneficiando a todos los intervinientes, pero que se advierte un claro impacto directo, sobre los procesos en donde se investiga violencia de género, doméstica o sexual, cuyas víctimas se encuentran más expuestas requiriendo un tratamiento especial.

El beneficio de la implementación de la tecnología en los procesos judiciales, radica básicamente en simplificar ciertos actos procesales engorrosos por la distancia de las personas con las sedes judiciales o por la temática investigada, acercando el servicio de justicia para que sea realmente accesible, remoto, eficaz y automático.

IV. Del expediente digital – tramitación digital completa y uso cero de papel, como objetivos a lograr

En Argentina, recientemente se ha puesto en marcha el decreto de "Tramitación digital completa" en la Administración pública[5] Nacional. Con este decreto se pretende efectivizar aún de mayor manera los trámites a nivel Estatal, quitándole la burocracia propia del papel, acercando a los ciudadanos al organismo correspondiente a través de sus computadoras, celulares o *tablets,* en la realización de distintos trámites.

Es dable señalar, que en la actualidad, varios organismos del Estado Nacional y de los distintos Estados Provinciales, cuentan con la posibilidad de efectuar trámites a distancia desde los distintos sitios *web* del órgano que se trate, ya sea

5 Decreto PEN 733/2018 Publicado en el Boletín Oficial de la República Argentina el día 09/08/2018 disponible en www.boletinoficial.gob.ar

mediante acreditación de identidad por el sistema de creación de usuarios y claves o con el aporte de datos biométricos, como es el caso de la Administración Federal de Ingresos Públicos (AFIP).

Que en relación a ello, puedo señalar normas de distinto rango que fueron fomentando la utilización de tecnología a favor de la eliminación de la burocracia en los trámites estatales.

Mientras que por el decreto 252/2000 Poder Ejecutivo Nacional que creó el programa Nacional para la Sociedad de Información, el Decreto del P.E.N. 434/2016 creó el Ministerio de Modernización, para de alguna manera unificar objetivos.

En la esfera judicial, el proceso de informatización, ocurrió en forma dispar en los poderes judiciales de algunas provincias, que pusieron en marcha en el ámbito penal en forma conjunta con el proceso oral, el expediente digital, entre otros institutos telemáticos.

A modo de ejemplo, desde el año 2006 en el caso de la Provincia del Chubut, más tarde en La Pampa, Rio Negro, Neuquén, entre otras, se fue implementando este sistema de expediente digital que, lamentablemente, se utilizó siempre en forma paralela con el expediente de papel. A su vez se implementó las comunicaciones telemáticas[6] y la realización de audiencia a través del sistema de video conferencia.

En el caso no se exige que los medios a través de los cuales se realice la audiencia por el sistema de video conferencia, requieran aprobación previa, como ocurre en Venezuela, en que mediante Resolución 2016-001 del Tribunal Supremo de Justicia, requiere en su artículo 1°, la aprobación previa del medio de comunicación telemático empleado.

Si bien la implementación de procesos digitales implica la conformación de procesos de gestión remota, simple, automática, ágiles e instantáneo, es notable que la continúa duplicación del expediente en papel, no consigue lograr el propósito central de la repercusión en los costos o a nivel ambiental.

Sin embargo, en Argentina, la Provincia de Neuquén, con la implementación más tardía de los procesos judiciales digitales, logró terminar con la dualidad de mantener el expediente en versión papel.

Lo que ocurre en general es que no se logra la confianza plena en la utilización del documento electrónico como único soporte de base de datos. Aún se sigue desconfiando de su nivel de seguridad; éste comportamiento puede deberse al desconocimiento sobre el tema, debido a una falta o deficiente capacitación respecto de seguridad y de la posibilidad de adulteración que brinda la mecanización de las actos procesales y los documentos electrónicos.

No podemos desconocer que la utilización del papel en la prestación del servicio de justicia, genera gastos innecesarios de insumos y de mantenimiento

6 Acuerdo Sala Penal 12/2006 de fecha 24/10/2006 art. 1° "Las comunicaciones Procesales que realice la Oficina Judicial (OFIJU) a los Defensores Generales, Fiscales, Querellantes y Defensores Particulares, se realizará mediante Correo electrónico Firmado Digitalmente".

de equipos, pero fundamentalmente, una tramitación más lenta, menos eficiente y menos transparente de los procesos en general.

Por ello, la telematización del proceso debe impactar sobre la totalidad de los actos procesales, que en definitiva van a integrar el expediente telemático.

Realizaré unas breves consideraciones de cómo funcionan, como deberían funcionar y que debería cambiarse respecto de la forma en que se llevan adelante algunos actos procesales telemáticos trascendentes.

a) La denuncia telemática

Una Justicia que pretenda ser digital en su máxima expresión, debe contar con una tramitación digital en forma completa, desde los inicios del proceso hasta su finalización con la ejecución de la sentencia.

Enfocándome en el proceso penal, diré que debe poderse tramitar en forma telemática desde la interposición de la denuncia, la etapa de investigación, la etapa preliminar, la etapa de debate oral y público, los recursos, y finalmente la ejecución de la pena.

En la actualidad, en lo que respecta a la denuncia, en Argentina existe la posibilidad de denunciar ciertas conductas ilícitas a través de números de teléfonos específicos, pero la denuncia siempre es personal ante la sede del Ministerio Público Fiscal o las distintas Comisarías zonales.

Más allá de la implementación de un sistema de enjuiciamiento oral y del expediente digital en Chubut, cierto es que la única forma de denunciar es a través de hacerse presente físicamente en los lugares antes mencionados.

Como novedad, recientemente en la Ciudad Autónoma de Buenos Aires, se implementaron unas cabinas de video *chat* o video conferencia en las dependencias policiales, con conexión directa a sedes del Ministerio Público Fiscal (MPF), las cuales en esa ciudad se encuentran descentralizadas por barrios[7], con el propósito de dar paso a una forma de denuncia telemática, para todo tipo de delitos.

Realmente, esta solución parece innovadora en relación con el sistema de denuncias vigente, pero no completa de forma eficiente los objetivos del trabajo y paso a explicar porque.

Si bien la implementación de estas cabinas, acercan a los ciudadanos con el órgano acusador del proceso penal, no evita la circunstancia de que la persona deba trasladarse a la dependencia policial más cercana, como tampoco reduce costos, pues debe implementarse una cabina en cada circunscripción judicial, teniendo la posibilidad de realizar éste trámite a través de medios tecnológicos y *software* ya utilizados por la sociedad en general.

7 Nota 31/10/2018 https://www.clarin.com/policiales/nuevo-sistema-cabinas-denunciar-robos-capital_0_coVoAzlZt.html; Nota 30/10/2018 https://www.infobae.com/sociedad/2018/10/30/ya-se-pueden-hacer-denuncias-por-videoconferencia-en-todas-las-comisarias-portenas/.

Allí justamente es donde radica mi propuesta, para que la denuncia pueda efectuarse a través de una plataforma digital ya creada o a crearse, a la que todos los ciudadanos tengan acceso, por medios electrónicos comunes ya utilizados por éstos.

Esa plataforma digital podría ser a través de una aplicación o desde la propia página *web* de cada poder judicial, en la que el ciudadano pueda registrarse y crear un usuario, acreditar identidad con la digitalización del documento de identidad o su incorporación a través de un código de barras, pues estamos hablando de una plataforma digital pública, en la que se pueda completar un formulario de denuncia que llegue directamente al órgano acusador o Ministerio Público Fiscal para poder dar inicio a esa causa.

El éxito de esta propuesta, radica en la agilización de los trámites que dan inicio al proceso penal y, podría ser aplicable incluso a otras materias, ya sea laboral, familia, reclamos civiles, administrativos o de cualquier otra índole.

Destaco, que sería muy conveniente y tendría un beneficio inmediato, los procesos en donde se investigue violencia doméstica, sexual o de género pues también se podrían dictar las medidas de protección hacia la víctima, de forma más expedita, ya que luego de recibida la denuncia el funcionario actuante puede dar inmediata intervención a un juez de turno del fuero penal o de familia, a través del mismo sistema.

En la actualidad en Argentina esto no se está llevando a cabo, la gente mayormente debe trasladarse a los lugares físicos dispuestos a recibir una denuncia, llámese Comisaría o sede del Ministerio Público Fiscal, sometiéndose al denunciante a un engorroso trámite de espera, que repercute en forma negativa en su vida laboral y privada.

La ventaja de la denuncia telemática, es que asegura la tutela judicial efectiva de los justiciables que reclaman por sus derechos, se trate del fuero que se trate, y evita la descentralización y creación de nuevas sedes del M.P.F., evitando la creación de nuevos puestos de trabajo innecesarios, ya que la misma gente que se encuentra trabajando en la actualidad, encargada de recepcionar las denuncias personales, será la que analice la seriedad y procedencia de las denuncias volcadas a través de ésta plataforma.

Advierto que esta propuesta tiene una incidencia directa en el presupuesto que se destina a la justicia, impacta directamente en la sociedad mejorando la imagen del servicio que presta la justicia acercando al ciudadano a través de la utilización de un servicio sencillo y al alcance de todos. ´

Ya no basta que el ciudadano tenga la posibilidad de ser informado a través de los medios tecnológicos de cómo proceder frente a una determinada situación en la que se encuentran vulnerados sus derechos, hoy resulta imprescindible que junto a la información obtenga la asistencia directa para accionar mecanismos que solucionen sus reclamos y, sin lugar a dudas la tramitación del expediente digital exige la posibilidad de entablar una denuncia digital o el inicio del trámite en forma digital.

Este mecanismo, puede ser aplicado al inicio de la demanda en otros procesos no penales.

En Argentina a nivel nacional o provincial, aún no se cuenta con esta posibilidad, dado que se continúa con el inicio de los distintos reclamos, a través del sistema escrito, acompañando tantos juegos de copias como partes existan en el proceso.

Resultaría de sencilla implementación, la interposición de la demanda en forma telemática, pues todo se reduciría a la utilización de una plataforma digital, una página o un programa o una dirección de correo a la que se pueda remitir el reclamo.

Pero, la implementación de ello, resulta un camino aún a trazar en nuestro país, en donde los primeros pasos, los está dando la Administración Pública Nacional, con la implementación de mecanismos digitales en la realización de trámites.

b) Participación telemática de los sujetos procesales

Cuando analicé la posibilidad de entablar la denuncia digital en el fuero penal o la interposición digital de la demanda en otras ramas del Derecho, pensaba también en la posibilidad de completar la denuncia con una especie de entrevista entre el denunciante y la persona que recibe la denuncia, no solo a través de la creación de un formulario contenido en una aplicación o en una página digital, sino en la posibilidad de completar la denuncia con el mecanismo de video conferencia con medios utilizados en forma masiva por la sociedad.

Recién en Argentina, se pudo pensar en aceptar este tipo de participación, en los albores del año 2006 en la Provincia del Chubut, en la que se modificó el paradigma procesal, en el que la mayor cantidad de actos del proceso se realizan a través de audiencias orales y públicas.

Frente a la frustración de las distintas audiencias, se comenzó a utilizar los distintos sistemas de video-comunicación que se encontraban instalados en las distintas sedes judiciales con fines de comunicación interna ya que las distancias entre las mismas oscilan entre 400 y 700 Km, con lo cual se redujeron costos de traslados de los sujetos procesales, que muchas veces insumía el propio órgano en pos de concretar el acto procesal y otras veces los particulares.

No existe legislación que habilite su utilización en forma específica, la costumbre se fue imponiendo como una práctica que benefició el modelo de proceso que se estaba instalando.

Hoy, muchas de las audiencias, imputación de cargos, audiencias de elevación de la causa a juicio, audiencias de debate oral en donde se interroga víctimas y testigos, se efectúan a través del sistema de videoconferencia instalado en todas las jurisdicciones de la Provincia, pero también esta conexión se realiza con otros poderes judiciales se encuentren o no, transitando por el mismo proceso de cambio.

Los sujetos procesales se presentan ante la sede más cercana a su domicilio (víctima, imputado o testigo), acredita su identidad y se lleva adelante la audiencia sin mayores inconvenientes a través de éste sistema que completa la exigencia de inmediación del juez y las partes porque se toma contacto instantáneo y automático aunque no físico.

Mi propuesta en relación a éste aspecto, va un poco más allá de este sistema que se está llevando adelante en varias provincias argentinas.

Pienso, en que una tramitación eficiente y eficaz del proceso, autoriza a habilitar la utilización de medios utilizados en forma masiva, por todos los ciudadanos.

Estimo que acreditando la identidad en forma previa, incluso exhibiendo en forma no presencial la documentación que acredite la identidad, la que podría escanearse a través de un código de barras por ejemplo, se podría efectuar la audiencia a través de un sistema de video conferencia como *Skype, Messenger, Zoom* o *Whatssapp* el que incluso se relaciona con un número de teléfono.

El planteo innovador radica, en la utilización de este sistema, por parte del sujeto procesal, desde su domicilio o su lugar de trabajo, mientras que el juez que intervenga puede aprobar la utilización del medio empleado.

Considero que una participación telemática en los procesos judiciales, para contemplar todas las facetas de la vida del hombre, debe permitir una participación amplia, con la utilización de todos los medios de comunicación masivos que el hombre actual tiene a su alcance.

Que la incorporación de tecnología a los distintos procesos judiciales no afectaría la intimidad o privacidad del ciudadano, límite constitucional y convencional, respecto de cualquier tipo de intromisión estatal[8].

Su utilización se justifica, en función de que consagra aún más los principios de oralidad e inmediación entre los sujetos procesales y el juez, pues se trata de un sistema de comunicación bidireccional y simultáneo, en donde se obtiene en tiempo real la voz y la imagen de los sujetos que participan, no afectando la utilización de éste medio, la percepción que el juez tenga de la persona que participa.

Que éste puede ser un instrumento procesal válido, pudiéndose contar con la sola aprobación del juez interviniente para su utilización.

Que además la documentación de dicho acto, también puede ser de modo electrónica, en forma conjunta con la video grabación, algo que en Chubut esta específicamente contemplado[9].

8 Art. 19 C.N. "Las acciones privadas de los hombres que de ningún modo ofendan al orden público y a la moral pública, ni perjudiquen a un tercero, están solo reservadas a Dios, y exentas de la autoridad de los magistrados….", Constitución Nacional Argentina año 1853, reformada en 1994.

9 Art. 131 CPP de Chubut "Se podrá utilizar imágenes y sonidos o grabaciones digitalizadas para documentar total o parcialmente actos de prueba o audiencias, quedando prohibida toda forma de edición, tratamiento o modificación de los registros. Se deberá asegurar su autenticidad

Ello repercute beneficiando todo tipo de procesos judiciales pero especialmente, en aquellos en los que intervengan sujetos vulnerables o especiales, ya sea en razón de edad, su padecimiento de salud o por la entidad del delito que lo afectó o en el que participó, procurando una expedita intervención, simplificando actos procesales engorrosos, a favor de preservar al hombre, su dignidad y sus derechos fundamentales.

c) La presencia telemática de los sujetos procesales en casos de cooperación judicial

La propuesta del uso de sistemas de video *chat* o videoconferencia o video-teleconferencia, utilizados en forma masiva por los ciudadanos, a través de sus equipos electrónicos de uso diario, puede tener también una incidencia positiva, en los casos de cooperación judicial internacional.

Por ejemplo, cuando un testigo, víctima o imputado se domicilie en otro país o estado, se puede utilizar no sólo para procurar la participación telemática en actos procesales sino que para realizar el intercambio de documentación por medios electrónicos.

Esta modalidad de participación a nivel inter estatal e internacional, no se ha puesto aún en práctica en Argentina.

Como antecedente legislativo a nivel internacional puedo citar, la Convención de Palermo[10] sobre crimen organizado, en relación a la cooperación judicial internacional, que establece la utilización de la videoconferencia siempre que sea posible y compatible con los principios fundamentales del derecho interno.

Siempre se prevé en relación a la declaración de testigos y peritos y en el caso en que no puedan comparecer personalmente al territorio del Estado en que se requiere su presencia, o sea, que se prevé de manera excepcional y no aplicable a personas acusadas, requiriendo la doble presencia judicial, tanto en el lugar donde se recepciona el testimonio como en el que se practica la audiencia.

El segundo protocolo al Convenio de Cooperación Penal del Consejo de Europa de 1959, de fecha 08 de noviembre de 2001, incorpora gran parte de los avances del Convenio 2000 en materia de cooperación internacional por medios telemáticos, también relacionados a testigos o peritos excluyendo en forma taxativa al acusado.

