Universidad Internacional de La Rioja
Facultad de Derecho

Máster Universitario en Ciberdelincuencia

Responsabilidad Penal de la Persona Jurídica por Delitos Informáticos en Venezuela

Trabajo fin de estudio presentado por:	Lisandro, Bautista Landaeta Yunai Josefina, Perche Fuenmayor
Tipo de trabajo:	Trabajo de Fin de Máster
Directora:	Dra. D. Gemma Martínez Galindo
Fecha:	2 de febrero de 2021

Resumen

La responsabilidad penal de la persona jurídica por delitos informáticos en Venezuela está prevista en la Ley especial contra los delitos informáticos (2001), bajo los postulados del modelo de atribución ecléctica de responsabilidad, del modelo de imputación por hechos propios, con concurrencia de personas naturales cuando actúan en su representación o con independencia de aquella, que genera una sanción penal corporal y no corporal: para la persona jurídica la pena es no corporal de multa por el doble del monto previsto para el delito (art. 10 Código penal, 2005) y para la persona natural la pena comprende prisión y multa. La incidencia de la delincuencia informática en Venezuela muestra un fenómeno criminológico en ascenso en el ciberespacio que involucra a personas jurídicas como sujetos pasivos y activos, lesionador de bienes jurídicos protegidos en menoscabo de los derechos humanos que exponen la sustentabilidad de la sociedad. Esta situación exige la adaptación de la dogmática penal incluyendo las políticas criminales entorno a la criminalidad informática de la persona jurídica, así como la adecuación de la legislación procesal penal.

Palabras claves: responsabilidad penal, persona jurídica, delitos informáticos, ciberespacio.

Abstract

The criminal liability of the legal entity for computer crimes in Venezuela is provided for in the special law against computer crimes (2001) under the postulates of the eclectic attribution model of responsibility, of the imputation model for own acts, with concurrence of natural persons acting on their behalf or independently of that, which generates a corporal and non-corporeal criminal sanction (art. 10 Penal code, 2005), for the legal person the penalty is non-corporeal of a penalty fee for twice the amount provided for the crime and for the natural person, the penalty includes imprisonment and a penalty fee. The incidence of computer crime in Venezuela shows a criminological phenomenon on the rise in cyberspace that involves legal persons as passive and active subjects, injuring protected legal assets to the detriment of human rights that expose the sustainability of society. This situation requires the adaptation of criminal dogma, including criminal policies around computer crime of the legal entity, as well as the adaptation of criminal procedural legislation.

Keywords: criminal responsibility, legal person, computer crimes, cyberspace.

Índice de contenidos

Índice de Gráficos

1. Introducción

Con la aparición de internet y la disposición global de las tecnologías de la información y comunicación (TIC) para la ejecución de los procesos y actividades, tanto personales como corporativos e institucionales, también apareció la ciberdelincuencia que ha evolucionado con la misma velocidad de aquellas al migrar su acción delictiva a internet y a las diversas plataformas informáticas alojadas en el ciberespacio (GIBSON 1982).

Puede señalarse que la presencia y dependencia de internet ha generado riesgos que son desconocidos para la mayoría de los usuarios en el ciberespacio, quienes además ignoran cómo defenderse; por otra parte, el anonimato de internet, el carácter transfronterizo y el poder de la ciberdelincuencia de victimizar con una acción a millones de personas en una mínima fracción de tiempo, representan oportunidades para la comisión de actos delictivos que causan inmensurables daños (MIRÓ 2011).

De esta situación no escapan las personas jurídicas (PJ) sin distingo del tipo de organización corporativa que se trate, ni de su tamaño o complejidad, quienes potencialmente pueden ser víctimas, pero también pueden incurrir en delitos informáticos y, eventualmente, ser responsables penalmente por conductas disvaliosas de esa clase. Este escenario ha requerido de la investigación, el estudio y la revisión constante de la incidencia de la cibercriminalidad de la empresa en el ciberespacio, de las políticas criminales y de las sanciones previstas en el ordenamiento jurídico penal de los Estados para persuadir y castigar la ciberdelincuencia empresarial, para controlar su expansión y evitar su impunidad ante hechos lesivos que, por un lado, atentan contra bienes jurídicos protegidos por la ley, pero que por el otro y en definitiva, afectan directamente los derechos humanos y la paz social.

1.1. Justificación del tema elegido

La previsión de la responsabilidad penal de la persona jurídica (RPPJ) por delitos informáticos es un tema controversial en Venezuela[1] aún veinte años después de sancionada la Ley especial contra los delitos informáticos (LECDI) en 2001; de modo que persiste el interés de profundizar

[1] Venezuela no es parte del Convenio sobre la Ciberdelincuencia firmado en Budapest (2001).

sobre su comprensión y el alcance de las complicaciones dogmáticas que se presentan entorno a los postulados del principio «*societas delinquere non potest*», de cara a la operacionalización de la responsabilidad penal de la persona jurídica, lo que ha motivado su escogencia como tema de esta investigación.

1.2. Problema y finalidad del trabajo

La cibercriminalidad es un fenómeno que trasciende a la persona jurídica (PJ) como sujeto activo del delito que deriva en la responsabilidad penal por la comisión de delitos informáticos conforme a la legislación penal especial que regula la materia[2] en Venezuela. Sin embargo, a pesar de su previsión legal todavía no queda claro para la doctrina ni la jurisprudencia ¿cuál es el modelo de atribución de la responsabilidad penal?, ¿cuál es el criterio de imputación de tal responsabilidad?, ni la determinación precisa de si se imputan hechos propios o hechos ajenos y, finalmente, si la sanción de multa que se aplica es en puridad de naturaleza penal.

Todos estos elementos deben ser claramente determinados para que, a partir de allí en la práctica se pueda establecer la responsabilidad penal de las personas jurídicas (RPPJ) y deslindarla de la responsabilidad penal de las personas naturales (RPPN) que actúan en nombre y representación de la primera, cuando aparecen involucrados como sujetos activos en los procesos penales por ciberdelitos, haciendo posible la aplicación efectiva de la ley en la persecución y sanción de tales hechos antijurídicos por el Ministerio Público y por el órgano jurisdiccional competente.