En materia de cooperación judicial internacional, ha tenido un desarrollo más próspero y con menos limitaciones quizás, el sistema de intercambio de

e inalterabilidad. La ordenará siempre una autoridad competente, acordando a las partes la oportuna intervención, y siempre será objeto de control por un juez a los fines de la validez del proceso" ley XV N°9 (ex ley 5.478), Chubut, año 2006 y sus modificatorias.

10 Resolución Asamblea General de las Naciones Unidas N° 55/25 de diciembre de 2000.

documentación electrónica como producto de la cooperación judicial internacional[11].

La ampliación del uso de este tipo de sistemas de comunicación, agilizaría los procesos, impidiendo la frustración de los actos procesales necesarios para el desarrollo del mismo, promoviendo en forma intensiva la colaboración e intercambio judicial internacional, actualiza y vincula a los ciudadanos de distintos estados, generando confianza entre los distintos gobiernos, no sólo en casos de delincuencia organizada, sino aplicada en los procesos en los cuales sea requerida la presencia de un ciudadano que no se encuentre residiendo, habitual o temporalmente, dentro del Estado requirente.

El objetivo de los distintos poderes judiciales del mundo, deben ser comunes. Todos debemos esforzarnos para que el proceso judicial sea en mecanismo ágil de resolución de conflictos, que el servicio de administración de justicia garantice el respeto irrestricto por los derechos del hombre.

La única forma de lograrlo es trabajando en equipo, creado o modificando legislación interna, creando o modificando legislación internacional, o sencillamente generando protocolos de buenas prácticas entre los Estados.

No generaría inconveniente de aplicación la propuesta, si se establecen cuestiones básicas con las exigencias necesarias, sin exageraciones.

Temas como la identificación de los sujetos procesales, deben estar resueltos de manera sencilla, y la validación de los actos llevados a cabo a través de estas modalidades debe constituir una prioridad.

La videoconferencia contribuiría a la conveniente deslocalización geográfica de la víctima de violencia de género, para el acusado y su entorno, evitando la oportunidad de ser perseguida después de la celebración de la comparecencia, en aquellos casos más graves, de residencia protegida o en niveles de riesgo extremo.

Otro motivo que sin duda legitimaría la utilización de la videoconferencia, lo es en supuestos en que previsiblemente se pueda alterar el desenvolvimiento correcto de la audiencia en forma presencial, garantizando el desarrollo de la misma en un clima de tranquilidad y respeto contribuyendo al normal funcionamiento institucional.

d) De la presentación telemática de escritos

A partir de páginas *web* específicas o un *software* instalado para cada Poder Judicial, hoy los operadores de la justicia y las partes acceden al expediente digital.

El proceso oralizado, cuenta con salas informáticas, donde se graban los distintos actos procesales que se llevan a cabo en las audiencias.

11 Barbero, 2018, data en https://www.eleconomista.es/legislacion/noticias/9179963/06/18/Bruselas-da-un-paso-mas-en-la-digitalizacion-de-la-Justicia-europea.html; también puede verse en http://europa.eu/rapid/press-release_IP-18-3991_es.htm consultada en 31/10/2018

Los audios y las actas telemáticas se cargan en el expediente digital, para que finalmente todos los operadores y partes intervinientes tengan acceso a él.

El proceso de la carga de datos no debe ser como se viene realizando en Argentina, que se presentan por mesa de entradas algunos escritos y luego se digitalizan e incorporan al expediente telemático.

En este aspecto, si bien el expediente digital ha logrado un cierto grado de aceptación local, lo cierto es que las presentaciones continúan siendo en formato de papel, por ello resulta claro que lo ideal sería la generación del expediente digital sea más sencilla para las partes.

Que las peticiones puedan hacerse a través de un *email* oficial o correo oficial, que se adjudique a las partes en forma previa por autoridades competentes y, que la presentación se efectúe directamente al mail de la oficina judicial o juzgado interviniente y se cargue en forma automática a dicho expediente previamente individualizado, y en el que las partes ya se encuentran vinculadas.

Que deben instalarse buenas prácticas en materia de presentación telemática de escritos, este aspecto, repercutiría provocando una mejora en la administración del tiempo de las partes.

Que la carga manual de datos o la digitalización de presentaciones escritas, no puede ser parte de una verdadera justicia telemática.

Por otra parte, frente al reclamo por escrito de un particular no letrado, puede subsanarse con el ingreso de los datos en forma digital por un empleado del organismo, contribuyendo a la tramitación del expediente digital.

La forma propuesta optimiza, simplifica y facilita la creación, el control y la consulta del expediente telemático, repercutiendo en la concretización de los derechos de los justiciables en cuanto a la celeridad del proceso y el acceso sencillo a la información de los actos allí desarrollados.

e) De las comunicaciones y notificaciones telemáticas

Hoy en día la utilización del papel en forma conjunta con la utilización de la informática es moneda corriente en la Administración Pública Nacional, Provincial y en los distintos Poderes Judiciales como en otros órganos estatales.

Este binomio "Papel-Plataforma Digital" debe desaparecer indefectiblemente.

El área en el proceso judicial, en que más se nota la incompatibilidad de éste binomio, al menos en Argentina, es sin duda en el de las comunicaciones procesales.

Las comunicaciones (cédulas, oficios, exhortos) se realizan a las partes técnicas (letrados), a otros organismos del estado (policía, policía científica, policía judicial o de investigación, hospitales, clínicas, otras oficinas estatales y oficinas privadas etc.) y a ciudadanos involucrados como víctimas o victimarios y a posibles testigos.

Las mismas se vienen implementando en forma de papel para todos menos para los letrados o partes técnicas que se les remite la comunicación procesal en forma telemática vía mail a una casilla otorgada por el organismo oficial previa acreditación de la identidad.

El principal problema que se genera podría ser la validación de la notificación electrónica, o bien para definirlo de otro modo, a partir de qué momento se puede considerar que se ha hecho efectiva la comunicación.

A modo de ejemplo, cito el C.P.P de Chubut que en su artículo 160 establece la facultad de las partes para que en cada caso concreto acuerden expresamente "*..una modalidad de comunicación efectiva de acuerdo con las posibilidades técnicas a las que ellas tengan acceso y el juez o tribunal..*".

Por lo que sin regular en forma específica la modalidad de las comunicaciones electrónicas, deja un margen para que pueda instalarse al menos progresivamente y en cada caso concreto.

En ese orden de ideas, y dentro de las facultades que le confiere la norma referida, el Superior Tribunal de Justicia local, mediante acuerdo 12/06 de fecha 24/10/2016 la realización de las comunicaciones procesales mediante correo electrónico firmado digitalmente, para defensores públicos y privados, fiscales, querellantes y la OFIJU.

También refiere la normativa mencionada, sobre la oportunidad en que se tiene por efectivizada la comunicación y al respecto señala que la oportunidad será cuando sea leída por el destinatario o bien sin estar leída a los tres días hábiles de su recepción, no dejando lugar a dudas al respecto de su efectividad.

En el caso de Venezuela, la legislación vigente en la materia resulta disímil a la de Argentina, pues LOJCA de fecha 27/06/2010 en su artículo 38 establece la facultad de practicar las notificaciones por medios electrónicos, dejándose constancia en el expediente, momento a partir del cual se lo tiene por notificado y comienzan a correr los plazos correspondientes, remitiéndose a la Ley Sobre Mensajes de Datos y Firmas Electrónicas de fecha 13/12/2000 (ley n° 1.204) que establece como regla general, que el mensaje de datos se tiene por emitido cuando el sistema de información del Emisor lo remita al destinatario, salvo acuerdo en contrario, en el que podrá considerarse notificado con acuse de recibo dentro del plazo de 24 horas, transcurrido dicho plazo se tendrá por no emitido.

Sin perjuicio del sistema que se adopte, resulta necesario legislar a favor del reconocimiento del mensaje de datos digital.

Con los alcances que sean necesarios implementar para tener por valida esa comunicación, tanto desde el aspecto temporal como del contenido.

Lo que advierto es que, aún no se ha contemplado la posibilidad de extender el uso del mensaje de datos electrónico a los particulares a los ciudadanos en general, que participan en el carácter que sea, de un proceso judicial, a los que aún se les envía comunicaciones en papel, algo que resulta claramente contrario al expediente digital.

Que ello, podría subsanarse con la creación de una aplicación o una plataforma de uso general en el celular, o la implementación de un espacio en la página *web* del Poder Judicial que se trate, en donde previa creación de un usuario y acreditación de la identidad sin necesidad de disponer de ningún otro dispositivo, se puede incorporar al ciudadano a la comunicación telemática.

Los documentos a notificar deberán estar firmados digitalmente por quienes adoptan las distintas disposiciones a notificar.

Las ventajas de éste sistema son infinitas, se ahorra personal para efectuar la notificación, la utilización de papel, tiempo, dinero y, se obtiene la inmediata incorporación de la notificación al expediente digital, se asegura la concreción de actos trascendentes del proceso y no tiene que invertirse en nueva tecnología para incluir a los ciudadanos.

f) Otras formas de comunicación procesal telemática posible

Recientemente en la Provincia del Chubut (Argentina) se realizó un concurso auspiciado por el Superior Tribunal de Justicia, cuya temática era la "innovación en la Administración de Justicia". En el marco de dicho evento, se presentó un proyecto relacionado a las comunicaciones telemáticas.

El proyecto presentado consistió en la utilización de una tableta por parte de los notificadores, con la posibilidad de que los notificados puedan firmar digitalmente sobre dicho aparato e incorporarse inmediatamente al expediente digital.

Este modo de notificar a particulares, podría ser considerado novedoso, con una fuerte crítica de mi parte en la inversión de insumos que hay que realizar y algunos poderes judiciales no están en condiciones de ello.

La propuesta anterior es ampliamente superadora de ésta última.

g) De la firma digital

Un instrumento de gran utilidad en el expediente telemático, a parte de los sistemas de *software* y *hardware* rápidos, es sin duda la firma digital, regulada en Argentina mediante ley nacional N° 25.506 del año 2001[12].

Cada Estado, debe procurar una tramitación sencilla, remota, inmediata y eficaz, que promueva su utilización generalizada de este instrumento, pues la burocracia instalada en el otorgamiento desalienta su utilización.

Este tipo de instrumento, no puede generar un costo al Estado, pues incluso cada ciudadano puede portar una firma digital propia para la realización de trámites públicos y privados.

12 En Venezuela mediante Ley 1.204 "Ley Sobre Mensajes de Datos y Firmas Electrónicas" de fecha 13/12/2000 publicada en Gaceta Oficial N°37.076.

Cuando hago hincapié en los costos me refiero a que no debe insertarse en un aparato o elemento electrónico, como ocurre en Argentina que se otorga solo a personas relacionadas con la función pública y para ser utilizada a través de un "*token*" que es el instrumento que la contiene, generándose a veces el inconveniente de falta de *stock*.

Sin duda, este eslabón es trascendente para la creación y formación continua del expediente digital.

La utilización actual, se da en el marco del fiscal para la presentación de peticiones ante el juez, el juez la utiliza para la firma de decretos, resoluciones y sentencias, la oficina judicial para suscribir las comunicaciones, y así el resto de los operadores estatales.

No encuentro inconveniente a la extensión de este valioso formato de identificación, al resto de los ciudadanos que no ejercen la función pública.

Esta idea no es descabellada, pues un simple código electrónico puede conformar la firma digital y ser aplicada por ejemplo en los nuevos contratos digitales o los llamados "*smart contract*".

Por ende la extensión del uso de ésta herramienta digital, hacia los particulares que participan de procesos judiciales, resultaría una idea prospera para la construcción del expediente digital.

h) Automatización de tareas sencillas – sistemas predictivos – experiencia en la ciudad de Buenos Aires

En la ciudad autónoma de Buenos Aires, en el ámbito del Ministerio Público Fiscal, se implementó éste año, un sistema de predicción en la resolución de casos, diseñado por operadores de esa área y, con el fin de que el sistema resuelva causas de menor complejidad para que el ser humano se avoque a causas de mayor complejidad.

Por supuesto que el proceso de predicción se logra luego de una exhaustiva carga de datos y de que el propio sistema acceda a datos ya volcados en otras páginas.

Relatan los creadores, que a partir de un caso el programa identifica y lee más de 300.000 documentos vinculados con el expediente, relaciona los patrones de dictámenes del órgano y en tan solo 15 segundos, predice la solución que debe adoptarse, siempre atravesando el filtro de la revisión obligatoria posterior hecha por un operador.

Dicen que es capaz de resolver 1.000 expedientes en 7 días de trabajo, y que esa misma cantidad de causas sin el sistema demandaría más de 83 jornadas de trabajo[13].

13 CORVALAN, Juan Gustavo (12/03/2018) "Prometea, el servicio de inteligencia artificial utilizado en la justicia argentina" data en https:laley.pe/art/5009/; Corvalan, Juan Gustavo (29/09/2017) La Primera Inteligencia Artificial predictiva al servicio de la justicia: Prometea" publicado en La Ley Tomo E año 2017, 1.

Por otro lado, quienes cuestionan la implementación de estas tecnologías, apelan al desempleo que generaría en un futuro.

El Foro económico mundial en su informe *The Future of Jobs* predice que para el año 2020, se perderán 5 millones de empleos, por la automatización y robotización del trabajo.

Por su parte el Banco Mundial, advierte que 2/3 de los trabajos del mundo pueden automatizarse, sin embargo la OIT habría estimado que la tasa de desempleo a nivel mundial tendría un leve descenso hasta el 5,5% en 2016, 5, 6 en 2017, estable en 2018 y en el 2019 sin cambios[14], anuncios que parecen haberse cumplido según el informe Inicial para la Comisión Mundial sobre el futuro del trabajo en el mundo[15]

Sin perjuicio de la importancia del empleo a nivel mundial, la aplicación de la tecnología en la vida diaria no es el único factor a ponderar como generador de desempleo.

La mecanización de tareas en las actividades laborales diarias, bien utilizada, puede contribuir a la satisfacción de otros derechos humanos relacionados con la recreación, esparcimiento, mayor contacto familiar, espacio temporal para desarrollar tareas de interés personal, incluso pueden mejorar el ámbito laboral, reduciendo la carga de trabajo y permitiendo al juzgador atender cuestiones complejas.

i) De la telematización de las medidas investigativas

En los albores del proceso, no sólo es importante contar con la posibilidad de denunciar o comunicar los actos procesales en forma telemática, sino que esa modalidad debe ser extendida a la realización de medidas investigativas, como allanamientos, intervenciones telefónicas, aperturas de teléfonos y ordenes de detenciones.

La utilización de la firma digital, válidamente reconocida por los gobiernos a través de sus distintos mecanismos legislativos, con más la utilización de correos oficiales en las comunicaciones telemáticas, lleva a considerar que pueda aplicarse este sistema a las medidas investigativas solicitadas por el fiscal, autorizadas por el juez y ejecutadas por personal policial.

Esto ya es una práctica habitual en Chubut (Argentina) y, quienes nos enrolamos en fomentarla, sencillamente utilizamos los mecanismos que tenemos a nuestra disposición.

El proceso es sencillo, se crea un documento electrónico [orden de allanamiento], con un número de registro digital, se firma digitalmente, se envía

14 OIT, 2015, "World Employment Social Outlook. Trend 2018" p. 8 data en https://bit.ly/2DrnoPt consultada el 03/11/2018.

15 OIT, 2017, Informe que puede leerse en http://www.ilo.org/wcmsp5/groups/public/—dgreports/—cabinet/documents/publication/wcms_591504.pdf consultada el 04/11/2018.

por correo oficial a un destinatario con correo oficial [Personal Policial y/o Ministerio Público Fiscal], se pide acuse de recibo en el caso de correos no oficiales, evitándose en el empleo de este mecanismo la utilización de papel, tinta, tiempo de diligenciamiento, ya que la orden sólo es impresa por el personal policial para ser entregada al destinatario de la medida, práctica que debe modificarse, a modo de cumplimentar los objetivos propuestos quizás notificando mediante las aplicaciones una vez formulada la orden, será algo en lo que habrá que desplegar el ingenio para efectivizarlo, además de dotar de los recursos necesarios al área en cuestión.

j) De la modernización de la etapa de ejecución penal

Una etapa sensible del proceso penal, a la que no ha llegado al menos en la Argentina, la revolución digital, es sin duda la del control del cumplimiento de la pena.

Justamente el proceso penal culmina con el cumplimiento de la pena impuesta en calidad de cosa juzgada, cuyo objetivo es la "re" socialización del individuo condenado.

Alejada de toda posible vinculación con la tecnología, esta etapa del proceso penal sobrevive al fenecido proceso inquisitivo, escrito y prácticamente secreto, pudiéndose modernizar con distintas herramientas ya puestas en vigencia en otras etapas del proceso o en la vida cotidiana y laboral de otros ciudadanos.

Por ejemplo:

- La implementación de sistemas de capacitación a través de videoconferencia, por sistemas específicamente dispuestos para capacitar a nivel de la escolaridad obligatoria o para la adquisición de arte, profesión y oficios. Un simple dispositivo de comunicación con las entidades brindadoras del servicio, y por su puesto la suscripción de los convenios necesarios, se puede capacitar a personas privadas de la libertad, sin correr riesgos de evasión por los sucesivos traslados, sin incrementar costos que insumen tanto los traslados como la contratación de docentes específicos, aprovechando los ya contratados a esos efectos.
- Sistemas de cómputos de pena informáticos, a los efectos de facilitar la tarea de los operadores y despejar dudas de las partes.
- La implementación de una biblioteca digital, con acceso mediante aparatos informáticos que contengan restricciones de accesibilidad a otras páginas *web* o redes sociales. Tomo como ejemplo el caso de Noruega, que digitalizó recientemente sus libros, con acceso gratuito a todo el mundo, creando así la biblioteca virtual mundial.
- La creación de la historia clínica digital de condenado, para que tengan acceso los médicos de los distintos nosocomios en los que son atendidos como los operadores que lo requieran, a los efectos de proveer de tratamientos privados o estatales más efectivos y eficaces en el menor

tiempo posible o realizar diagnósticos forenses en relación a los padecimientos psíquicos y físicos de los detenidos, garantizando el derecho a la salud.

k) Del control de medidas de protección de personas y de coerción personal morigeradas a través de sistemas de georreferenciación satelitales.

Es conocido por todos en el mundo, que muchas de las aplicaciones o también llamadas *apps* descargadas en nuestros equipos de comunicaciones móviles, tienen incorporado un GPS satelital que muestra nuestra localización si la misma no es negada por el usuario.

Fácilmente podría implementarse este sistema de geolocalización utilizando plataformas existentes como *google maps* o creando las necesarias, obligando al destinatario del seguimiento a llevar consigo por ejemplo un celular, un reloj inteligente modificado, o cualquier otro dispositivo extraíble o no del cuerpo humano y controlado a través de éste sistema por la víctima, las autoridades policiales y judiciales.

Su implementación no exigiría la inversión de grandes sumas de dinero, y propendería a un mecanismo de control más efectivo sin insumir gran cantidad de personal, automático, remoto, instantáneo y por ende de mayor eficacia, disminuyendo quizás el número de personas privadas de la liberad en cumplimiento de medidas cautelares en lugares comunes de detención, suplantando quizás otros dispositivos más costosos.

En la actualidad, al menos en Argentina, sólo contamos con la utilización del dispositivo llamado "pulsera electrónica" a la que muchas veces no se puede acceder por su falta, generando que no pueda aprovecharse de su utilidad.

V. A modo de conclusión

Cuando un hombre se encuentra vinculado con un proceso judicial, tiene un conflicto que seguramente pone en juego algunos de los derechos que debe garantizar el Estado.

En el proceso por resolver ese conflicto, busca una respuesta óptima en el tiempo más corto posible.

Por ello, el proceso judicial, entendido como el trámite necesario para resolver ese conflicto, debe ser rápido, expedito, sencillo, claro, publico, oral, económico, siendo éste el desafío principal que deben enfrentar los Estados, cuando diseñan o modernizan sus procesos o prácticas judiciales.

Deben estipularse los objetivos, unificarse esfuerzos para detectar obstáculos en el cumplimiento de éstos, maximizando la utilización de los recursos, procurando que la modernización no sea una utopía.

La inversión mayor es no salir del modelo tradicional.

La idea es la utilización de la tecnología en todos los procesos judiciales repercuta en el medio ambiente, como derecho principal del hombre y reduciendo el impacto que genera la utilización del papel o el desecho de equipos informáticos en desuso.

Normativizar aspectos centrales de la aplicación de la tecnología en los procesos judiciales, favoreciendo y fomentando su utilización.

Resulta un imperativo adaptar la justicia a la sociedad de la información, buscando extender los múltiples beneficios de ello a todas las etapas del proceso judicial, sin distinción, y a todas las facetas de la vida del hombre, pensando en garantizar los derechos de éste y con ello afianzar el servicio de justicia.

La firma electrónica como mecanismo de agilización en los procesos de extradición venezolano, respecto a la participación del Ministerio Público

Vladimir José Lezama Bárcenas*

SUMARIO: Introducción. 1. Nociones generales del proceso de extradición en Venezuela. 2. Proceso de implementación de la firma electrónica en el procedimiento de extradición en Venezuela. 3. El proceso de aplicabilidad de la firma electrónica en la transmisión de información relativa al procedimiento de extradición en Venezuela. 4. El proceso de aplicabilidad de la firma electrónica en la transmisión de información relativa al procedimiento de extradición en Venezuela. Conclusión.

Resumen

En la presente investigación se analizará la viabilidad de la implementación de la firma electrónica como mecanismo de agilización en los procesos de extradición, haciéndose especial énfasis en: 1) describir las nociones generales del procedimiento de extradición en Venezuela; 2) determinar el proceso de implementación de la firma electrónica en el procedimiento de extradición venezolano y; 3) identificar el proceso de aplicabilidad de la firma electrónica en el envío de información relativa al procedimiento de extradición en Venezuela.

Palabras clave: Extradición. Firma electrónica. Agilización de procesos.

Recibido: 21/11/2019 • Aceptado: 18/12/2019

* Abogado, egresado de la Universidad Santa María, Especialista en Derecho Penal por la Universidad Santa María, Especialista en Derecho Administrativo por la Universidad José María Vargas, Especialista en Derecho Penal Internacional por la Universidad Latinoamericana y del Caribe, Especialista en Ejercicio de la Función Fiscal por la Escuela Nacional de Fiscales del Ministerio Público, cursando actualmente el Doctorado en Derecho en la Universidad Católica Santa Rosa. Se desempeña como Fiscal Tercero del Ministerio Público para actuar ante la Sala Plena, Constitucional y Salas de Casación del Tribunal Supremo de Justicia.

Abstract

In this research, the viability of the implementation of the electronic signature as a mechanism for speeding up extradition processes, will be analyzed, with special emphasis on: 1) describe the general notions of the extradition procedure in Venezuela; 2) determine the process of implementing the electronic signature in the Venezuelan extradition procedure and; 3) identify the process of applicability of the electronic signature in the sending of information related to the extradition procedure in Venezuela.

Keywords: Extradition. Electronic Signature. Streamlining process.

Introducción

El tema a ser desarrollado se encuentra enmarcado en una investigación innovadora, en el sentido de que el procedimiento venezolano de extradición (activa y pasiva) podría reducirse en lo que respecta a su duración, debido a que cuando un Estado hace la solicitud a otro, mediante la vía diplomática, lo hace a través de documentación que debe ser consignada en papel, lo cual representa pérdida de tiempo en el ir y venir de la correspondencia a través de las valijas.

Otro inconveniente que se presenta en el procedimiento de extradición, es la lentitud en la circulación de la información entre los órganos que intervienen en el ámbito interno (Poder Judicial y Ministerio Público, entre otros); resultando palpable, que con la implementación de la firma electrónica, se podría diluir el nudo en el flujo de la información. Si bien es cierto que internacionalmente la extradición ha resultado ser una herramienta de utilidad para que personas investigadas con requisitorias de los tribunales de justicia de un país o condenados por la comisión de algún delito, puedan ser trasladados al país solicitante, previo cumplimiento de los requisitos y formalidades para ser enjuiciados o para que cumplan sus penas, no es menos cierto, que el proceso resulta lento, por la dificultad de transmisión de la información.

En la presente investigación, se sentarán las bases normativas y procedimentales, para el establecimiento de una propuesta viable respecto a la firma electrónica como vía idónea para dotar de autenticidad el envío a través de los medios de mensajería electrónica, de la documentación oficial en los procedimientos de extradición, acortando los tiempos de respuesta, lo que redundaría en beneficio tanto para el justiciable como para la administración de justicia, que no tendrían que esperar tanto tiempo por el pronunciamiento del Tribunal Supremo de Justicia. Resulta necesario hacer una adecuación a la manera como es llevado el procedimiento de extradición, de acuerdo con las disposiciones referidas al documento y la firma electrónica, establecidas en el

Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas (LMDFE)[1].

1. Nociones generales del proceso de extradición en Venezuela

A continuación se procederá a establecer una serie de fundamentos que permitirán conocer la esencia de la extradición, para ir orientando la investigación a las especificidades de su proceso en la República Bolivariana de Venezuela, con la finalidad de poder determinar, en qué partes de su procedimiento puede ser utilizada la firma electrónica, como mecanismo de agilización procesal.

A tales efectos, resulta pertinente antes de entrar en la materia, debido a que con mucha frecuencia serán utilizados, hacer la distinción entre los vocablos "proceso" y "procedimiento" para lo cual se trae a colación lo señalado por Amoni Reverón (2012)[2], que define al primero citando a Ortíz, como la "*relación jurídica que se produce por la acción de los particulares y la jurisdicción del Estado para la tutela de intereses jurídicos*", y al segundo citando a Montero, que lo define como "…*el conjunto de forma solemnes reguladas por la ley, por medio de las cuales actúan los tribunales*".

1.1. Definición de extradición

Para Acosta[3] la extradición es una institución jurídica de Derecho Procesal e Internacional Público, mediante la cual los Estados, en ejecución de las potestades que legalmente le permiten sus relaciones, solicitan o entregan personas para que sean procesadas penalmente o para que cumplan una pena impuesta, previo el cumplimiento del procedimiento pautado en el tratado correspondiente o fundamentado en la reciprocidad internacional, como principio que les permite concederse mutuamente peticiones a las cuales no estarían legalmente obligados, con el compromiso de que el otro Estado también se obligue.

De acuerdo con el concepto que antecede, se puede inferir que la extradición es un procedimiento utilizado por el Derecho Internacional Público, que tiene como objeto que los hechos delictivos realizados por una persona en cualquier país no queden impunes al radicarse esta en otra nación, por ello los países suscribieron convenios y tratados internacionales en materia de extradición, que permiten solicitar al individuo para su juzgamiento en el lugar donde cometió

1 Publicada en la Gaceta Oficial Nº 37.313 del 30 de octubre de 2001.

2 Gustavo AMONI-REVERÓN: "De los procedimientos judiciales orales a los electrónicos. La e-justicia". *Libro-Fodertics Estudios sobre Derecho y Nuevas Tecnologías*. Santiago de Compostela-España. 2012, Pp. 29.

3 Victor ACOSTA: "Notificación o difusión roja internacional y derecho a la libertad en Venezuela". Trabajo Especial de Grado para optar al Título de Especialista en Ejercicio de la Función Fiscal. Escuela Nacional de Fiscales. Caracas-Venezuela, 2005.

el hecho punible, aunque puede darse el caso de que, aun cuando no se haya suscrito un convenio o tratado, proceda la extradición en respeto al principio de reciprocidad[4].

1.2. Naturaleza jurídica y fuente de la extradición

En cuanto a la naturaleza jurídica del procedimiento de extradición se puede decir que existen dos vertientes de análisis, en primer lugar la doctrinal, apoyada por Rengifo (2005)[5] que expresa que en la extradición es "*un requisito sine qua non, que se proceda, de conformidad con los trámites establecidos, a tal efecto, por los Tratados Internacionales, suscritos por Venezuela, y que se encuentran vigentes; a falta de estos, por lo establecido en las leyes venezolanas*"; y en segundo lugar la legal, que corresponde a lo señalado en el Código Orgánico Procesal Penal (2012) en los artículos 6, 382, 383, 385 y 386 que establecen que el procedimiento de extradición se rige por lo previsto en la Constitución de la República Bolivariana de Venezuela, los Tratados, los Convenios y Acuerdos Internacionales suscritos y ratificados por la República. Por su parte Monroy[6], en relación al mismo punto señala que no existe un acuerdo respecto a la doctrina, debido a que algunos doctrinantes consideran que la extradición es un acto de asistencia y cooperación judicial internacional, otros que se trata del cumplimiento de la reciprocidad jurídica y los que admiten la extradición únicamente por razones meramente utilitarias, es decir, por conveniencia de los Estados requerido y requirente.

Desde esta perspectiva se debe manifestar que la génesis o fuente del procedimiento de extradición según Arteaga[7] se encuentra en lo fundamentado por el legislador en la "*Constitución de la República Bolivariana de Venezuela, el Código Penal, el Código Orgánico Procesal Penal y en los dispositivos de los Tratados de Extradición suscritos por Venezuela con otros Estados; y por los principios de Derecho Internacional, específicamente por la Costumbre Internacional y la reciprocidad*"[8].

4 Sala de Casación Penal del Tribunal Supremo de Justicia, Sentencia N° 501, del 6 de diciembre de 2016.

5 RENGIFO, R. (2005). *Naturaleza jurídica de la extradición en Venezuela*. Editorial Livrosca. Caracas, Venezuela.

6 MONROY, M. (1987). *Régimen jurídico de la extradición*. Editorial Temis, S.A. Bogotá, Venezuela.

7 ARTEAGA, A. (2008). *La extradición en Venezuela*. Academia de Ciencias Políticas y Sociales. Editorial Torino, C.A. Caracas, Venezuela.

8 Al respecto Amoni, Gustavo "En materia de extradición, 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.

1.3. Clasificación de la extradición

Resulta necesario destacar la clasificación dada al procedimiento de extradición, siendo la más sencilla y adaptada a la realidad normativa venezolana, la esgrimida por Vásquez[9], que la divide en: "*activa y pasiva, según se la analice desde el ángulo del Estado requirente o requerido* (…) *el Estado que solicita la entrega funge como requirente y plantea la extradición activa, mientras que el Estado que recibe la solicitud de entrega es el requerido y respecto de su posición se trata de una extradición pasiva*".

Es de hacer notar, que a criterio de quien suscribe, la clasificación de la extradición que antecede, es la de mayor aceptación, es decir, activa y pasiva, en vista de que tanto la normativa interna e internacional, así como la Sala de Casación Penal del Tribunal Supremo de Justicia, la citan de esa manera[10].

1.4. El proceso de extradición en Venezuela

Uno de los aspectos más importantes en el desarrollo de la presente investigación es determinar de manera clara y concisa cuál es el procedimiento que se debe seguir en la extradición y cuáles son las instituciones u órganos que intervienen en él, para lo cual se observa que en el caso de la extradición activa, Vásquez[11] indica, que "*en el caso venezolano el procedimiento se inicia con la solicitud del Juez en funciones de Control a la Sala de Casación Penal del Tribunal Supremo de Justicia, previa instancia del Ministerio*

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". Derecho y Tecnología 2016. Disponible en: http://www.ucat.edu.ve/web/investigacion-y-postgrado/publicaciones/revistas/ [Consultado: 2019, septiembre, 20]

9 VÁSQUEZ, M. (2016). *Procedimientos penales especiales*. Universidad Católica Andrés Bello (UCAB). Caracas, Venezuela.

10 Sobre el tema el Dr. Gustavo A. Amoni Reverón, se ha pronunciado en sus obras que se mencionan a continuación: "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* (N° 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* (N° 12), julio-diciembre, Colombia: Universidad de Los Andes, 2014.

11 VÁSQUEZ, M (2015). *Derecho Procesal Penal Venezolano*. Universidad Católica Andrés Bello (UCAB). Caracas, Venezuela.

Público", afirmando además que "la fiscalía debe opinar en los procesos de extradición ventilados ante el TSJ".

De este modo, visto lo anterior se evidencia que el Ministerio Público tiene un rol protagónico debido a que está llamado a impulsar el proceso, en el caso de la extradición activa, cuando tiene conocimiento de que alguna persona sobre la cual pesa una orden de aprehensión librada por parte de un tribunal de control de la República Bolivariana de Venezuela, se encuentra en territorio extranjero, y en el caso de la extradición pasiva, también funge como impulsor del proceso, porque cuando le es informada la detención de una persona sobre la cual pesa una Alerta Roja de Interpol, de un país extranjero, hace el trámite de presentación ante un juez de control, y en ambos casos, tiene la obligación de presentar su opinión ante la Sala de Casación Penal del Tribunal Supremo de Justicia, la cual no resulta vinculante al momento que esta decide acerca de la procedencia o no de la pretensión de extradición.

Por otra parte, se debe mencionar que cuando la persona solicitada en extradición se encuentre sometida a juicio oral se fuga a otro país, el trámite de extradición activa ante la Sala de Casación Penal debe ser realizado por el juez de juicio que lleva la causa; mientras que si se fuga durante el período de cumplimiento de la condena, el proceso de extradición debe ser iniciado a instancia del juez de ejecución.