Por otra parte, impulsar el conocimiento multidisciplinario sobre el tema es esencial, dado que, en Venezuela, son escasos los estudios y los trabajos de investigación sobre la RPPJ y su consecuencia, así como es escasa la jurisprudencia sobre el tema. En este estado, resulta oportuna la investigación por su novedad, su pertinencia jurídica y también práctica en la identificación clara del modelo de atribución de la responsabilidad penal a la persona jurídica, el criterio de imputación y la naturaleza de la sanción de la previsión de la RPPJ que el

[2] Ley especial contra los delitos informáticos dictada en el año 2001 por la Asamblea Nacional.

legislador plasmó en la LECDI (2001), como elementos esenciales respecto de los cuales se pretende hacer un análisis y ofrecer un aporte.

1.3. Objetivos

Se ha planteado en este trabajo un objetivo general y varios objetivos específicos que aportarán la orientación necesaria de la investigación para lograr de forma ordenada y estructurada la consecución de los resultados como propósito final de su ejecución.

1.3.1. Objetivo general

El objetivo general trazado es analizar la responsabilidad penal de la persona jurídica en Venezuela a partir de la Ley especial contra los delitos informáticos (2001).

1.3.2. Objetivos específicos

Con el propósito de alcanzar el objetivo general se han trazado varios de orden específico, que permitirán plasmar de manera ordenada los resultados de la investigación como contenido de la memoria de este trabajo y aporte final a la comunidad científica. Estos objetivos son los siguientes: conocer las referencias de Derecho Comparado sobre la RPPJ; identificar la previsión legal sobre la responsabilidad penal de la persona jurídica en Venezuela por delitos informáticos; considerar los antecedentes doctrinarios sobre la RPPJ; analizar la responsabilidad penal de la persona jurídica en Venezuela a partir del artículo 5 de la LECDI (2001); comprender las teorías sobre la responsabilidad penal de la persona jurídica; estudiar el modelo de atribución de la responsabilidad penal de la persona jurídica según el artículo 5 de la LECDI (2001); analizar el modelo de imputación de responsabilidad penal de la persona jurídica según el artículo 5 de la LECDI (2001); explicar la naturaleza de la sanción que se impone a la persona jurídica según el artículo 5 de la LECDI (2001); explorar los aportes y perspectivas de la jurisprudencia del Tribunal Supremo de Justicia sobre la responsabilidad de la PJ en Venezuela; exponer la incidencia de la ciberdelincuencia en Venezuela; analizar la responsabilidad penal de la persona jurídica por ciberdelitos; y señalar los tipos penales en la LECDI (2001).

1.4. Método

Para abordar el logro de los objetivos formulados se desarrolló una investigación documental con un diseño analítico interpretativo, conforme al método y técnicas de análisis cualitativo de las fuentes documentales bibliográficas, escritas, electrónicas, gráficas y audiovisuales relacionados con el tema, que incluye doctrina científica, jurisprudencia, legislación vigente nacional e internacional. Este trabajo se encuentra enmarcado en la línea de investigación Derecho Penal Económico y Empresarial del Grupo de Investigación PENALCRIM de la Universidad Internacional de La Rioja.

En la primera fase se concretó la búsqueda en las fuentes bibliográficas y audiovisuales, para lo cual se recurrirá a bases de datos físicas y digitales, repositorios de investigación académicos, libros, textos, revistas especializadas, trabajos de grado, tesis, ensayos, artículos y videos que albergan información relacionada con el cumplimiento normativo aplicado a las tecnologías de la información y comunicación. Luego, mediante la lectura exploratoria, se procedió a su selección con base en los criterios de pertinencia, exhaustividad y actualidad, para dar paso a su recopilación y almacenamiento en físico y en dispositivos informáticos.

En la fase intermedia, se inició la sistematización y el procesamiento de los datos recabados mediante las técnicas de lectura y citas. El almacenamiento de la información relevante se determinó por su contenido, cronología y tipo de documento. Concluida esa etapa, se procedió al análisis e interpretación de la información mediante las técnicas de lectura reflexiva y análisis cualitativo para su comprensión, su contrastación y la construcción del conocimiento sobre el alcance y regulación de la responsabilidad penal de la persona jurídica por delitos informáticos en Venezuela y otros aspectos de comprensión relevante que integran los objetivos trazados.

En la fase final, tendrá lugar el desarrollo de la etapa de escritura y redacción del resultado, con especial énfasis en la aportación de los autores y sus conclusiones producto del proceso cognitivo intelectual jurídico-deductivo incluso inductivo ejecutado para coadyuvar al conocimiento y dominio del tema por las organizaciones que hacen uso de sistemas informáticos e interactúan en el ciberespacio, desde la construcción de un marco teórico base a considerar entorno a los riesgos de delitos informáticos y la eventual responsabilidad penal de la persona jurídica como parte del tratamiento de la problemática planteada.

2. Responsabilidad penal de la persona jurídica en Venezuela

La delincuencia penal económica es un fenómeno que ha menoscabado el bienestar y la sustentabilidad de la sociedad desde hace ya varias décadas y que ha dado paso al cambio de paradigma sobre la RPPJ, en oposición al principio «*societas delinquiere non potest*», el cual ha perdido vigencia en cada vez más legislaciones por varias razones: primero, porque no abarca las conductas delictivas de las organizaciones como sujetos o personas de derecho, que quedan excluidas del sistema de responsabilidad penal, favoreciéndose de esta manera la impunidad; segundo, porque devino ineficaz para explicar el derecho penal respecto de las personas jurídicas; tercero, porque no responde a la realidad de la delincuencia corporativa y, en definitiva, no sirve para la persecución y castigo de los agravios a los bienes jurídicos protegidos por la ley penal. Puede señalarse que ese postulado no es coherente con el sistema de garantía de derechos humanos. En este orden de ideas, se aborda el estudio, alcance y estado actual de la RPPJ por delitos informáticos en conjunción con la postura del legislador venezolano y la incidencia de la ciberdelincuencia en Venezuela como condición base esencial para abordar un análisis sobre datos que muestran una panorámica real de la situación en Venezuela, que podría generar la responsabilidad penal de una persona jurídica como sujeto activo de ciberdelitos.