Desde esta perspectiva, resulta importante señalar que en el caso de la extradición activa, la Sala de Casación Penal del Tribunal Supremo de Justicia tiene un plazo de treinta días contados a partir del momento en que recibe la documentación (esto va a depender del lapso establecido en cada convenio internacional), indicando si es procedente o no la pretensión de extradición, ello con la previa, necesaria y obligatoria opinión fiscal del Ministerio Público.

En ese mismo orden de ideas, se trae como precedente la sentencia N° 1072, de fecha 08 de diciembre de 2017, dictada por la Sala Constitucional, en el expediente Nº 2017-1141, bajo ponencia del Magistrado Doctor Arcadio Delgado Rosas, a través de la cual declaró con lugar, la solicitud de revisión constitucional presentada por los apoderados judiciales del ciudadano Fernando Agustín Ramírez Quijada, en contra de la sentencia Nº 324 dictada el 4 de septiembre de 2017 por la Sala de Casación Penal del Tribunal Supremo de Justicia, a través de la cual se declaró procedente la solicitud de extradición activa del referido ciudadano; anuló la referida sentencia y ordenó a la Sala de Casación Penal del Tribunal Supremo de Justicia, dictar nueva decisión.

La referida sentencia, entre otros particulares determinó que la Sala de Casación Penal, a pesar de haber librado oficio al Fiscal General de la República, informándole del procedimiento de extradición activa y requiriéndole su opinión, resolvió dictar sentencia sin contar con la opinión requerida en el artículo 383 del Código Orgánico Procesal Penal, razón por la cual se acordó anular la sentencia N° 324, de fecha 4 de septiembre de 2017, ordenando que la Sala de

Casación Penal dicte nueva decisión, en aras de garantizar el debido proceso y la seguridad jurídica en los procesos.

El criterio esgrimido por la Sala Constitucional, indica acertadamente que no es posible que la Sala de Casación Penal, dicte su veredicto en el marco de un procedimiento de extradición activa, sin que medie en actas previamente, la necesaria opinión fiscal.

Se debe resaltar, que otro órgano que interviene en el procedimiento de extradición activa, es el Ministerio del Poder Popular para Relaciones Exteriores a través de su Oficina de Relaciones Consulares que se encarga de la tramitación con la representación diplomática de otros países, teniendo la obligación de traducir los documentos que sean necesarios con la consecuente certificación, a los efectos de consignar los mismos en un plazo no mayor de sesenta días, lo cual se encuentra consagrado en el artículo 384 del Código Orgánico Procesal Penal (2012)[12].

Ahora bien, en lo que respecta al procedimiento de extradición pasiva Vásquez[13], señala que este: "se inicia, conforme al COPP, con la solicitud que el gobierno extranjero presenta al Poder Ejecutivo, solicitud que este debe remitir al Tribunal Supremo de Justicia con la documentación recibida" (p. 199).

Se plantea entonces, que la extradición pasiva en Venezuela permite que la Sala de Casación Penal del Tribunal Supremo de Justicia, determine la viabilidad o no de la entrega, quedando así en manos del Poder Judicial la decisión final acerca de la procedencia o no de dicho procedimiento.

En ese mismo orden de ideas, resulta importante resaltar que de conformidad con lo previsto en el artículo 387 del Código Orgánico Procesal Penal[14], una vez verificada la aprehensión del solicitado en extradición por parte del Ministerio Público, dicho ciudadano debe ser llevado en un plazo no mayor de cuarenta y ocho horas (48), ante la presencia del juez de control que ordenó su detención, con el objeto de que sea impuesto de los motivos de su detención, en pro de salvaguardar el derecho a la defensa y debido proceso, siendo el caso que por tratarse de una detención con fines de extradición, en la audiencia no puede otorgarse ninguna medida cautelar sustitutiva.

Otro factor importante que se debe resaltar es, que en caso de que venza el lapso establecido sin que la documentación ofrecida sea consignada en la Sala de Casación Penal del Tribunal Supremo de Justicia, estando ésta en la obligación de ordenar la libertad del solicitado en extradición, en el entendido de que si con posterioridad se entrega dicha documentación, puede acordarse nuevamente la privación de libertad, con miras a la prosecución del proceso.

12 Publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 6.078 Extraordinario, de fecha 15 de junio de 2012.

13 VÁSQUEZ, M. (2016). *Procedimientos penales especiales*. Universidad Católica Andrés Bello (UCAB). Caracas, Venezuela.

14 Publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 6.078 Extraordinario, de fecha 15 de junio de 2012.

En cuanto a la decisión que debe tomar la Sala de Casación Penal del Tribunal Supremo de Justicia, una vez consignada la documentación que la sustenta, este órgano debe convocar a una audiencia dentro de los treinta días siguientes a la notificación del solicitado, quién debe concurrir a la misma con su defensor, siendo convocados también el Ministerio Público, con la finalidad de que dé su opinión, el abogado del gobierno extranjero en caso de haber sido designado, quienes expondrán sus alegatos, para que el órgano jurisdiccional dicte su sentencia en un lapso de quince días después de concluida la audiencia.

Cabe destacar, que existe la posibilidad de realizar la audiencia con la participación de personas a través de videoconferencia, a partir del 12 diciembre de 2016, a raíz de la Resolución N° 2016-001 SOBRE PARTICIPACIÓN TELEMÁTICA DE LOS SUJETOS PROCESALES EN LAS AUDIENCIAS DE LA SALA DE CASACIÓN PENAL[15], que estableció en su artículo 1, entre otros particulares, que 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, por telepresencia, videoconferencia u otro medio de comunicación telemático, audiovisual, bi o multidireccional e instantáneo, lo cual constituye un extraordinario apoyo para evitar las incomparecencias.

Los procedimientos tanto de extradición activa como el de extradición pasiva antes explanados, se constituyen en una importante herramienta que debe ser observada por todos los factores que intervienen en el proceso, para lo cual en el transcurso de la presente investigación se procederá a identificar en qué momento procesal puede ser implementada la firma electrónica como mecanismo de agilización.

2. Implementación de la firma electrónica en el proceso de extradición en Venezuela

El desarrollo de la tecnología ha tenido un aporte importante en la sociedad, lo que ha generado que se incluyan mecanismos valiosos para agilizar cualquier tipo de trámites administrativos y legales en cualquier país del mundo, como por ejemplo la implementación de la firma electrónica.

En ese sentido, Parra[16] afirma que:

> Todos los humanos nos habíamos acostumbrados a confundir documentos con papel, pero desde hace algún tiempo, se logró que las personas se acostumbraran a entender que un video, un disco también eran documentos, esto amplio la mente para aceptar que puede hablarse de documentos, cuando esta contenido en soporte informático. Esto último no desdice de lo que se ha entendido hasta

15 http://zdenkoseligo.blogspot.com/2016/12/resolucion-no-2016-001-del-lunes-12.html

16 PARRA, J: *Manual de Derecho Probatorio*. 14 edición. Colombia. Librerías, Ediciones del Profesional LTDA, 2004, p. 560.

> ahora por documento, que será toda cosa capaz de representar un hecho cualquiera o una manifestación del pensamiento, donde la cosa es el soporte electrónico.

Desde esta perspectiva, se procede a explanar teóricamente en este aparte de la investigación la importancia que tiene la implementación de la firma electrónica en el procedimiento de extradición en Venezuela.

Por tal motivo, se debe mencionar que el Decreto con fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas[17] regula los mensajes de datos, la firma electrónica y toda información que tenga como soporte los sistemas informáticos, la cual viene a dar soporte jurídico al comercio electrónico y a la generación de documentos electrónicos, resultando del análisis de dicha normativa, a criterio de quien suscribe, una evidencia de la eficacia que pueden tener las firmas electrónicas en el proceso de extradición, siempre y cuando se siga el debido procedimiento para su certificación y uso.

Al respecto, la exposición de motivos de dicha ley, establece la creación de mecanismos para que la firma electrónica, en adelante, tenga la misma validez y valor probatorio de la firma escrita, siempre y cuando cumpla con los requisitos mínimos establecidos en el Decreto-Ley.

En ese sentido, resulta conveniente destacar la definición de la firma electrónica dada por la norma patria[18] en materia de firmas electrónicas, que la presenta como la: "*Información creada o utilizada por el Signatario, asociada al Mensaje de Datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado…*".

Asimismo, resulta interesante la definición de firma electrónica ofrecida en la página web de la empresa privada PROCERT, C.A.[19], en la que indica que:

> Es un esquema matemático que sirve para demostrar la autenticidad de un mensaje digital o de un documento electrónico. La firma digital le brinda al destinatario la seguridad que el mensaje fue creado por el remitente, y que no fue alterado durante la transmisión, si se realiza con un certificado emitido por el PSC Procert, le brinda al documento la misma validez legal que una firma manuscrita.

Por su parte, la propia ley establece en su artículo 22 una serie de requisitos para que la firma electrónica tenga validez jurídica y eficacia probatoria. Asimismo, la norma ordena la creación de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), la cual tiene por objeto "*…acreditar, supervisar y controlar, en los términos previstos en este Decreto-Ley y sus reglamentos, a los Proveedores de Servicios de Certificación públicos o privados…*"

17 Publicada en la Gaceta Oficial Nº 37.313 del 30 de octubre de 2001.
18 Publicada en la Gaceta Oficial N° 37.313 del 30 de octubre de 2001.
19 http://zdenkoseligo.blogspot.com/2016/12/resolucion-no-2016-001-del-lunes-12.html

Ahora bien, de acuerdo con lo propuesto por la ley, el órgano encargado del trámite de la certificación de la firma electrónica es la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), quien se encargará de verificar que los proveedores de servicios de certificación (PSC) cumplan con todos los requisitos exigidos para darle plena validez a las firmas electrónicas que ellos respalden, así las cosas, si algún PSC quiere inscribirse ante la SUCERTE para recibir su acreditación, debe cumplir con lo pautado en el artículo 31 de la Ley sobre Mensajes de Datos y Firmas Electrónicas.

Resulta imperante resaltar lo establecido por el Decreto con fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas[20], en su artículo 16, en lo que respecta a las firmas electrónicas, que señala 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*".

De esta manera se evidencia con lo contemplado en la Ley que la firma electrónica será completamente válida y se considerará como una firma realizada en papel, siendo tácita la responsabilidad adquirida al autorizar su firma electrónica en cualquier trámite.

De acuerdo con lo antes expuesto, se debe entender que incluir la firma electrónica en los procedimientos de extradición venezolanos, previo cumplimiento de los requisitos establecidos en la normativa especial relacionada a este tema, debe estar certificada de acuerdo a lo establecido en el artículo 18 de la Ley, que establece que "*La Firma Electrónica, debidamente certificada por un Proveedor de Servicios de Certificación conforme a lo establecido en este Decreto-Ley, se considerará que cumple con los requisitos señalados en el artículo 16…*".

Ahora bien, para que una persona pueda ser titular de una firma electrónica y tenga validez y eficacia conforme a la ley, debe acudir a un Proveedor de Servicios de Certificación debidamente inscrito ante la Superintendencia de Servicios de Certificación Electrónica. Estos proveedores de Servicios de Certificación están definidos en el artículo 2 donde se indica: "*…Proveedor de Servicios de Certificación: Persona dedicada a proporcionar Certificados Electrónicos y demás actividades previstas en este Decreto-Ley…*".

En este sentido, el 26 de mayo del año 2010, la providencia Nº 004-10 emanada de Superintendencia de Certificación Electrónica (SUSCERTE)[21], que contempla en su artículo 2, lo siguiente:

> A los fines de garantizar el cumplimiento de lo establecido en los artículos 1, 4, 5, 7 y 8, de la ley sobre mensajes de datos y firmas electrónicas se hace imperante que toda firma electrónica, mensaje de datos e información inteligible en formato

20 Publicada en la Gaceta Oficial Nº 37.313 del 30 de octubre de 2001.
21 Publicada en la Gaceta Oficial N° 39.432 del 26 de mayo de 2010.

> electrónico emitidos en Portales y Sistemas de Información de Instituciones Públicas o Privadas, que ameriten eficacia, valor jurídico, protección de la integridad de la información y garantizar su autoría, deberán estar en la cadena de confianza de certificación electrónica, avalada por un Proveedor de Servicios de Certificación debidamente acreditado ante esta Superintendencia.
> En virtud de lo expuesto, los mensajes de datos, correos electrónicos y demás transacciones de semejante naturaleza, para los cuales se requiera que cumplan o generen consecuencias jurídicas para las instituciones y usuarios, sean éstos públicos o privados, deberán obligatoriamente someterse a lo establecido por dicha providencia. Esta exige el uso de firmas electrónicas en el caso de usuarios y representantes de empresas públicas o privadas, así como también, la certificación electrónica de procesos o transacciones en el caso de empresas o entidades públicas y/o privadas.
>
> De esta manera, se demuestra claramente la obligatoriedad de la existencia de los sistemas de certificación electrónica y dada la importancia que tiene este instrumento tecnológico en los trámites de cualquier proceso legal en el ordenamiento jurídico venezolano, el 14 de diciembre de 2004 se publicó el Reglamento Parcial de la Ley sobre Mensaje de Datos y Firmas Electrónicas[22], cuyo artículo 1 establece su objeto:
>
> Desarrollar la normativa que regula la acreditación de los Proveedores de Servicios de Certificación ante la Superintendencia de Servicios de Certificación Electrónica, la creación del Registro de Auditores, así como los estándares, planes y procedimientos de seguridad, de conformidad con el Decreto Ley.

En la actualidad en Venezuela están acreditados dos entes, uno de naturaleza pública y el otro privado, el primero de ellos es la Fundación Instituto de Ingeniería (FII), que es un ente adscrito al Ministerio del Poder Popular para Educación Universitaria, Ciencia y Tecnología, creado en 1980 a través del Decreto Nº 733 de la Presidencia de la República de Venezuela y tiene como misión desarrollar actividades y proyectos de investigación, desarrollo tecnológico, innovación, servicios, asistencia técnica y asesorías, con eficiencia y óptima calidad en las áreas de la ingeniería, la geomática, la certificación electrónica y otras áreas afines del conocimiento.

Esta información fue necesaria colocarla en este aparte del artículo científico en virtud que sirva como una guía de cuáles serán los pasos para implementar la firma electrónica en el proceso de extradición venezolano por parte del Ministerio Público.

En relación a lo antes expuesto, Amoni G.[23] es de la opinión que la Ley de Interoperabilidad autoriza a los órganos y entes del Estado a sustanciar sus

22 Publicada en la Gaceta Oficial N° 38.086 del 14 de diciembre de 2004

23 Gustavo AMONI-REVERÓN: "El Procedimiento administrativo a partir de la Ley de interoperabilidad y la Ley de Infogobierno". *Revista Venezolana de Legislación y Jurisprudencia*, N° 7. 2016, Pp. 432.

actuaciones administrativas, total o parcialmente, por medios electrónicos, y la Ley de Infogobierno impone al Poder Público el uso de tecnologías de información para relacionarse con los particulares, quienes podrán presentar solicitudes, pagos, recibir notificaciones, acceder a la información pública y al expediente que se esté tramitando, presentar documentos y pedir copias, todo mediante el uso de tecnologías de información y con igual valor que los mismos actos realizados de forma tradicional, están reiterando la validez del procedimiento del artículo 1 de la Ley sobre mensajes de Datos y Firmas Electrónicas.

En ese sentido, el antes referido artículo señala que el Decreto Ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la firma electrónica, al mensaje de datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los proveedores de servicios de certificación y los servicios electrónicos.

Continúa señalando Amoni G., citando y analizando a Monsalve, que esta disposición engloba casi todas las categorías de sujetos de derecho y que a partir de ella, si toda persona natural o jurídica, inclusive pública, podía usar firmas electrónicas y mensajes de datos, con validez en el mundo del Derecho, entonces los funcionarios podían utilizar tales herramientas tecnológicas para el cumplimiento de las competencias que el ordenamiento jurídico le atribuye al órgano o ente en virtud del cual actúan.

En vista de lo anterior, se puede concluir que efectivamente existe un entramado de normas legales y fundamentos doctrinales que avalan el establecimiento de la firma electrónica en los procedimientos donde participen órganos del Estado, lo cual no resulta ajeno al proceso de extradición.

3. El proceso de aplicabilidad de la firma electrónica en la transmisión de información relativa al procedimiento de extradición en Venezuela

A los fines de hablar de aplicabilidad de la firma electrónica como herramienta de uso regular en el procedimiento de extradición, resulta pertinente traer a colación la sentencia de la Sala Constitucional del Tribunal Supremo de Justicia N° 656, de fecha 30 de junio de 2000, mencionada por Amoni Reverón[24] donde se estableció la necesidad de adaptar el ordenamiento jurídico a las nuevas realidades sociales como consecuencia de la cláusula del Estado social de derecho y de justicia prevista en el artículo 2 de la Constitución de la República Bolivariana de Venezuela, lo cual significa:

24 AMONI, Gustavo. "El uso de la videoconferencia en cumplimiento del principio de inmediación procesal". *Revista del Instituto de Ciencias Jurídicas de Puebla*, Mexico, ISSN: 1870-2147. Año VII No. 31, Enero-Junio de 2013, PP. 67-85. https://revistaius.com/index.php/ius/article/view/21/478

> Que dentro del derecho positivo actual y en el derecho que se proyecte hacia el Futuro, la ley debe adaptarse a la situación que el desarrollo de la sociedad vaya creando, como resultado de las influencias provenientes del Estado o externas a él [...] El Estado constituido hacia ese fin, es un Estado social de derecho y de justicia, cuya meta no es primordialmente el engrandecimiento del Estado, sino el de la sociedad que lo conforma, con quien interactúa en la búsqueda de tal fin.

Tal aseveración establece el andamiaje jurídico para que el Estado venezolano dote a la justicia de herramientas de vanguardia que le permitan ser más expeditos en el sentido de dar respuesta oportuna a los justiciables y ciudadanía en general, siendo el establecimiento de la firma electrónica, uno de los grandes logros alcanzados, resultando de vital importancia su proliferación masiva.

Es el caso que la extradición no es una excepción de esa necesidad de obtención de un procedimiento fluido que permita acortar los tiempos de espera, en el entendido que durante el proceso, la persona se encuentra privada de libertad, con todas las implicaciones que esto trae.

Ahora bien, con el objeto de avanzar en la consecución del presente artículo científico se hará énfasis en la figura del Fiscal General de la República como máxima autoridad del Ministerio Público, sobre quien recae la responsabilidad de suscribir y consignar el escrito de opinión fiscal en los procedimientos de extradición en la República Bolivariana de Venezuela.

Es de hacer notar, que la antes referida atribución le fue concedida según lo establecido en el artículo 25 numeral 15 de la Ley Orgánica del Ministerio Público[25] y en el numeral 16 del artículo 111 del Código Orgánico Procesal Penal[26], en concordancia con el primer aparte del artículo 383 del texto adjetivo[27].

A los fines de establecer de una manera expedita cuáles podrían ser los aportes en el mejoramiento del proceso de extradición con la aplicación de la firma electrónica se tomó como parámetro de estudio la intervención en el proceso del Ministerio Público, bajo la dirección y responsabilidad del Fiscal General de la República, en razón que de esto depende directamente el compromiso de actuar en la consignación del informe fiscal ante la Sala de Casación Penal del Tribunal Supremo de Justicia y que dicho funcionario de conformidad con lo previsto en el artículo 284 de la Constitución de la República Bolivariana de Venezuela, será designado para un período de siete (7) años, lo cual representa un indicativo de su permanencia en sus funciones durante un largo tiempo y la firma electrónica en caso de implementarse no requerirá de una constante renovación por el cambio de este.

En razón de cómo debe ser el proceso de aplicabilidad de la firma electrónica en la transmisión de información relativa al procedimiento de extradición en Venezuela, específicamente en lo atinente al escrito de opinión fiscal que debe

25 Publicada en Gaceta Oficial N°38.647 del 19 de marzo de 2007.
26 Publicada en Gaceta Oficial N° 9.042 del 12 de junio de 2012.
27 Publicada en Gaceta Oficial N° 5.908 del 19 de febrero de 2009.

consignar el Fiscal General de la República ante la Sala de Casación Penal del Tribunal Supremo de Justicia en el caso de la extradición procede lo siguiente:

En primer lugar en el caso de la extradición pasiva, el procedimiento se inicia cuando el Ministerio Público solicita al órgano jurisdiccional competente, bien sea el caso al juez de control cuando se tenga noticias de que un imputado en contra del cual se ha acordado una medida cautelar de privación de libertad se encuentra en el extranjero; cuando el acusado en situación de fuga se encuentre en el extranjero se solicitara ante el Juez de Juicio.

Una vez acordada la detención del imputado por parte del órgano jurisdiccional competente, éste remitirá las actuaciones a la Sala de Casación Penal del Tribunal Supremo de Justicia ante quien el Ministerio Público, por órgano del Fiscal General de la República, consignará la opinión fiscal contentiva de los argumentos que considere pertinentes para solicitar la pertinencia o no del procedimiento.

Con posterioridad, la Sala de Casación Penal del Tribunal Supremo de Justicia emitirá su pronunciamiento donde podrá declarar procedente o no la solicitud de extradición activa donde en caso de ser afirmativo deberá remitir copia de lo actuado al Ejecutivo Nacional a los fines de continuar con el procedimiento y hacer el pedimento respectivo a través del Ministerio de Relaciones Exteriores al Estado requerido, siendo que en caso de resultar improcedente la extradición activa se acuerda la inmediata libertad del solicitado en extradición.

Cabe destacar que el procedimiento para la elaboración del escrito de opinión fiscal que consigna el ciudadano Fiscal General de la República, en ejercicio de la atribución conferida en el artículo 25, numeral 15 de la Ley Orgánica del Ministerio Público y en el numeral 16 del artículo 111 del Código Orgánico Procesal Penal, tiene un procedimiento dentro del Ministerio Público, en virtud que el mismo para su elaboración transita por un largo recorrido interno pasando por la Dirección General de Servicios Jurídicos, Dirección de Asuntos Internacionales, Fiscalía con Competencia ante el Tribunal Supremo de Justicia, Vice Fiscalía y Despacho del Fiscal General de la República, donde finalmente es suscrito dicho escrito.

En lo que respecta al procedimiento para la extradición pasiva, el mismo se inicia a solicitud del país requirente, quien realiza el pedimento al Poder Ejecutivo por órgano del Ministerio del Poder Popular para Relaciones Exteriores, quien a su vez notifica al Ministerio Público con la finalidad que este solicite la orden de aprehensión ante un Tribunal de Control con Competencia en materia penal.

Recibida la solicitud con los recaudos por parte del Ministerio Público, los mismos son remitidos por la Dirección de Servicios Jurídicos a la Dirección de Asuntos Internacionales, indicando que Fiscal de Proceso se encargara del caso y que fiscal ante el Tribunal Supremo de Justicia será comisionado para el trámite.

La Dirección de Asuntos Internacionales se encarga de la verificación de la solicitud, en el sentido que se encuentre acompañada de todos los recaudos necesarios para dar continuidad al trámite; siendo que deberá devolver las

actuaciones conjuntamente con su análisis a la Dirección General de Servicios Jurídicos.

Con posterioridad, la Dirección General de Servicios Jurídicos al recibir nuevamente la solicitud de extradición pasiva, procederá a comisionar un fiscal con competencia ante las Salas de Casación del Tribunal Supremo de Justicia y a un fiscal del proceso, para que conjuntamente intervenga en el procedimiento que se seguirá ante el órgano jurisdicción.

El fiscal de proceso solicitará al juez de control mediante escrito razonado la orden de aprehensión con fines de extradición en contra del requerido, expresando en dicha solicitud las circunstancias que dieron lugar a la petición así como los motivos y fundamentos de hechos y de derecho en los que sustenta la acusación.

Una vez aprehendido el ciudadano requerido en extradición ante del plazo de 48 horas deberá realizarse ante el tribunal de control la respectiva audiencia de presentación, donde será acordada la detención preventiva y posterior remisión de las actuaciones a la Sala de Casación del Tribunal Supremo de Justicia.

La Sala de Casación Penal del Tribunal Supremo de Justicia al recibir los recaudos de la solicitud de extradición pasiva notifica al Ministerio Público, a los fines que emita la opinión correspondiente, la cual solo podrá ser presentada en la audiencia convocada para resolver la extradición.

En el caso de la extradición pasiva, en la actualidad pareciera no revestir mayor importancia el uso de la firma electrónica para la consignación del escrito de opinión fiscal suscrito por el Fiscal General de la República, ante la Sala de Casación Penal del Tribunal Supremo de Justicia, en razón de que el expediente por tener su soporte en papel, el mismo debe ser entregado en papel en el momento de la audiencia convocada por esa Sala.

Tal aseveración hace surgir la reflexión de que mientras el procedimiento sea realizado con soporte en papel, no habría la posibilidad de usar la firma electrónica, lo que lleva a plantear la posibilidad de solicitar la sustitución de dicho procedimiento por uno digital, con la finalidad de obtener ventajas en el ahorro de tiempo, horas hombre, consumibles de oficina y en definitiva la optimización de la administración de justicia, siendo que tal iniciativa de implementación de nuevas tecnologías debe partir de los órganos jurisdiccionales.

Por el contrario, en el caso de la extradición activa, por constituir el escrito de opinión fiscal suscrito por el ciudadano Fiscal General de la República, un elemento fundamental en el proceso para que la Sala de Casación Penal, emita su pronunciamiento sobre la procedencia o no de la entrega del requerido en extradición y siendo que no amerita la realización de una audiencia, el trámite de la remisión del referido escrito bien podría realizarse directamente desde el despacho de la máxima autoridad del Ministerio Público a la Sala de Casación Penal, sin mayores dilaciones y trámites burocráticos que retarden el proceso.

Conclusión

La presente investigación propuesta en esta oportunidad por el autor fue motivada por la interesante figura de la extradición y la posibilidad de implementar herramientas innovadoras desde el punto de vista tecnológico en la agilización del proceso, en especial la firma electrónica como instrumento de vanguardia en el ordenamiento jurídico venezolano.

En el transcurso de la investigación se realizó una serie de planteamientos que ayudaron a definir una clara posición en lo que respecta en primer lugar a los antecedentes históricos y normativos de la extradición en sus dos modalidades, es decir activa y pasiva.

Es el caso que para poder profundizar de manera seria y responsable en un tópico de connotación frecuente en los estrados judiciales por constituir el remedio más eficiente para evitar la impunidad que podría ser generada por la comisión de delitos por parte de delincuentes que se trasladan a otros países para evitar la acción de la justicia.

En segundo lugar, se trató de una manera sucinta cual es el procedimiento a seguir para la obtención, validación y certificación de la firma electrónica, ello con la finalidad de explicar de manera sencilla que es una firma electrónica, para que sirve y cuál es la utilidad que tiene la misma en las relaciones interpersonales, intercomerciales e intergubernamentales, específicamente en el ámbito jurídico, el que nos interesa primordialmente que es su inclusión en un procedimiento que tiene tanta importancia como lo es la extradición.

Asimismo, se pudo concluir que en el caso de la extradición pasiva, si bien es cierto que en la actualidad no resulta relevante el establecimiento de la firma electrónica para la remisión de la opinión fiscal por parte del Fiscal General de la República, por cuanto la misma tiene un momento específico para su consignación en papel, es decir en la audiencia convocada ante la Sala de Casación Penal del Tribunal Supremo de Justicia, por parte del Fiscal con Competencia ante esa Sala, surge la necesidad de sugerir la modificación del proceso que debe tender a la digitalización de sus actuaciones.

Por último, se concluyó con la realización de esta investigación que en la extradición activa, la firma electrónica si constituiría una herramienta de apoyo en la agilización del proceso, por cuanto el escrito de opinión del fiscal suscrito por el ciudadano Fiscal General de la República, podría ser remitido a través de este medio de manera directa desde el despacho de dicho funcionario sin mayores dilaciones y trámites burocráticos que retarden el proceso de consignación del escrito de opinión fiscal a la Sala de Casación Penal del máximo tribunal de la república.

JURISPRUDENCIA

Jurisprudencia sobre uso procesal de las Tecnologías de Información y Comunicación en el Tribunal Supremo de Justicia durante 2019

Gustavo Adolfo Amoni Reverón*

I. Acto administrativo telemático

1. **SSPA**[1] **N° 116 del 6 de marzo**[2]: Validez de acto administrativo enviado por correo electrónico.
2. **SSPA N° 213 del 8 de mayo**[3]: Referencia a acto administrativo notificado por correo electrónico.
3. **SSCS N° 104 del 9 de mayo**[4] **y 424 del 9 de diciembre**[5]: Referencia a Certificado Electrónico Zamorano emitido por el Instituto de Tierras.
4. **SSPA N° 153 del 10 de abril**[6]: Solicitud de recaudos, por correo electrónico, en procedimiento administrativo.
5. **SSPA N° 452 del 11 de julio**[7]: Valor de las copias de mensajes de correo electrónico por el cual se aprueba y luego se niega una solicitud ante la extinta Comisión Nacional de Administración de Divisas (CADIVI).

---

* Abogado «summa cum laude» de la Universidad de Carabobo, especialista «cum laude» en Derecho Administrativo, profesor de pregrado y postgrado en Derecho, Universidad Central de Venezuela.

1 Sentencia de la Sala Político Administrativa del Tribunal Supremo de Justicia.

2 http://historico.tsj.gob.ve/decisiones/spa/marzo/304046-00116-6319-2019-2018-0756.html

3 http://historico.tsj.gob.ve/decisiones/spa/mayo/304779-00213-8519-2019-2019-0020.html

4 http://historico.tsj.gob.ve/decisiones/scs/mayo/304802-0104-9519-2019-18-286.html

5 http://historico.tsj.gob.ve/decisiones/scs/diciembre/308650-0424-91219-2019-16-722.html

6 http://historico.tsj.gob.ve/decisiones/spa/abril/304418-00153-10419-2019-2017-0531.html

7 http://historico.tsj.gob.ve/decisiones/spa/julio/306071-00452-11719-2019-2018-0703.html

6. **SSPA N° 463 del 17 de julio**[8]: Referencia a los certificados electrónicos de registro emitidos por el Servicio Autónomo de Propiedad Intelectual (SAPI).
7. **SJSSPA N° 254 del 22 de mayo**[9]: Referencia al Certificado Electrónico de Registro Nacional de Contratistas**.**
8. **SSPA N° 574 del 2 de octubre**[10]: Acto administrativo electrónico («…proveimiento administrativo, entiéndase, la comunicación electrónica S/N…»).
9. **SSCS N° 464 del 13 de diciembre**[11]: Referencia al Certificado Electrónico de Recepción de declaración por Internet del Impuesto sobre la Renta.

II. Procedimiento administrativo telemático

1. **SSPA N° 15 del 30 de enero**[12]: Procedimiento para las consignaciones arrendaticias. Notificación de consignación y de la solvencia por medios electrónicos.
2. **SSPA N° 159 del 10 de abril**[13]: Deber de enviar cierta información bancaria en formato electrónico a la SUPERINTENDENCIA DE BANCOS Y OTRAS INSTITUCIONES FINANCIERAS (SUDEBAN) hoy SUPERINTENDENCIA DE LAS INSTITUCIONES DEL SECTOR BANCARIO (SUDEBAN).
3. **SSPA N° 338 del 12 de junio**[14] **y 445 del 11 de julio**[15]: Derecho de presentar manualmente el Manifiesto de Carga cuando por causa justificada no pueda hacerse electrónicamente mediante el Sistema Aduanero Automatizado (SIDUNEA).

8 http://historico.tsj.gob.ve/decisiones/spa/julio/306283-00463-17719-2019-2018-0516.html
9 http://historico.tsj.gob.ve/decisiones/spa/mayo/305102-00254-22519-2019-2015-0148.html
10 http://historico.tsj.gob.ve/decisiones/spa/octubre/307327-00574-21019-2019-2018-0560.html
11 http://historico.tsj.gob.ve/decisiones/scs/diciembre/309000-0464-131219-2019-19-235.html
12 http://historico.tsj.gob.ve/decisiones/spa/enero/303457-00015-30119-2019-2018-0729.html
13 http://historico.tsj.gob.ve/decisiones/spa/abril/304384-00159-10419-2019-2018-0092.html
14 http://historico.tsj.gob.ve/decisiones/spa/junio/305462-00338-12619-2019-2018-0611.html
15 http://historico.tsj.gob.ve/decisiones/spa/julio/306064-00445-11719-2019-2019-0011.html

4. **SSPA 339 del 12 de junio**[16]: Notificación telemática de acto administrativo.
5. **SSE**[17] **N° 37 del 20 de junio**[18]: El deber de publicar en un diario de circulación nacional, la convocatoria a la Asamblea de Asociados para la conformación de la Comisión Electoral de una caja de ahorros no puede sustituirse por otros medios, aunque se realizare, además, por correo electrónico.
6. **SSPA N° 498 del 6 de agosto**[19]: Notificación de acto administrativo por correo electrónico y reiteración en papel.
7. **SSPA N° 804 del 11 de diciembre:** Validez del pago manual del impuesto sucesoral aunque solo se prevea su ejecución en formato digital.