2.1. Consideraciones previas

A lo largo de la historia, los Estados se han dado el marco jurídico que los rige, en atención a sus valores culturales, sociales, políticos y económicos en ejercicio del derecho de la autodeterminación de los pueblos[3]. Así el Derecho encuentra su razón en la función social y política de consolidar el orden, el tratamiento y resolución de las situaciones fácticas de diversas índoles que surgen de la interrelación diaria de las personas naturales y jurídicas, públicas o privadas y entre ambas, con base en normas jurídicas reconocidas y aceptadas que comprenden principios de equidad, justicia, igualdad, legalidad, así como derechos y

[3] Conforme a los artículos 1.2 de la Carta de Naciones Unidas (1945), artículo 1 del Pacto Internacional sobre derechos civiles y políticos de 16 de diciembre de 1966 y artículo 1 del Pacto Internacional de derechos económicos, sociales y culturales, de la misma fecha.

obligaciones, para garantizar la existencia y convivencia pacífica de las personas cualquiera sea su naturaleza; factores éstos necesarios para lograr el desenvolvimiento de la persona, la sustentabilidad de las sociedades y el estado de derecho. En la época contemporánea no ha sido diferente. Las sociedades siguen experimentando cambios inimaginables producto de la evolución de la humanidad en todas las áreas: social, política, económica, cultural, tecnológica, científica y otras, que dan paso a nuevos paradigmas en cuanto a la forma de actuar, hacer y relacionarse, en medio de nuevas dinámicas generadoras de hechos y situaciones que luego son objeto de regulaciones jurídicas adaptadas a esa realidad.

Es un hecho notorio que tras el crecimiento del aparato empresarial y la dinámica de los negocios, acelerada por la expansión y globalización de los mercados así como la proliferación de organizaciones multinacionales y transnacionales como estructuras complejas, se ha experimentado a nivel mundial, desde hace ya varias décadas, un considerable incremento de conductas delictivas traducidas en actos de criminalidad económica (TIEDEMANN 1993, ACHENBACH 1995, VEGA DUEÑAS 2021), que han tenido relación directa con las organizaciones corporativas como sujetos activos[4], en cuanto sus representantes u órganos hubieren actuado en su nombre y en beneficio de la empresa, desplegando una acción antijurídica, tipificada y penalizada como delito en la ley penal, generadoras de graves consecuencias para las organizaciones, las personas responsables y las marcas afectadas. En efecto, según un trabajo del Max-PlanckInstitut für Ausländisches und Internationales Strafrecht[5] durante los años 1974 y 1985, más del 80% de los delitos de orden económico fueron cometidos por intermedio de empresas. Esas conductas ilícitas ejecutadas desde las empresas motivaron nuevas leyes y regulaciones dirigidas a persuadir y sancionar esas conductas disvaliosas a partir de nuevos criterios.

Con la aparición de internet y la expansión de las TIC e innumerables plataformas informáticas, que funcionan como sistemas de interconexión remota y masiva en la red (MAYER LUX 2017), surge un nuevo paradigma en las relaciones humanas y de éstas con las máquinas, que además de representar una trascendental evolución en materia tecnológica en la historia contemporánea (CARLINI 2016) es, sobre todo, la materialización de un cambio de patrones

[4] Referenciado en la Circular 1/2011 del 1 de junio, de la Fiscalía General de la República, España.
[5] Instituto Max-Planck para el Derecho Penal Extranjero e Internacional.

de socialización que facilitan enormemente los intercambios comerciales (QUINTERO 2001) y la conquista de mercados globalizados en la red. Este fenómeno dio paso a la migración de las actividades cotidianas y procesos a los entornos digitales (MIRÓ 2011) no solo de los humanos sino también de los entes corporativos, creándose en el ciberespacio[6], un nuevo escenario digital de oportunidades para agilizar procesos y actividades, incluso sociales, culturales, de formación, comerciales y, por supuesto, también para la ciberdelincuencia[7] que migró a esos entornos (MIRÓ, 2012), valiéndose de la infraestructura informática como medio para ejecutar conductas disvaliosas punibles -criminalidad informática en sentido amplio-, de carácter transfronterizo, altamente efectivas y eficaces, de coste muy bajo, de ejecución simple y de riesgos mínimos (MIRÓ 2012), contra bienes jurídicos protegidos colectivos o individuales, también contra los sistema, equipos y datos como objeto del delito para causar daño -criminalidad informática en sentido estricto- (MAYER LUX, 2017). De allí que dada la expansión del uso de la telemática, los sistemas y plataformas informáticos en todas las áreas del quehacer, tanto por entes públicos como privados, cualquier diversidad de delitos, desde terrorismo, odio, fraude, pornografía infantil, sabotajes homicidios, drogas, sobornos, corrupción, entre otros, pueden ser cometidos mediante las TIC (HERNÁNDEZ 2009), por individuos y por organizaciones u entes colectivos.

En una concepción contemporánea, la empresa es un verdadero agente económico, una unidad de producción de bienes y servicios, que a su vez es un consumidor a gran escala. Sin embargo, hay acuerdo en que la PJ no solo ejecuta actos lícitos o persigue fines legales sino también propósitos delictivos, que han de convertirlas en verdaderas organizaciones delincuenciales, ahora en los entornos digitales y de alcance trasnacional (SÁNCHEZ 2006). En este sentido, la influencia y presión internacionales ejercidas por países que se han visto afectados de alguna manera por las conductas delictivas de compañías trasnacionales[8],

[6] Según Air Force Doctrine Publication 3-12, Cyberspace Operations, el cyberespacio es considerado como «a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers».

[7] Considerada como un fenómeno que va el alza y que refiere a la ejecución de conductas antijurídicas mediante el uso de TIC o contra estas, que se encuentra tipificadas como delitos en la ley penal que atentan contra bienes jurídicos protegidos y afectan directamente a personas naturales como personas jurídicas (MIRÓ 2012, FERNÁNDEZ 2019).

[8] Sobre conductas referidas a sobornos, contaminación ambiental y corrupción entre otros. Notorios han sido algunos casos como los de Volkswagen, Siemens, Parmalat y otros.

impulsó la tendencia de penalizar a las organizaciones como entes morales o colectivos.

En el «postinternet»[9] (OLSON, 2008), entendido como el fenómeno de interrelación social desde el ámbito físico con transición al ciberespacio digital (JAISHANKAR 2012), que constituye la expresión de un nuevo paradigma de conducta, como modalidad normal para la realización de la mayoría de las actividades humanas y de las organizaciones, se consolida la deslocalización como factor hegemónico en esas tareas y relaciones vivas que favorece la delincuencia particularmente la empresarial. Este fenómeno comprende de forma intrínseca los primeros visos que impulsaría la evolución o expansión del derecho penal[10], que demanda del Estado considerar la situación existente y diseñar políticas criminales para dar respuesta y desalentar a las personas jurídicas de incurrir en esas conductas delictivas; además, tomar medidas para prevenir y controlar estas conductas disvaliosas, puesto que a pesar de que los órganos de administración y de decisión se renovaban cada cierto período, se seguían presentando actos delictivos a lo largo de los años, lo que era una forma de hacer negocios o, más bien, una política corporativa, a partir de la cual era muy difícil identificar al responsable de esas prácticas disvaliosas (CANCIO MELIÁ en MIRO, 2006), por lo que debía erradicarse o al menos perseguirse; y para ello también era urgente lograr que las empresas trabajaran en la prevención a lo interno de la organización, incorporando la obligación legal de hacerlo.

La caducidad de los dogmas y principios penales tradicionales centrados en la persona física como sujeto activo con capacidad de delinquir (MIRÓ, 2006) existentes hasta entonces, quedaron expuestos en esta crisis generada por la delincuencia empresarial, que para muchos países se hacía insostenible pues es evidente que cada vez más perdían vigencia por ineficacia, lo que por supuesto generó un debate de dogmática penal sobre la responsabilidad penal de las personas jurídicas, que impulsó reformas en la legislación de varios países para incorporar normas penales y, en otras, normas administrativas, así como cambios en su política criminal como medidas dirigidas a castigar o sancionar los hechos punibles cometidos por los entes colectivos o morales.

[9] Término acuñado por Marisa Olson en 2008 que surgió de un debate sobre el internet art, alusivo a las nuevas formas de relacionarse con internet luego de su aparición seguida de las TIC, y el cambio de paradigmas en todos los aspectos de la humanidad incluyendo el arte.

[10] Para profundizar el tema de la expansión del derecho penal, véase Jesús-María Silva Sánchez en Expansión del Derecho Penal, referido en la bibliografía.

2.2. Acercamiento a la teorización sobre la responsabilidad penal de la persona jurídica

Aunque entrar de lleno a explicar de forma exhaustiva cada una de las teorías excedería el propósito del presente trabajo de fin de máster, una referencia breve de algunas posturas abundaría en un acercamiento a las reflexiones y criterios como antecedentes necesarios para comprender la evolución de la doctrina jurídica sobre el tema de la responsabilidad penal de la persona jurídica. Así, encontramos las siguientes:

2.2.1. Teoría de la ficción

Su exponente es SAVIGNY (1840)[11]. Defiende que las únicas personas reales son las naturales y solo éstas pueden cometer delitos, pues los entes morales no tienen consciencia ni voluntad, elementos esenciales de la imputabilidad. En este sentido, de existir la conducta criminal de la empresa debe castigarse en la persona física, por considerar que aquella carece de las dos condiciones que son propias del hombre. Asimismo, el concepto de «persona» es equivalente al de «persona natural», al de «individuo», es decir, el ser humano, excluyente de las personas jurídicas, entes colectivos o de derecho.

2.2.2. Teoría de la voluntad legal

Sostiene que precisamente por cuanto la persona jurídica carece de voluntad natural la ley le asigna una voluntad legal, por lo que puede incurrir en contravenciones administrativas, pero no puede cometer delitos porque si bien no son ficciones sí son consideradas abstracciones carentes de voluntad natural (Teoría de MICHOUD). La PJ existe cuando hay una unidad jurídica que reúne el interés de varias personas naturales para lograr los objetivos comunes conforme al derecho (Teoría de FERRARA).

2.2.3. Teoría de la realidad

Parte de la existencia real de la persona jurídica como sujeto de derecho igual que la persona natural. Ambas son personas reales y reconocidas por los ordenamientos jurídicos. Sostiene que no hay correlación entre el concepto de persona y el de hombre por cuanto no son coincidentes. Así «persona» es un sujeto de derecho y éste como tal, puede ser: individual,

[11] Teoría publicada en su obra «Tratado de Derecho Romano» en 1840 (GUERRA 2005, ESTEPA, 2012).

en el caso del ser humano, por una parte; y, por la otra, plural o social, que son los entes colectivos, también llamados morales, en todas las formas de asociación que tienen fines y objetivos propios con capacidad de adquirir derechos y obligaciones (Teoría de HAURIOU). En general, la teoría de la realidad sugiere tener en cuenta que las personas pertenecen, unas al contexto del derecho privado (civil) y otras al derecho público, en el cual se ubica el derecho penal, son pues personas reales de derecho privado o público sean individuales o colectivas y no meras ficciones; en otras palabras, las personas jurídicas son organismos vivos compuestos por varios individuos (Teoría de GIERKE); y, como entes colectivos, tienen voluntad propia de querer hacer y la potestad de lograr sus objetivos sociales, que es diferente de la voluntad y potestad de cada individuo (Teoría de ZITELMAN). A partir de estas ideas la persona jurídica sí tiene la capacidad de delinquir, postulado de la Teoría de BESELER seguido de WEISKE, DERNBURG y otros; (GUERRA 2005, ESTEPA 2012).