III Procedimientos jurisdiccionales electrónicos

1. **SSCS N° 39 del 18 de marzo**[20], **78 del 25 de abril**[21], **80 del 29 de abril**[22], **231 del 18 de julio**[23], **343 del 14 de agosto**[24], **359 del 4 de octubre**[25], **398 del 5 de noviembre**[26], **406 del 19 de noviembre**[27] **y 449 del 13 de diciembre**[28]: Si estuviera en práctica en el tribunal, el juez ejecutor procederá a aplicar el Reglamento del Procedimiento Electrónico para la Solicitud de Datos al Banco Central de Venezuela publicado en la Gaceta Oficial de la República Bolivariana de Venezuela n° 40.616 del 9 de marzo de 2015, con preferencia a la experticia complementaria del fallo, para el cálculo de los intereses moratorios e indexación de los conceptos condenados.

16 http://historico.tsj.gob.ve/decisiones/spa/junio/305463-00339-12619-2019-2019-0069.html
17 Sentencia de la Sala Electoral del Tribunal Supremo de Justicia.
18 http://historico.tsj.gob.ve/decisiones/selec/junio/305632-037-20619-2019-2018-000046.html
19 http://historico.tsj.gob.ve/decisiones/spa/agosto/306731-00498-6819-2019-2015-1199.html
20 http://historico.tsj.gob.ve/decisiones/scs/marzo/304128-0039-18319-2019-18-453.html
21 http://historico.tsj.gob.ve/decisiones/scon/abril/304624-0078-25419-2019-17-0178.html
22 http://historico.tsj.gob.ve/decisiones/scs/abril/304661-0080-29419-2019-15-871.html
23 http://historico.tsj.gob.ve/decisiones/scs/julio/306368-0231-18719-2019-19-119.html
24 http://historico.tsj.gob.ve/decisiones/scs/agosto/307111-0343-14819-2019-19-154.html
25 http://historico.tsj.gob.ve/decisiones/scs/octubre/307353-0359-41019-2019-19-009.html
26 http://historico.tsj.gob.ve/decisiones/scs/noviembre/307895-0398-51119-2019-18-299.html
27 http://historico.tsj.gob.ve/decisiones/scs/noviembre/308134-0406-191119-2019-19-184.html
28 http://historico.tsj.gob.ve/decisiones/scs/diciembre/308995-0449-131219-2019-19-137.html

2. **SSCC N° 275 del 10 de julio**[29]: Indexación con base en los indicadores del Banco Central de Venezuela, según lo establecido en el Reglamento del Procedimiento Electrónico para la Solicitud de Datos del Banco Central de Venezuela, mediante experticia complementaria del fallo de conformidad con el artículo 249 del Código de procedimiento Civil la cual será realizada por un (01) experto contable designado por el Tribunal.

IV. Intercambio de información procesal por correo electrónico

1. **SJSSPA**[30] **N° 18 del 5 de febrero**[31], **27 del 13 de febrero**[32], **33 del 14 de febrero**[33], **59 y 64 del 3 de abril**[34], **66 del 4 de abril**[35], **76 del 23 de abril**[36], **80 del 24 de abril**[37], **91 del 7 de mayo**[38], **122 del 29 de mayo**[39], **134**[40] **y 136**[41] **del 12 de junio, N° 166 del 9 de julio de 2019**[42], **205 del 24 de septiembre**[43], **N° 245 del 29 de octubre**[44], **251 del 31 de octubre**[45]; **271 y 272**[46] **del 19 de noviembre**[47]; **y 286 del 5 de diciembre**[48]: Remisión de opinión

29 http://historico.tsj.gob.ve/decisiones/scc/julio/306027-rc.000275-10719-2019-18-655.html
30 Sentencia del Juzgado de Sustanciación de la Sala Político Administrativa del Tribunal Supremo de Justicia.
31 http://historico.tsj.gob.ve/decisiones/jspa/febrero/303539-18-5219-2019-2019-0003.html
32 http://historico.tsj.gob.ve/decisiones/jspa/febrero/303754-27-13219-2019-2018-0533.html
33 http://historico.tsj.gob.ve/decisiones/jspa/febrero/303795-33-14219-2019-2019-000001.html
34 http://historico.tsj.gob.ve/decisiones/jspa/abril/304303-64-3419-2019-2018-0460.html
35 http://historico.tsj.gob.ve/decisiones/jspa/abril/304322-66-4419-2019-2019-0028.html
36 http://historico.tsj.gob.ve/decisiones/jspa/abril/304600-76-23419-2019-2016-0386.html
37 http://historico.tsj.gob.ve/decisiones/jspa/abril/304608-80-24419-2019-2017-0195.html
38 http://historico.tsj.gob.ve/decisiones/jspa/mayo/304750-91-7519-2019-2014-0278.html
39 http://historico.tsj.gob.ve/decisiones/jspa/mayo/305268-122-29519-2019-2019-0127.html
40 http://historico.tsj.gob.ve/decisiones/jspa/junio/305482-134-12619-2019-2019-0131.html
41 http://historico.tsj.gob.ve/decisiones/jspa/junio/305495-136-12619-2019-2019-0144.html
42 http://historico.tsj.gob.ve/decisiones/jspa/julio/305987-166-9719-2019-2019-0165.html
43 http://historico.tsj.gob.ve/decisiones/jspa/septiembre/307265-205-24919-2019-2019-0216.html
44 http://historico.tsj.gob.ve/decisiones/jspa/octubre/307812-245-291019-2019-2019-0242.html
45 http://historico.tsj.gob.ve/decisiones/jspa/octubre/307859-251-311019-2019-2018-0732.html
46 http://historico.tsj.gob.ve/decisiones/jspa/noviembre/308177-272-191119-2019-2019-0262.html

por correo electrónico, de personas u organizaciones cuyo ámbito de actuación esté vinculado con el objeto de la controversia, en procesos contencioso-administrativos de contenido patrimonial (Art. 58 LOJCA).

2. **SJSSPA N° 123 del 28 de mayo**[49], **N° 125 del 30 de mayo**[50], **N° 148 del 20 de junio**[51], **N° 200 del 13 de agosto**[52], **N° 216 del 2 de octubre**[53], **249 del 30 de octubre**[54], **269 del 19 de noviembre**[55] **y 274 del 26 de noviembre**[56]: Remisión de opinión por correo electrónico, de personas u organizaciones cuyo ámbito de actuación esté vinculado con el objeto de la controversia, en procesos contencioso-administrativos de contenido patrimonial (numeral 3 del artículo 78 LOJCA)
3. **SSC N° 20 del 12 de febrero**[57], **N° 57 del 27 de febrero**[58], **N° 195 del 12 de julio**[59] , **SSCP N° 176 del 7 de agosto**[60] **y SSCC N° 465 del 12 de noviembre**[61]: Remisión mediante correo electrónico, por parte de un tribunal, de respuesta a información solicitada por el Tribunal Supremo de Justicia.

47 http://historico.tsj.gob.ve/decisiones/jspa/noviembre/308176-271-191119-2019-2019-0261.html
48 http://historico.tsj.gob.ve/decisiones/jspa/diciembre/308630-286-51219-2019-2018-0500.html
49 http://historico.tsj.gob.ve/decisiones/jspa/mayo/305269-123-29519-2019-2019-0120.html
50 http://historico.tsj.gob.ve/decisiones/jspa/mayo/305283-125-30519-2019-2019-0132.html
51 http://historico.tsj.gob.ve/decisiones/jspa/junio/305644-148-20619-2019-2019-0132.html
52 http://historico.tsj.gob.ve/decisiones/jspa/agosto/306984-200-13819-2019-2019-0211.html
53 http://historico.tsj.gob.ve/decisiones/jspa/octubre/307334-216-21019-2019-2019-0225.html
54 http://historico.tsj.gob.ve/decisiones/jspa/octubre/307847-249-301019-2019-2019-0243.html
55 http://historico.tsj.gob.ve/decisiones/jspa/noviembre/308169-269-191119-2019-2019-0092.html
56 http://historico.tsj.gob.ve/decisiones/jspa/noviembre/308260-274-261119-2019-2019-0270.html
57 http://historico.tsj.gob.ve/decisiones/scon/febrero/303685-0020-12219-2019-18-0074.html
58 http://historico.tsj.gob.ve/decisiones/scon/febrero/303996-0057-27219-2019-17-0123.html
59 http://historico.tsj.gob.ve/decisiones/scon/julio/306080-0195-12719-2019-19-0021.html
60 http://historico.tsj.gob.ve/decisiones/scp/agosto/306910-176-7819-2019-r18-155%20.html
61 http://historico.tsj.gob.ve/decisiones/scc/noviembre/308071-rc.000465-121119-2019-19-170.html

4. **SSC[62] N° 13 del 12 de febrero**[63]: Envío de copia de auto de la Sala Constitucional, por correo electrónico, a empresa privada (demandada) solicitando informe.
5. **SSPA N° 63 del 21 de febrero**[64]: Inclusión en el expediente del oficio remitido vía correo electrónico por la Directora General de Consultoría Jurídica del Ministerio del Poder Popular para las Comunas y los Movimientos Sociales.
6. **SSC N° 59 del 27 de febrero**[65]: Consignación de demanda de amparo por correo electrónico, ratificada dentro de los tres días siguientes en papel.
7. **SSC N° 42 del 27 de febrero, N° 139 del 12 de junio de 2019**[66], **N° 271 del 15 de agosto**[67] **y 285**[68], **301**[69], **302**[70], **306**[71], **301**[72] **del 16 de agosto, 487 del 4 de diciembre**[73] **y 502 del 9 de diciembre**[74]: Remisión de copia de sentencia y de oficio por correo electrónico de la Sala Constitución a otro órgano jurisdiccional.
8. **SJSSCS N° 239 del 27 de febrero**[75]: Envío a la Sala de Casación Social, por correo electrónico, del cómputo procesal de los días de despacho transcurridos en el tribunal.

62 Sentencia de la Sala Constitucional del Tribunal Supremo de Justicia.
63 http://historico.tsj.gob.ve/decisiones/scon/febrero/303673-0013-12219-2019-08-0664.html
64 http://historico.tsj.gob.ve/decisiones/spa/febrero/303881-00063-21219-2019-2016-0358.html
65 http://historico.tsj.gob.ve/decisiones/scon/febrero/303999-0059-27219-2019-17-1090.html
66 http://historico.tsj.gob.ve/decisiones/scon/junio/305479-0139-12619-2019-17-1252.html
67 http://historico.tsj.gob.ve/decisiones/scon/agosto/307136-0271-15819-2019-15-1131.html
68 http://historico.tsj.gob.ve/decisiones/scon/agosto/307150-0285-16819-2019-16-0506.html
69 http://historico.tsj.gob.ve/decisiones/scon/agosto/307166-0301-16819-2019-17-0196.html
70 http://historico.tsj.gob.ve/decisiones/scon/agosto/307167-0302-16819-2019-16-0885.html
71 http://historico.tsj.gob.ve/decisiones/scon/agosto/307150-0285-16819-2019-16-0506.html
72 http://historico.tsj.gob.ve/decisiones/scon/agosto/307178-0310-16819-2019-17-0224.html
73 http://historico.tsj.gob.ve/decisiones/scon/diciembre/308488-0487-41219-2019-15-0577.html
74 http://historico.tsj.gob.ve/decisiones/scon/diciembre/308711-0502-91219-2019-16-0506-19-0272.html
75 http://historico.tsj.gob.ve/decisiones/jscs/febrero/304138-239-27219-2019-18-464.html

9. **SJSSPA N° 46 del 27 de febrero**[76]: Orden de notificar del recibo de comunicación judicial mediante la dirección de correo electrónico spad.juzsu@tsj.gob.
10. **SJSSPA N° 62 del 3 de abril**[77]: Envío de documento por correo electrónico, del Tribunal Supremo de Justicia a un tribunal municipal del interior del país, por haberse omitido el envío de ese documento en papel a propósito de una comisión.
11. **JSSPA N° 102 del 14 de mayo**[78] **y 193 del 6 de agosto**[79]: Solicitud de informe judicial para ser remitido por correo electrónico.
12. **SJSSCC N° 446 del 21 de junio de 2018**[80]: Remisión de un documento administrativo de la Dirección Ejecutiva de la Magistratura a la Secretaría de la Sala de Casación Civil vía correo electrónico.
13. **SSC N° 84 del 25 de abril de 2019**[81], **200 del 12 de julio**[82] **y 297**[83] **del 16 de agosto**: Consignación de comprobante de pago de multa por correo electrónico enviado a la Sala Constitucional.
14. **SJSSCS N° 599 del 4 de junio de 2019**[84] **y 801 del 6 de agosto**[85]: Remisión por correo electrónico, del tribunal de la recurrida al Tribunal Supremo de Justicia, del auto de admisión de recurso de casación omitido en el envío del expediente original (en papel).
15. **SSC N° 169 del 4 de julio**[86]: Remisión por correo electrónico de copia de decisión de la Sala Constitucional por la que ordena al accionante aclarar su pretensión en el escrito presentado.

76 http://historico.tsj.gob.ve/decisiones/jspa/febrero/303976-46-27219-2019-2016-0564.html
77 http://historico.tsj.gob.ve/decisiones/jspa/abril/304300-62-3419-2019-2017-0193.html
78 http://historico.tsj.gob.ve/decisiones/jspa/mayo/304834-102-14519-2019-2019-0083.html
79 http://historico.tsj.gob.ve/decisiones/jspa/agosto/306814-193-6819-2019-2019-0083.html
80 http://historico.tsj.gob.ve/decisiones/jscc/junio/304878-0446-21618-2018-16-976.html
81 http://historico.tsj.gob.ve/decisiones/scon/abril/304630-0084-25419-2019-18-0278.html
82 http://historico.tsj.gob.ve/decisiones/scon/julio/306085-0200-12719-2019-18-0273.html
83 http://historico.tsj.gob.ve/decisiones/scon/agosto/307162-0297-16819-2019-16-0725.html
84 http://historico.tsj.gob.ve/decisiones/jscs/junio/305421-599-4619-2019-16-999.html
85 http://historico.tsj.gob.ve/decisiones/jscs/agosto/307059-801-6819-2019-19-088.html
86 http://historico.tsj.gob.ve/decisiones/scon/julio/305864-0169-4719-2019-16-1256.html

V. Citación y notificación telemáticas

1. **SSC N° 59 del 27 de febrero y N° 304 del 16 de agosto**[87]: Notificación electrónica conforme a lo señalado en el numeral 3 del artículo 91 de la Ley Orgánica del Tribunal Supremo de Justicia.
2. **SSPA N° 238 del 15 de mayo**[88]: Publicación de cartel en secretaría, portal web y correo electrónico pero contando solo a partir de la fijación del cartel.
3. **SJSSPA N° 60 del 3 de abril**[89] **y 143 del 18 de junio**[90]: Notificación mediante comisión judicial y correo electrónico, pero esta última modalidad solo tiene fines informativos y no procesales.
4. **SJSSCS**[91] **N° 151 del 14 de febrero de 2018**[92], **507 del 15 de mayo**[93] **y 652 del 17 de junio**[94], **y SSCS N° 25 del 20 de febrero, 86**[95], **87**[96], **91**[97] **del 8 de mayo y 192 del 4 de julio**[98]: Citación por cartel y en el portal de Internet del Tribunal Supremo de Justicia.
5. **SJSSPA N° 62 del 3 de abril**[99]: Aplicación del artículo 13 del Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas para la confirmación de recepción de un notificación.
6. **SSCS N° 97 del 9 de febrero**[100], **228 del 18 de julio**[101], **344 del 14 de agosto**[102], **405 del 11 de noviembre**[103], **y SSE N° 63 del 21 de febrero**[104]**:** Citación mediante cartel fijado en la cartelera

87 http://historico.tsj.gob.ve/decisiones/scon/agosto/307169-0304-16819-2019-17-1168.html
88 http://historico.tsj.gob.ve/decisiones/spa/mayo/304905-00238-15519-2019-2012-1593.html
89 http://historico.tsj.gob.ve/decisiones/jspa/abril/304298-60-3419-2019-2013-0591.html
90 http://historico.tsj.gob.ve/decisiones/jspa/junio/305571-143-18619-2019-2016-0701.html
91 Sentencia del Juzgado de Sustanciación de la Sala de Casación Social del Tribunal Supremo de Justicia.
92 http://historico.tsj.gob.ve/decisiones/jscs/febrero/303842-151-14219-2019-16-042.html
93 http://historico.tsj.gob.ve/decisiones/jscs/mayo/305214-507-15519-2019-18-299.html
94 http://historico.tsj.gob.ve/decisiones/jscs/junio/305733-652-17619-2019-15-1447.html
95 http://historico.tsj.gob.ve/decisiones/scs/mayo/304769-0086-8519-2019-15-860.html
96 http://historico.tsj.gob.ve/decisiones/scs/mayo/304770-0087-8519-2019-17-096.html
97 http://historico.tsj.gob.ve/decisiones/scs/mayo/304786-0091-8519-2019-15-938.html
98 http://historico.tsj.gob.ve/decisiones/scs/julio/305850-0192-4719-2019-17-604.html
99 http://historico.tsj.gob.ve/decisiones/jspa/abril/304300-62-3419-2019-2017-0193.html
100 http://historico.tsj.gob.ve/decisiones/scc/abril/304460-exeq.000106-11419-2019-15-485.html
101 http://historico.tsj.gob.ve/decisiones/scs/julio/306355-0228-18719-2019-17-657.html
102 http://historico.tsj.gob.ve/decisiones/scs/agosto/307114-0344-14819-2019-17-925.html
103 http://historico.tsj.gob.ve/decisiones/scs/noviembre/308044-0405-111119-2019-18-240.html
104 http://historico.tsj.gob.ve/decisiones/selec/diciembre/308433-063-21219-2019-2017-000022.html

de la Secretaría de la Sala y en el portal de Internet del Tribunal Supremo de Justicia.