2.3. Otros aspectos controvertidos: ¿Cómo se atribuye e imputa la responsabilidad penal de la persona jurídica? ¿Cuál es la naturaleza de la sanción?

Puede decirse que, entre otros, son tres los ejes más polémicos entorno a la RPPJ que la doctrina ha abordado para sustentar la aplicación de la sanción penal a la persona jurídica:

2.3.1. Modelo de atribución de la responsabilidad penal de la persona jurídica

Atiende al criterio de dependencia a partir del cual se determina la RPPJ con relación a la RPPN. Se ubican varios sistemas: (i) Aquel en el que **la responsabilidad penal de la organización es atribuida de forma subsidiaria**, es decir, cuando sea imposible identificar o imputar a la PN (sujeto activo) la conducta delictiva, como condición *sine qua non.* Es el caso del código penal suizo. Se le cuestiona que esta modalidad interfiera en la eficacia de las políticas criminales,[12] porque puede promover la impunidad de la PJ en casos de «actitud criminal de grupo» (SCHÜNEMANN 1979)[13], mediante la práctica de escogencia selectiva de

[12] Véase SILVA SÁNCHEZ (2001), p. 319 y ss., para profundizar sobre los inconvenientes que presenta el modelo de atribución subsidiaria de responsabilidad penal de la PJ.
[13] SCHÜNEMANN (1979) citado por MANSDÖRFE 2007 p. 4.

personas para los cargos directivos para que sean éstas quienes, llegado el caso, asuman la responsabilidad penal e impedir de esta forma que se sancione a la PJ. (ii) El modelo de **atribución directa y cumulativa** de la RPPJ, también denominado **modelo vicarial**. Bajo esta modalidad, la organización siempre será directamente responsable cuando las personas naturales titulares de los órganos de administración o representantes actuando como tales incurran en la comisión de un delito por acción u omisión. Estados Unidos, Francia, España en el Código de 2010 y Reino Unido acogen el sistema vicarial de atribución de responsabilidad penal[14]. (iii) El modelo **ecléctico** de atribución de la RPPJ, conocido como **modelo mixto** por la combinación del modelo de atribución de responsabilidad directa y del vicarial. Bajo este esquema, la PJ es directamente responsable tanto por acción como por omisión de los delitos que cometiere en el desarrollo de su actividad, con sus recursos y en su beneficio, con independencia de la responsabilidad penal de las personas naturales que actuaron en su nombre y representación, como administradores, empleados o directores por sus conductas antijurídicas y culpables en ejercicio de sus funciones o si efectivamente son identificadas e imputables; y también por la actuación u omisión conjunta con ellas.

2.3.2. Modelo de imputación de la responsabilidad penal de la persona jurídica

Siguiendo a ROBLES PLANAS (2006) se identifican dos modelos de imputación de la responsabilidad de la persona jurídica con relación a quién ejecuta el hecho delictivo, que permiten la imposición de la consecuencia jurídica por la ejecución de una conducta antijurídica y culpable tipificada como delito. Entre ellos se ubican: (i) El modelo de **imputación por hecho ajeno**, que consiste en que se imputa a la persona jurídica la responsabilidad penal de la persona natural, cuando ésta actúa como órgano de aquella, esto es, se imputa la responsabilidad por la comisión de hechos que no son propios sino ajenos. Esta modalidad ha sido muy cuestionada porque sugiere la imputación de la responsabilidad por la conducta delictiva de otra persona. (ii) El modelo de **imputación por hechos propios,** también llamado de autorresponsabilidad pura, de culpabilidad o de responsabilidad originaria de la PJ. Se basa en que la PJ responde directamente por su propia conducta antijurídica y culpable, aunque acepta que, una PN actuando como administrador, empleado o directivo, haya ejecutado una acción delictiva en nombre y representación de la PJ, con sus recursos y en beneficio de ésta,

[14] NIETO (2016) citado por FERNÁNDEZ y CHANJAN (2016, p.5)

solo sería responsable penalmente cuando realice una acción propia tipificada como delito. En este modelo, ese hecho propio del ente colectivo puede manifestarse como un defecto u omisión de organización o de una precaria cultura corporativa, de otro modo puede ser un delito societario (DÍEZ RIPOLLE 2012)[15], pero siempre de hechos que dependen directamente de la propia PJ. Este modelo tiene más aceptación entre la doctrina, pues resulta la consecuencia penal por la conducta ilícita propia de la PJ (LAMPE 1994, HEINE 1995, GÓMEZ-JARA DÍEZ 2005).

2.3.3. Naturaleza de la sanción

El debate sobre el tipo de sanción a imponer se mantiene activo en aras de identificar si la sanción que se aplica por un hecho punible, cometido por la empresa, es de naturaleza penal o administrativa. Aunque podría parecer indiscutible, la controversia se plantea entre quienes parten del supuesto de que la PJ puede ser responsable penalmente por sus delitos y ser castigada con una pena no corporal y quienes sostienen que no existe la RPPJ y no puede ser sancionada penalmente la PJ porque no se le pueden aplicar las penas corporales por razones evidentes y, por tanto, conciben que sólo le sería aplicable una sanción en vía administrativa (RODRÍGUEZ 2011), porque se trata del incumplimiento de una obligación de carácter administrativo contemplada en las leyes y normas sub legales que imponen deberes y obligaciones a las organizaciones, caso en el cual, serían los órganos u entidades de la Administración Pública, en cualesquiera de sus niveles político territoriales, centralizados o descentralizados, los rectores autorizados legalmente para imponer ese tipo de sanciones en el marco de un proceso administrativo. En todo caso, es claro que existen penas corporales y no corporales y las sanciones administrativas son totalmente autónomas de las penales, tienen un origen diferente y procedimientos de diferente naturaleza, que no deben confundirse. De allí que estos no son criterios contundentes para negar la existencia de la RPPJ.