7. **SJSSCC N° 376 del 22 de abril**[105] **y 505 del 11 de julio**[106]: Notificación mediante cartel fijado en la cartelera de la Secretaría de la Sala y en el portal de Internet del Tribunal Supremo de Justicia.
8. **SJSSPA N° 185 del 1° de agosto**[107], **237 del 17 de octubre**[108] **y 266 del 12 de noviembre**[109]: Citación a peritos por correo electrónico y en el portal de Internet del Tribunal Supremo de Justicia para ampliar o aclarar el informe pericial.
9. **SSCC N° 397 del 14 de agosto**[110]: Citación telemática en el «nuevo procedimiento civil único».
10. **SSC N° 326 del 3 de octubre**[111]: Notificación mediante correo electrónico y carta rogatoria
11. **SSPA N° 588 del 9 de octubre**[112]: Notificación de abogado, por correo electrónico, para ejercer la función de defensor *ad litem*.

VI. Prueba electrónica

1. **SSCS N° 15 del 12 de febrero y SSCC 480 del 20 de noviembre**[113]: Impresión de mensajes de correo electrónico desechados del proceso, no por su naturaleza sino porque «nada aporta a los hechos controvertidos».
2. **SJSSPA N° 5 del 16 de enero**[114], **SSCC N° 150 del 16 de mayo**[115] **y N° 83 del 21 de marzo**[116]: Valoración de las impresiones

105 http://historico.tsj.gob.ve/decisiones/jscs/abril/304606-376-22419-2019-13-558.html
106 http://historico.tsj.gob.ve/decisiones/jscc/julio/306039-0505-11718-2018-16-837.html
107 http://historico.tsj.gob.ve/decisiones/jspa/agosto/306651-185-1819-2019-2014-1402.html
108 http://historico.tsj.gob.ve/decisiones/jspa/octubre/307586-237-171019-2019-2014-1402.html
109 http://historico.tsj.gob.ve/decisiones/jspa/noviembre/308087-266-121119-2019-2017-0852.html
110 http://historico.tsj.gob.ve/decisiones/scc/agosto/307126-rc.000397-14819-2019-19-065.html
111 http://historico.tsj.gob.ve/decisiones/scon/octubre/307349-0326-31019-2019-19-0510.html
112 http://historico.tsj.gob.ve/decisiones/spa/octubre/307461-00588-91019-2019-2012-0775.html
113 http://historico.tsj.gob.ve/decisiones/scc/noviembre/308185-rc.000480-201119-2019-19-245.html
114 http://historico.tsj.gob.ve/decisiones/jspa/enero/303379-5-16119-2019-2002-1169.html
115 http://historico.tsj.gob.ve/decisiones/scc/mayo/304943-rc.000150-16519-2019-16-812.html

de mensajes de correo electrónico conforme al artículo 429 del Código de Procedimiento Civil.

3. **SSCS N° 33 del 25 de febrero**[117], **130 del 17 de mayo 2019**[118] **y 398 del 5 de noviembre**[119]: Valoración de las impresiones de mensajes de correo electrónico como una copia o reproducción fotostática, debiendo efectuarse su control, contradicción y evacuación, de la forma prevista para los documentos escritos.
4. **SSC N° 50 del 27 de febrero**[120]: **a.** La autenticidad de los mensajes de correo electrónico puede ser objeto de experticia. **b.** Valoración de la impresión de mensajes de correo electrónico conforme al artículo 429 del Código de Procedimiento Civil.
5. **SSPA N° 8 del 30 de enero**[121]: Validez del testimonio mediante videoconferencia.
6. **SSCC N° 108 del 11 de abril**[122]**:** 1. No debe desecharse la impresión de un mensaje de correo electrónico sin medios de prueba auxiliares como la exhibición, la inspección judicial o la experticia. 2. «las copias fotostáticas o las reproducciones realizadas por cualquier medio mecánico (impresiones de correos electrónicos), se reputarán fidedignas, siempre que no sean impugnadas por la contraparte… esto es, la no impugnación… se entenderá como un reconocimiento de la autenticidad y veracidad de su contenido».
7. **SSC N° 78 del 25 de abril**: Referencia a sentencia del 27 de octubre de 2016 de la Sala de Casación Social donde afirma el valor de la «… información impresa de un portal de internet de un órgano del Poder Público, conforme a lo dispuesto en el artículo 18 de la Ley de Infogobierno…» (sentencia de revisión constitucional declarada «no ha lugar»).
8. **SSCS N° 122 del 17 de mayo**[123]: La copia del expediente administrativo consignado en un disco compacto, certificado por la

116 http://historico.tsj.gob.ve/decisiones/scc/marzo/304275-rc.000083-21319-2019-18-224.html
117 http://historico.tsj.gob.ve/decisiones/scs/febrero/303947-0033-25219-2019-13-1554.html
118 http://historico.tsj.gob.ve/decisiones/scs/mayo/304964-0130-17519-2019-18-539.html
119 http://historico.tsj.gob.ve/decisiones/scs/noviembre/307895-0398-51119-2019-18-299.html
120 http://historico.tsj.gob.ve/decisiones/scon/febrero/303988-0050-27219-2019-16-0908.html
121 http://historico.tsj.gob.ve/decisiones/spa/enero/303450-00008-30119-2019-2016-0025.html
122 http://historico.tsj.gob.ve/decisiones/scc/abril/304463-rc.000108-11419-2019-18-460.html
123 http://historico.tsj.gob.ve/decisiones/scs/mayo/304954-0122-17519-2019-18-268.html

autoridad emisora, al ser impugnado en su contenido, debe compararse con el original en papel que consta en la sede administrativa.

9. **SSCC N° 83 del 21 de marzo**[124], **373**[125], **379**[126] **del 14 de agosto SSPA N° 790 del 5 de diciembre**[127]: Experticia sobre mensajes de correo electrónico.
10. **SSCS N° 216 del 11 de julio**[128]: Los mensajes de «… correo electrónico carecen de valor probatorio de conformidad con lo establecido en el artículo 92 de la Ley Orgánica Procesal del Trabajo, por cuanto se requiere del nombramiento de un experto para verificar su veracidad».
11. **SSCP N° 176 del 7 de agosto**[129]: Valoración de **«…**notas periodísticas en versión electrónica…» para fines de radicación.
12. **SSCC N° 373 del 14 de agosto**[130]. Valoración de impresiones de correo electrónico: 1. «… al no haber sido objeto de tacha, desconocimiento o impugnación alguna, se le otorga valor de plena prueba como instrumento privado reconocido, a tenor de lo previsto en el artículo 1363 del Código Civil, en concordancia con el artículo 4 de la Ley de Mensaje de Datos y Firmas Electrónicas y el artículo 429 del Código de Procedimiento Civil y tiene también valor indiciario conforme a lo previsto en el artículo 510 *eiusdem».* 2. «… impresión de correo electrónico de fecha 13 de abril de 2015, el cual, al haber sido reconocido por la representación judicial de la demandante, se le otorga valor de plena prueba como instrumento privado reconocido, a tenor de lo previsto en el artículo 1363 del Código Civil, en concordancia con el artículo 4 de la Ley de Mensaje de Datos y Firmas Electrónicas y el artículo 429 del Código de Procedimiento Civil y tiene también valor indiciario conforme a lo previsto en el artículo 510 ejusdem».

124 http://historico.tsj.gob.ve/decisiones/scc/marzo/304275-rc.000083-21319-2019-18-224.html
125 http://historico.tsj.gob.ve/decisiones/scc/agosto/307087-rc.000373-14819-2019-17-722.html
126 http://historico.tsj.gob.ve/decisiones/scc/agosto/307095-rc.000379-14819-2019-18-168.html
127 http://historico.tsj.gob.ve/decisiones/spa/diciembre/308589-00790-51219-2019-2015-0055.html
128 http://historico.tsj.gob.ve/decisiones/scs/julio/306049-0216-11719-2019-14-1524.html
129 http://historico.tsj.gob.ve/decisiones/scp/agosto/306910-176-7819-2019-r18-155%20.html
130 http://historico.tsj.gob.ve/decisiones/scc/agosto/307087-rc.000373-14819-2019-17-722.html

13. **SJSPA N° 259 del 7 de noviembre**[131]: La admisión de la impresión de mensajes de correo electrónico no requiere de la promoción de otro medio probatorio.
14. **SSPA N° 710 del 14 de noviembre**[132]: Valor probatorio de los mensajes de correo electrónico.
15. **SSCS N° 375 del 21 de octubre**[133]: Inspección judicial en portal de Internet.
16. **SSPA N° 813 del 11 de noviembre**[134]: La copia certificada de documento impreso de los datos del Sistema Venezolano de Información Tributaria (SIVIT) y el sitio web www.seniat.gob.ve, correspondiente a un contribuyente es una medio de prueba admisible y no «manifiestamente ilegal».
17. **SSCC N° 590 del 13 de diciembre**: Valor probatorio de la experticia informática.

VII. Contrato civil telemático

1. **SSC N° 243 del 18 de julio**[135]: La revocatoria de un contrato de mandato por correo electrónico requiere acuse de recibo o el cumplimiento del procedimiento pactado al efecto.
2. **SSCC N° 387 del 7 de agosto**[136]: Referencia a «…contrato de arrendamiento con opción a compra venta (documento electrónico)…».

VIII. Extradición por delitos informáticos

SSCP N° 54 de 2 de abril[137]: Cumplimiento del principio de doble incriminación a fin de extradición activa por fraude electrónico (de España a Venezuela).

131 http://historico.tsj.gob.ve/decisiones/jspa/noviembre/308020-259-71119-2019-2018-0302.html
132 http://historico.tsj.gob.ve/decisiones/spa/noviembre/308101-00710-141119-2019-2015-0042.html
133 http://historico.tsj.gob.ve/decisiones/scs/octubre/307631-0375-211019-2019-04-1682.html
134 http://historico.tsj.gob.ve/decisiones/spa/diciembre/308778-00813-111219-2019-2017-0779.html
135 http://historico.tsj.gob.ve/decisiones/scon/julio/306401-0243-18719-2019-18-0362.html
136 http://historico.tsj.gob.ve/decisiones/scc/agosto/306883-rc.000387-7819-2019-18-387.html
137 http://historico.tsj.gob.ve/decisiones/scp/abril/304291-54-2419-2019-e19-46.html

IX. Robótica

SSCS N° 60 del 5 de abril[138]: Referencia al uso de un robot en el lugar de trabajo.

138 http://historico.tsj.gob.ve/decisiones/scs/abril/304327-0060-5419-2019-16-220.html

ÍNDICE ACUMULADO

ARTÍCULOS

- El derecho a la protección de datos de las sentencias. **5** Ed. Digital / **20**, (2019), 9-46.

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.

GARCÍA OJEDA, Liliana del Valle.
- Algunas consideraciones sobre el uso de las redes sociales para la difusión y comercialización de la pornografía infantil en Venezuela. **5** Ed. Digital / **20**, (2019), 87-103.

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 REMOLINA ANGARITA.
- 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

HERRERA BRAVO, Rodolfo.
- Los registros de ADN y los derechos fundamentales: ¿Cómo esquilar 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

paridad relativa?. **16**, (2015), 65-80

MARTÍNEZ NADAL, Apollònia y FERRER GOMILÁ, Josep Luis.
- Delimitación de responsabilidades en caso de revocación de un certificado de firma electrónica: soluciones legales de Derecho europeo. **1**, (2002), 53-71.

MARTÍNEZ NADAL, Apollònia y ROSSELLÓ RUBERT, Francisca M.
- Auge del alquiler turístico vacacional y restricciones legales en España: Un análisis desde la perspectiva del Derecho de la Competencia. **3** Ed. Digital / **18**, (2017), 29-42.

MATA, Miguel Ángel.
- La protección al consumidor en la contratación a distancia. **8**, (Enero/Diciembre 2006), 73-94.

MATTUTAT MUÑOZ, Marjorie.
- La electronificación 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, Mª 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 contración informática. **4**, (Enero/Julio 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

co de la CNUDMI. **3**, (Julio/Diciembre 2003), 99-125.

SENENT VIDAL, María José.
- La protección jurídica del denominado "conocimiento libre". **6-7**, (Enero/Diciembre 2005), 141-170.

SOSA OLAN, Henrry.
- Régimen jurídico del derecho de desistimiento del consumidor a nivel comunitario y en el ordenamiento jurídico español. **3** Ed. Digital / **18**, (2017), 91-119

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.

SUÁREZ, Mariel Alejandra
- Tecnología, proceso judicial y derechos fundamentales. **5** Ed. Digital / **20**, (2019), 125-144.

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

CONTRIBUCIONES ESPECIALES

COMENTARIOS ESPECIALIZADOS

RESEÑA

RESEÑA LEGISLATIVA

CRÓNICA JURÍDICA

SECCION MONOGRÁFICA

Las implicaciones jurídicas de las redes sociales en Internet

ARRIETA ZINGUER, Miguel.
- El impacto de las redes sociales en el comercio electrónico con consumidores. **14**, (2013), 135-164

CHACÓN GÓMEZ, Nayibe.
- La responsabilidad de los proveedores de servicio en las redes sociales. **14**, (2013), 207-230

LÓPEZ JIMÉNEZ, David.
- Las redes sociales como espacios publicitarios: el papel de la autorregulación. **14**, (2013), 165-186

RAMÍREZ, Sulmer Paola.
- Los contenidos publicados por el trabajador en *Facebook* y sus consecuencias jurídico laborales. **14**, (2013), 187-205

RICO CARRILLO, Mariliana y LÓPEZ JIMÉNEZ, David.
- Las redes sociales en Internet: consideraciones generales y problemática jurídica. **14**, (2013), 101-112

RICO CARRILLO, Mariliana.
- El ejercicio de los derechos fundamentales y las libertades públicas a través de *Facebook*. **14**, (2013), 113-134

LEGISLACIÓN

II.1. Nacional

Decretos

Decreto N° 825 del 10 de mayo de 2000 mediante el cual se declara el acceso y el uso de Internet como política prioritaria para el desarrollo cultural, económico, social y político de la República Bolivariana de Venezuela. **1**, (2002), 185-188.

Decreto N°1.093 de 24 de noviembre de 2000 mediante el cual se decreta el Reglamento de Interconexión. **2**, (Enero/Junio 2003), 163-180.

Decreto Nº 1.094 de 24 de noviembre de 2000 mediante el cual se decreta el Reglamento sobre Habilitaciones Administrativas y Concesiones de uso y explotación del espectro radio-eléctrico. **2**, (Enero/Junio 2003), 181-207.

Decreto Nº 1.095 de 24 de noviembre de 2000 mediante el cual se decreta el Reglamento de apertura de los servicios de telefonía básica. **2**, (Enero/Junio 2003), 209-245.

Decreto Nº 2.189 de 13 de diciembre de 2002 mediante el cual se decreta el Reglamento sobre los tributos establecidos en la Ley Orgánica de Telecomunicaciones. **2**, (Enero/Junio 2003), 255-280.

Decreto-Ley de Mensajes de Datos y Firmas Electrónicas. **1**, (2002), 255-273.