2.4. Un debate doctrinario vigente en Venezuela

Durante varias décadas la responsabilidad penal de la persona jurídica también ha sido un

[15] DÍEZ RIPOLLE (2012) citado en FERNÁNDEZ y CHANJAL 2016, p. 6)

tema polémico en nuestro país, en el seno del cual han florecido varias posturas doctrinarias que intentan explicar su factibilidad o su inexistencia bajo el prisma de la dogmática penal que imperó hegemónicamente hasta hace menos de un siglo, cuando comenzó a ser insuficiente para sostener el razonamiento y justificación de la aplicación de una pena a la PJ producto de su actividad delictiva ejecutada por sus representantes u órganos de administración, actuando en nombre, en beneficio y con recursos de aquella, lo que implicaría su obligación de soportar el castigo asignado por la ley, pues de lo contrario estaría quedando impune a pesar de ser un sujeto de derecho y obligaciones.

Las previsiones del Código penal venezolano (2005), históricamente se han interpretado en apego a los postulados de la teoría de la ficción de SAVIGNY (1840), a partir de la cual las personas jurídicas no son personas reales sino ficticias, una creación del derecho, de allí que no podrían admitirse como sujetos activos de delitos, sino exclusivamente a la PN, sea nacional o extranjera que, en ese caso, actúe en nombre o representación de aquella. No obstante, frente a la innegable incidencia de la delincuencia corporativa nacional y trasnacional por delitos penales económicos[16] cometidos en perjuicio de la sociedad, persiste el interés de la doctrina científica patria entorno a la capacidad de las personas jurídicas para delinquir y la consecuente responsabilidad penal, aunque no menos cierto es que la doctrina nacional es mayoritaria en sostener los postulados de la teoría de la ficción respecto de la responsabilidad penal y la capacidad de las personas de delinquir, perspectiva bajo la cual considera que los actos de la PJ son los previstos como objetivos y fines de su organización, de los cuales siembre están excluidos la comisión de delitos, al menos en sus estatutos de creación, razón que las excluye de la categoría de sujetos activos de delitos (MENDOZA 1985, RODRÍGUEZ 2019).

Ahora bien, el Código penal venezolano (2005) [17] no prevé expresamente la RPPJ como tal. Sin embargo, también es cierto que al establecer en el artículo 3, que «**todo el que cometa un delito** o una falta en el espacio geográfico de la República, **será penado con arreglo a la ley**

[16] Recientemente el caso de Odebrecht en Latinoamérica.
[17] En 1897, fue adoptado en Venezuela el Código de Zanardelli traducido del italiano, justo durante el gobierno de Joaquín Crespo. Ese código fue derogado en 1904 y sustituido por el Código español, luego en el gobierno de Juan Vicente Gómez, el Código de Zanardelli fue nuevamente adoptado y se mantuvo hasta sufrir insustanciales reformas en 1926,1964, 2000 y 2005.

venezolana», esto es, a las leyes especiales, se trata de una cláusula abierta que abarca a cualquier sujeto activo, sea un individuo como PN o una empresa como PJ. De esta manera, el legislador mantuvo una postura neutra al utilizar la expresión «todo el que...» para abarcar a todas las personas, sujetos de derecho, que pueden llegar a ser sujetos activos de un delito, sin que el intérprete pueda excluir a la persona jurídica, a pesar de que es claro que dicho código fue creado bajo el imperio del principio «*societas delinquere non potest*».

Así, el artículo 4 *ejusdem* vendría a confirmar que la norma contempla un sentido amplio del cual no se desprende delimitación o exclusión alguna, al referirse a los sujetos a enjuiciamiento enumerados en dieciséis supuestos, en los cuales expresamente no precisa si se trata de personas naturales o jurídicas. En este sentido, se observa que, por una parte, se utiliza el criterio de la nacionalidad, con base en el cual señala a «los venezolanos» y a «los extranjeros»; además del criterio de la función que desempeña el sujeto, al agregar a: «los empleados diplomáticos», «capitanes de buque», «patronos» y «oficiales del ejército». Es por ello por lo que, aun haciendo una interpretación exegética de las normas del CP (2005), no puede excluirse la responsabilidad penal de la persona jurídica.

De allí que varias posturas, en uno y otro sentido, podrían tener cabida pues el CP (2005) no es expreso sobre este punto, por lo que indefectiblemente no podría identificarse *at initio* un sistema de atribución de responsabilidad penal a la PJ sin haber asumido antes una posición al respecto. Sin embargo, la doctrina venezolana mayoritaria se inscribe en la teoría de la ficción, al considerar que sólo las personas naturales tienen la capacidad de delinquir y que no existe la RPPJ, conforme al principio «*societas delinquere non potest*» (ARTEAGA SÁNCHEZ 2012, RODRÍGUEZ 2011).

Ahora bien, en el Título II, De las penas, el artículo 8 del Código Penal (2005) señala expresamente que **las penas se dividen principalmente en corporales y no corporales**. Las primeras de las nombradas se aplican exclusivamente a la PN porque su tipo afecta el derecho a la libertad de ésta, como es el caso de la privación de la libertad por condena a prisión o presidio, que es la sanción penal por excelencia. A diferencia de éstas, las penas no corporales, son de diversa índole y resultan aplicables tanto a personas naturales como a las jurídicas, pues establecen limitaciones a otros derechos del condenado, entre las cuales destacan, para los efectos que nos interesan, las penas pecuniarias, las suspensiones de licencias y las que consisten en el pago de una cantidad de dinero fijada por la ley, como es el caso de las multas.

A pesar de la naturaleza de ambos tipos de penas, el elemento común es que ambas se aplican como sanción por conductas tipificadas como delitos en la ley y por intermedio del juez en un proceso penal, cuando se ha comprobado la culpabilidad de la persona acusada.

El Código penal (2005) no determina si se refiere a una PN o a una PJ, en tanto que al utilizar la palabra "persona", esto es, un sustantivo sin calificativo, no determina si sólo se refiere a un individuo o a la PJ, o más bien y con todo sentido e intención es así para abarcar tanto a las personas naturales y a las jurídicas también, ambos sujetos de derechos y obligaciones que no pueden escapar del cumplimiento de la ley ni de la responsabilidad penal si llegaren a cometer algún delito y pueden ser sancionadas penalmente con una pena no corporal.