Decreto N° 2.614, de fecha 24 de septiembre de 2003 mediante el cual se decreta el Reglamento de la Ley Orgánica de Telecomunicaciones sobre el Servi-

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 22/207, de 11 de julio, sobre Comercialización a Distacia de Servicios Financieros destinados a los Consumidores. **9**, (Enero/Diciembre 2007), 185-2005.

Ley 16/2009 de 13 de noviembre, sobre Servicio de Pago. **11**, (2010), 255-304.

Ley 7/2010 de 31 de marzo, General de la Comunicación Audivisual. **12**, (2011), 313-393

Real Decreto 322/2008 de 29 de febrero sobre el régimen jurídico de las entidades de dinero electrónico, **10**, (2008-2009), 303-322.

JURISPRUDENCIA

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.

VEGA SACASA, José Francisco

- La criptomoneda venezolana *PETRO* y su implementación como unidad de cuenta por parte del Tribunal Supremo de Justicia. **4** Ed. Digital / **19**, (2018), 155-159

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

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. Marcial 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 CALETRIO, Alfredo: *Pago con tarjeta de crédito: Naturaleza y régimen jurídico*, Revista Aranzadi de Derecho Patrimonial Nº 15 (monográfico), Thomson-Aranzadi, Navarra, 2005, 429 págs. **6-7**, (Enero/Diciembre 2005), 377-378.
- 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
- MARTÍNEZ NADAL, Apol.lonia, *Las cláusulas de paridad tarifaria en la comercialización electrónica de servicios de alojamiento turístico*. Thomson Reuters Aranzadi, 2017. **3** Ed. Digital / **18**, (2017), 159-163
- CHAMATROPULOS, Demetrio Alejandro. *Estatuto del consumidor comentado.* Thomson Reuters La Ley. Buenos Aires, Argentina (2016). **4** Ed. Digital / **19**, (2018), 191-196

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 WindowsTM 3.0 o superiores. Los gráficos o imágenes que contenga el artículo deben estar especificados con los formatos o extensiones en que se hicieron (Exce1TM, Corel DrawTM, jpg, gif, bmp, y otros), asimismo, las ilustraciones deben estar numeradas y a continuación del texto (no se aceptarán las que se encuentren al final del artículo). Las revistas podrán decidir no incluirlas, previa comunicación al autor o autores, si éstas no llenan los requisitos técnicos para su reproducción.

3. El texto del artículo debe redactarse tomando en cuenta los siguientes parámetros:
   3.1. La primera página debe contener:
      a) Título del artículo
      b) Nombre del autor o autores
      c) Título académico y afiliación institucional
      d) Dirección del autor y correo electrónico
      e) Síntesis curricular no mayor a diez (10) líneas

   3.2. La segunda página debe contener un resumen no mayor de ciento cuarenta (140) palabras, concentrándose en los objetivos, métodos de estudio, resultados y conclusiones. A1 final del mismo se deben incluir las palabras claves en un número no mayor a cinco (5).
      a) El resumen y las palabras claves deben venir redactadas en español e inglés
      b) Se podrán aceptar artículos redactados en inglés, francés u otros idiomas sólo en casos especiales, debiendo contener las palabras claves en español e inglés.

   3.3. El texto del artículo debe estructurarse en secciones debidamente identificadas, siendo la primera la introducción (o reseña de los conocimientos existentes, limitada estrictamente al tema tratado en el artículo). Las secciones deben identificarse sólo con números arábigos. Cada artículo antes de la primera sección o sección introductoria, debe tener un sumario en el que se enumeren los temas que se van a desarrollar (las secciones en las cuales fue dividido el trabajo).

   3.4. Si parte del material trabajado (textos, gráficos e imágenes utilizados) no son originales del autor o de los autores, es necesario que los mismos estén acompañados del correspondiente permiso del autor (o de los autores) y el editor donde fueron publicados originalmente, en su defecto, se debe indicar la fuente de donde fueron tomados.

   3.5. En las referencias bibliográficas se debe utilizar el sistema de cita formal, haciendo 1a correspondiente referencia en las notas a pie de página, las cuales deben ser enumeradas en números arábigos, siguiendo un orden correlativo.

Las citas, en las notas al pie de página, se harán siguiendo los siguientes ejemplos; según se trate de:

A. Libros

Mariano Aguilar Navarro: *Derecho Internacional Privado*, VI. 4a. edición, 2a. reimpresión. Madrid. Universidad Complutense de Madrid, 1982, p.199 (o pp. 200 y ss).

Marino Barbero Santos: "Consideraciones sobre el Estado peligroso y las Medidas de Seguridad, con especial referencia al Derecho Italiano y Alemán". *Estudios de Criminología y Derecho Penal*. Valladolid. Universidad de Valladolid, 1972, pp. 13-61.

Vicente Mujica Amador: *Aproximación al Hombre y sus Ideologías*. Caracas. Editorial Vidabun, 1990.

Hans Kelsen: *Teoría Pura del Derecho*. XVII edición. Buenos Aires. EUDEBA, 1981.

B. Cita sucesiva del mismo libro

M. Aguilar N.*: Derecho Internacional* V.II.… op. cit., p.78 y ss.

C. Obras colectivas

Haydée Barrios: "Algunos aspectos de cooperación judicial internacional en el sistema venezolano de derecho internacional privado". *Libro-Homenaje a Werner Goldschmidt*. Caracas. Facultad de Ciencias Jurídicas y Políticas, Universidad Central de Venezuela. 1997, pp. 383-419. Si se desea citar un determinado párrafo o página se agrega: especialmente, p. 80 o pp. 95-98.

D. Revistas

Gonzalo Parra-Aranguren: "El Centenario de la Conferencia de La Haya de Derecho Internacional Privado". *Revista de la Facultad de Ciencias Jurídicas y Políticas*, N° 85. Caracas. Universidad Central de Venezuela, 1992, pp. 75-100.

E. Cita sucesiva del mismo artículo

G. Parra-Aranguren: "*El Centenario de la Conferencia*..." op.cit., pp.80-85.

F. Citas de jurisprudencia

Orden de citar: Tribunal, N° y fecha de la sentencia, partes y fuentes de publicación. Ejemplo:
Corte Superior del Distrito Federal, N°…, 6-5-1969 (Jacques Torfs vs. Clemencia de Mier Garcés), Jurisprudencia Ramirez y Garay, Vol. 21, p. 163.

G. Citas de testimonios verbales y entrevistas

Se indicará el nombre de la persona que proporciona la información, la forma como se obtuvo y la fecha. Por ejemplo:

F. Rodríguez. Entrevista, 30/03/1999.

Esta información puede suministrarse siempre que lo autorice quien proporciona la información[1].

H. Citas de páginas web

Si la cita se refiere a un sitio web (cita de carácter general) se coloca el *home page*. Si es una página específica dentro de un sitio web (cita de carácter especial) se debe colocar en primer lugar, la dirección del *link* (sub-página) y en segundo lugar la dirección donde aparece alojada la información, (*home page*). Debe indicarse también la fecha de la consulta, entre corchetes, indicando el año, luego el mes y finalmente el día
Ejemplos:

a) Cita de carácter general:
www.zur2.com.fipa. [Consulta: 2008, Noviembre 27].

b) Cita de carácter especial:
   - Tatiana B. de Maekelt: La Ley de Derecho Internacional Privado http:// zur2.com/users/fipa/objetivos/leydip1/tamaek.htm 10/02/2001. www.zur2.com.fipa. [Consulta: 2008, Noviembre 27].

   - Haydée Barrios: El Domicilio http://zur2.com/users/fipa/objetivos/leydip1/barrios.htm 8/04/2002. www.zur2.com.fipa. [Consulta: 200, Noviembre 27].

4. Los artículos deben tener una extensión no mayor de cuarenta (40) cuartillas o páginas, escritas a espacio y medio y con un margen izquierdo de cuatro (4) centímetros. Tipo de letra: Times New Roman 12.

5. Los artículos pueden ser remitidos en un archivo adjunto, a la dirección electrónica: albornoz@ucat.edu.ve, o al correo electrónico del director de la revista:

   - Revista Tachirense de Derecho: Prof. José Luis Villegas villegas@ucat.edu.ve
   - Revista *Tributum*: Prof. Jesús Manuel Oliveros joliveros@ucat.edu.ve
   - Revista Paramillo: Prof. Felipe Guerrero felipeguerrero11@gmail.com
   - Revista Derecho y Tecnología: Prof. Mariliana Rico marilianarico@yahoo.com

6. Los autores deberán firmar una autorización (en un formato que remitirá a tal efecto) donde se especifica el derecho que tiene la revista, y por ende, la Universidad Católica del Táchira, de reproducir el artículo en este medio de comunicación, sin ningún tipo de retribución económica o compromiso de la Universidad con el autor o los autores, entendiéndose éste como una contribución a la difusión del conocimiento y/o desarrollo tecnológico, cultural o científico de la comunidad o del país en el área en que se inscribe.

7. Cuando se envíen textos que estén firmados por más de un autor, se presumirá que todos los autores han revisado y aprobado el original enviado.

1 UPEL: *Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales*. Caracas. FEDEUPEL. 2003, p. 91.

8. Se reserva el derecho de hacer las correcciones de estilo que se consideren convenientes, una vez que el trabajo haya sido aceptado por el Consejo de Redacción para su publicación.
9. Los artículos serán analizados por un Comité de Árbitros y por un Consejo de Redacción. El cumplimiento de las normas no garantiza su publicación, si el trabajo no es aprobado por estas instancias.
10. La Universidad Católica del Táchira, el editor y el Consejo de Redacción de la revista, no se responsabilizarán de las opiniones expresadas por los colaboradores en sus respectivos artículos.
11. La UCAT se reserva el derecho de distribuir el contenido de la revistas en su página web o en otras páginas de contenido académico o científico.

Article Submissions Guidelines

1. The material must be unpublished, understanding it had not been published or presented to be evaluated by other divulging means. The Editorial Board reserves the right to publish articles, in exceptional cases, when they have already been published.

2. Articles must be redacted in editor programs that work in Windows™ 3.0 or higher. The graphics or images that present the article must be specified with the formats or extensions where they were made (Excel™, Corel Draw™, jpg, gif, bmp, and others). In the same way, the illustrations must be numbered just after the text (Those illustrations at the end of the article will be not accepted). The journals could decide not to include them, by communication to the author or authors in advance, if them do not fulfill the technical requirements to their publication.

3. The text of the article must be redacted considering the following parameters:
   3.1. The first page must have:
      a) Title of the article
      b) Author or author's name
      c) Academic title and institutional affiliation
      d) Author address and e-mail
      e) Resume no longer than 10 lines

   3.2. The second page must have an abstract no longer than one hundred and forty words (140), focusing on the goals, methodology, results and conclusions. At the end, the key words must be included in a maximum number of five (5).
      a) The abstract and the key words must be written in Spanish and English.
      b) Articles in English, French and other languages could be accepted, just in special cases. In all cases they must have the key words in Spanish and English.

   3.3. The text article must be structured in clearly identified sections, being the first the introduction (description of the existent knowledge, limited to the subject of the article). The sections must be identified with Roman and Arabic numerals. Each article, before section one or introduction, must have a summary where appear numbered the subjects to be discuss on the paper (sections the article was divided).

   3.4. If part of the material (text, graphics, images) is not original of the author or authors, is necessary that this material to be authorized by the original author (or authors) and the editor where were first published, in lack of this, the source where they were taken must be indicated.

   3.5. The formal citing system must be used for the bibliographic references, doing the right reference at the foot of the page numbered in Arabic numeral, following a correlative order.

   The references in the footnotes will be included according to the following examples:

A. Books

Mariano Aguilar Navarro: *Derecho Internacional Privado*, VI. 4a. edición, 2a. reimpresión. Madrid. Universidad Complutense de Madrid, 1982, p.199 (o pp. 200 y ss).

Marino Barbero Santos: "Consideraciones sobre el Estado peligroso y las Medidas de Seguridad, con especial referencia al Derecho Italiano y Alemán". *Estudios de Criminología y Derecho Penal*. Valladolid. Universidad de Valladolid, 1972, pp. 13-61.

Vicente Mujica Amador: *Aproximación al Hombre y sus Ideologías*. Caracas. Editorial Vidabun, 1990.

Hans Kelsen: *Teoría Pura del Derecho*. XVII edición. Buenos Aires. EUDEBA, 1981.

B. Subsequent quotations of the same book

M. Aguilar N.*: Derecho Internacional* V.II.… op. cit., p.78 y ss.

C. Collective Works

Haydée Barrios: "Algunos aspectos de cooperación judicial internacional en el sistema venezolano de derecho internacional privado". *Libro-Homenaje a Werner Goldschmidt*. Caracas. Facultad de Ciencias Jurídicas y Políticas, Universidad Central de Venezuela. 1997, pp. 383-419. Si se desea citar un determinado párrafo o página se agrega: especialmente, p. 80 o pp. 95-98.

D. Journals

Gonzalo Parra-Aranguren: "El Centenario de la Conferencia de La Haya de Derecho Internacional Privado". *Revista de la Facultad de Ciencias Jurídicas y Políticas*, N° 85. Caracas. Universidad Central de Venezuela, 1992, pp. 75-100.

E. Subsequent quotations of the same article

G. Parra-Aranguren: "*El Centenario de la Conferencia...*" op.cit., pp.80-85.

F. Quotation of jurisprudence:

Corte Superior del Distrito Federal, N°…, 6-5-1969 (Jacques Torfs vs. Clemencia de Mier Garcés), Jurisprudencia Ramirez y Garay, Vol. 21, p. 163.

G Quotation of oral testimonies and interviews

It must include the name of the person providing the information, how it was obtained, and the date:

F. Rodríguez. Entrevista, 30/03/1999.

This information can be provided only if it is authorized by the provider of the information[1].

1 UPEL: *Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales*. Caracas. FEDEUPEL. 2003, p. 91.

H. Quotation of web pages

If a quote refers to an entire website (general citation), should include the reference of the home page. If is a **specific page within a website** (special citation), should include in first place, the link (sub-page) and in second place, the reference of the home page. It should also indicate the date the page was visited. This information should be in listing showing year, month, and day.

a) General quotation:
www.zur2.com.fipa. [Visited: 2008, Noviembre 27].

b) Special quotation:
   - Tatiana B. de Maekelt: La Ley de Derecho Internacional Privado http://zur2.com/users/fipa/objetivos/leydip1/tamaek.htm 10/02/2001. www.zur2.com.fipa. [Consulta: 2008, Noviembre 27].

   - Haydée Barrios: El Domicilio http://zur2.com/users/fipa/objetivos/leydip1/barrios.htm 8/04/2002. www.zur2.com.fipa. [Visited: 200, Noviembre 27].

4. Articles must have a maximum extension of forty (40) pages written in 1.5 space with a left margin of four (4) centimeters. The type letter will be Times New Roman 12.

5. Articles must be sent in an attachment to the e-mail: albornoz@ucat.edu.ve, or to the e-mail of the director of the journal:
   - Revista Tachirense de Derecho: Prof. José Luis Villegas villegas@ucat.edu.ve
   - Revista *Tributum*: Prof. Jesús Manuel Oliveros joliveros@ucat.edu.ve
   - Revista Paramillo: Prof. Felipe Guerrero felipeguerrero11@gmail.com
   - Revista Derecho y Tecnología: Prof. Mariliana Rico marilianarico@yahoo.com

6. Authors should sign an authorization (a format will be sent to this purpose) where it is specified the right of the journal, as well as the Universidad Católica del Táchira, to publish the article on this divulging means, without any economic retribution or commitment of the University with the author or authors, understanding the article is a contribution to the divulging of knowledge and technological development, cultural or scientific of the community or the country in the area where it is registered.

7. When articles are sign by more than an author, it would be presumed that all authors have been check and approved the original text sent.

8. The right of change of stylus that is considered convenient is reserved, once the article has been accepted by the Editorial Board for its publication.

9. An Arbitral Committee and an Editorial Board will analyze the articles. The observance of these rules does not guarantee the publication of the article if this is not approved by these instances.

10. The Universidad Católica del Táchira, the editor, and the Editorial Board of the journal, are not responsible of the expressed opinions by the collaborating and the articles.

11 The Universidad Católica del Táchira reserves the right to distribute the contents of their journals on its website, or on other pages of academic or scientific content.

DERECHO Y TECNOLOGÍA

VICERRECTORADO ACADÉMICO DECANATO DE INVESTIGACIÓN Y POSTGRADO	5/2019 Edición Digital 20/2019 Edic Ordinaria

Revista de Derecho y Tecnología, Enero / Diciembre 2019,
de la Universidad Católica del Táchira.
San Cristóbal - Venezuela