Al decantarse el legislador por el uso de términos o expresiones indeterminadas como técnica legislativa para dar mayor vigencia a las normas del código penal e imprimirle proyección futura, nos conduce a afirmar que, la intención es abarcar a la PJ como sujeto activo del derecho penal que puede ser sancionada con una pena no corporal; que aunque en el código no se encuentra ningún título destinado especialmente a la RPPJ, también es cierto que no lo prohíbe y, por el contrario, de esta forma asegura la armonización de éste, por vía del artículo 7 (CP 2005) con las previsiones legales especiales que sí prevén la responsabilidad penal directa de la PJ como es el caso de la LECDI (2001) que es anterior al código en comento sancionado en 2005, el cual utiliza en todo momento expresiones genéricas al referirse a los sujetos activos que les dan cabida. A partir de esas precisiones es forzado señalar que la multa aplicada en un proceso penal por el juez como sanción a la comisión de un delito es de naturaleza penal y no puede confundirse con la sanción administrativa de multa, solo por ser de tipo pecuniario; puesto que, en este último caso, la sanción es la consecuencia de una infracción o un ilícito de carácter administrativo que es aplicada en el marco de un procedimiento administrativo sustanciado por el órgano de la Administración Pública competente y afín a la norma administrativa que ha sido infringida.

Empero, conviene destacar que si bien el CP (2005) no es expreso sobre el tema, el legislador sí ha previsto la RPPJ en varias leyes especiales, entre las cuales destaca particularmente la LECDI (2001) que prevé la responsabilidad penal de las personas jurídicas (art. 5 LECDI) que se abordará más adelante.

2.5. Referencias en el Derecho Comparado

La RPPJ se ha impuesto en diferentes regiones. Al respecto, Gómez-Jara Díez (2005) refiere la pluralidad de legislaciones de varios grupos de países que la contemplan. Así identifica a Estados Unidos e Inglaterra como países que tradicionalmente han previsto la responsabilidad penal de los entes colectivos en sus legislaciones; a quienes posteriormente se agregaron Dinamarca y Holanda. No sin debates y detractores, **en Europa** la legislación de la mayoría de los países acoge la responsabilidad penal de la PJ desde un sistema vicarial[18], por delitos cometidos en su nombre y beneficio, como es el caso de España (CPE 2015). Sin embargo, la actualización de las políticas criminales y legislaciones sigue siendo una necesidad imperiosa para combatir la delincuencia empresarial (MIRÓ 2006) en aquellos países de la UE donde todavía se discute sobre su factibilidad. En algunos países europeos se encuentra que las sanciones que se imponen a la PJ son de naturaleza esencialmente administrativas, como consecuencia de «ilícitos administrativos», en este grupo se ubican las legislaciones de Portugal y Alemania[19] que no prevén la sanción penal por la responsabilidad penal autónoma de los entes colectivos sino sanciones administrativas, en el caso alemán, conforme a la Sección 30 de la OWiG (Gesetz über Ordnungswidrigkeiten)[20], esto es, la Ley de infracciones administrativas; en este sentido, las penas son impuestas a la persona natural sólo por la comisión de delitos cometidos cuando actúan con el carácter de representantes y en nombre de la empresa[21].

---

[18] Esto refiere a la adopción de un sistema atributivo de responsabilidad dual, por una parte, las personas naturales que componen el órgano de decisión son responsables y también las jurídicas por no haber hecho lo necesario para prevenir y controlar hechos delictivos mediante políticas.

[19] Aunque en Alemania se presentó un proyecto de Ley de sanciones a las corporaciones, que contempla la RPPJ y la imposición de una sanción penal de multas más elevadas en casos de delitos que supongan el incumplimiento de deberes de la empresa o el enriquecimiento de ésta, por haber omitido con intención, por imprudencia o negligencia las medidas de vigilancia o control que pudieran haber evitado dicho delito. De aprobarse esa ley, podría cambiar el sistema de sanción administrativa como consecuencia de ilícitos administrativos que ha tenido hasta ahora (TEJADA PLANA 2021). Mayor información en: https://gobercom.com/alemania-la-responsabilidad-penal-de-las-personas-juridicas-de-nuevo-a-la-palestra/. Ver propuesta de ley en: https://www.steuerberater-center.de/media/VerSanG_RefE.pdf

[20] Gesetz über Ordnungswidrigkeiten (OWiG) neugefasst durch B. v. 19.02.1987 BGBl. I S. 602; zuletzt geändert durch Artikel 31 G. v. 05.10.2021 BGBl. I S. 4607 Geltung ab 01.01.1975; FNA: 454-1. Traducción: Ley de Infranciones Administrativas (OWiG) revisada por B. v. Gaceta de Leyes Federales de 19 de febrero de 1987, pág.602; modificado por última vez por el artículo 31 G. v. 05.10.2021, Boletín de Leyes Federales I p. 4607 válido desde el 01.01.1975; FNA: 454-1.

[21] A pesar de la postura firme que la doctrina alemana ha sostenido sobre la inexistencia de la responsabilidad penal de los entes colectivos, a comienzos de este año 2021 fue presentado un proyecto de ley que prevé la RPPJ,

Como se indicó España y también Francia acogen el sistema vicarial, puesto que la legislación prevé la responsabilidad penal directa y cumulativa de la PJ, con la particular exclusión del Estado, por delitos los cometidos (arts. 31 bis y 31 ter del CPE, 2015 y el art. 121.2 del CPF, 2005) y la consecuente imposición de penas[22], así como la responsabilidad penal de las personas naturales implicados en los hechos como autores o cómplices[23]. La responsabilidad penal de los entes morales no descarta otras como la administrativa, que deriva de la infracción de obligaciones de naturaleza esencialmente administrativa; o bien la civil, que surge por previsión e incumplimiento de la norma civil.

En **América Latina,** los códigos penales de algunos países como Argentina, Colombia y Chile contienen previsiones sobre la responsabilidad penal de las organizaciones como entidades colectivas. Así, encontramos que:

- En Argentina la Ley 27.401 de 1 de diciembre de 2017 del Código Penal, prevé la responsabilidad penal de los entes morales, en los delitos de cohecho y tráfico de influencias nacional y transnacional (artículos 258 y 258 bis), negocios incompatibles (artículo 265), concusión (artículo 268), enriquecimiento ilícito (artículos 268.1 y 268.2) y balances e informes falsos (artículo 300 bis).
- En Colombia, su código penal (2000)[24] no contempla la responsabilidad penal directa o autónoma de la PJ, por el contrario, prevé una cláusula de actuar en nombre de otro, que es el caso típico del representante que actúa en nombre de aquella; sin embargo, no se exime de imponer medidas que afectan directamente a la PJ frente a hechos delictivos, lo que resulta un contrasentido, cuestionado por la doctrina (VEGA DUEÑAS 2021). En este sentido, PETRO, MOSQUERA Y TORRES (2014), al referirse al tema sostienen que: «En la actualidad, si bien el código penal colombiano en la parte general no contempla la posibilidad de castigar de forma directa a la persona jurídica a través de las cuales se desarrollen comportamientos delictivos,

que representa un cambio radical como respuesta a la delincuencia empresarial. Para acceder al proyecto de ley ir a: https://www.steuerberater-center.de/media/VerSanG_RefE.pdf

[22] Que pueden afectar derechos pecuniarios o de otra índole, como de multas, disolución de la PJ, suspensión de actividades, clausura de locales, prohibición de realizar actividades, prohibición de contratar con el sector público y de obtener subvenciones, intervención judicial, entre otras (artículo 33.7 CPE, 2015).

[23] Por ley N° 2000-647 de 10 de julio de 2000, se incorporó al CPF, que la responsabilidad de las personas morales no excluye aquella de las personas físicas, autoras o cómplices de los mismos hechos, consolidándose el modelo vicarial.

[24] Diario Oficial No. 44097 del 24/07/2000 Poder Público – Rama Legislativa, LEY 599 de 2000 de julio 24.

ello en virtud de la cláusula del actuar por otro, contenida en el Artículo 29 *eiusdem*, existen otras disposiciones del ordenamiento jurídico penal, que resultaron para las personas jurídicas implicadas en delitos que pueden ser sancionadas con multas, la suspensión o disolución definitiva de su personalidad jurídica. Es así como los artículos 65 de la Ley 600 de 2000 (Congreso de la República de Colombia, 2000), 91 de la Ley 906 de 2004 (Congreso de la República de Colombia, 2004) y 34 de la Ley 1474 de 2011 (Congreso de la República de Colombia, 2011) incorporan en el ordenamiento jurídico penal colombiano las denominadas medidas accesorias, en las que se sanciona a la PJ por su "actuar"».

- En Chile, la Ley N° 20.393, prevé la responsabilidad penal de la persona jurídica independiente de la responsabilidad penal de la persona natural (artículo 5) tanto de derecho privado como a las empresas públicas (artículo 2) de cualquier tamaño, por la comisión de los delitos de lavado de dinero, financiamiento al terrorismo y soborno o cohecho activo de empleados públicos nacionales y extranjeros (artículo 1).

2.6. Previsiones legales en Venezuela

La dispersión de la legislación penal especial en Venezuela es un fenómeno marcado y concurrente que implica la creación de leyes penales especiales para cada materia, en cuerpos separados del CP (2005) en el cual, a pesar de ser reformado, no fueron incorporadas las normas especiales que cursan en aquellos cuerpos normativos. Así encontramos que la RPPJ está prevista en varias leyes especiales de naturaleza penal que contemplan varios tipos penales con sanciones corporales de penas de prisión para las personas naturales y penas no corporales, pecuniarias y de otro tipo para las personas jurídicas; sin embargo, se observa que en ellas fundamentalmente se imputa la RPPJ, por hecho ajeno, a las personas naturales que actúan en su representación, aunque no hay uniformidad en la posición del legislador sobre la RPPJ. Estas leyes especiales rigen en materia de: migración y extranjería (2004), delincuencia organizada y financiamiento al terrorismo (2012), ambiente (2012), precios justos (2013), prevención, condiciones y medio ambiente de trabajo (2005), telecomunicaciones (2010), mercado de valores (2010), estafa inmobiliaria (2012), sustancias, materiales y desechos peligrosos (2001), secuestro y extorsión (2009), drogas (2010) y corrupción (2014), entre otras.

2.7. Jurisprudencia del Tribunal Supremo de Justicia de Venezuela

La jurisprudencia del Tribunal Supremo de Justicia de Venezuela en Sala Constitucional y en Sala de Casación Penal, ha realizado escasos aportes en materia de RPPJ. Sin embargo, en las siguientes sentencias se observan breves referencias al tema con fundamentación diferente pero que apuntan a la existencia de la responsabilidad penal de la persona jurídica. A continuación, se citan los extractos pertinentes.

- SSC/TSJ Sentencia N° 834/2009 de 18 de junio, expediente N°03-0296: [25]

«La responsabilidad penal debe ser entendida -en su función social- como atribución de pena de acuerdo con los parámetros constitucionales de protección preventiva de bienes jurídicos. Reorientar el concepto de imputación en la teoría del delito para concluir que las personas jurídicas ostentan la capacidad de culpabilidad penal -imputabilidad-, puesto que la culpabilidad ya no se concibe como un juicio de reproche eminentemente personal sino como un juicio que - en tanto función social- protege preventivamente los bienes jurídicos. Aceptar lo contrario y aferrarse al principio tradicional *societas delinquere non potest* implicaría -frente a novedosas formas de criminalidad- dotar de impunidad a los entes colectivos y convertirlos así en gérmenes para la sociedad. A esa nueva dimensión de la responsabilidad penal apunta el Derecho Comunitario de la Unión Europea, que estipula la responsabilidad de las personas jurídicas, entendidas como una *unidad económica.* Así merece destacar las siguientes sentencias del Tribunal de la Comunidad Europea, recaídas en los casos: Christiani *& Nielsen del 18 de junio de 1969, Farbstoffe* del 24 de julio de 1969; *Johnson & Johnson* del 25 de noviembre de 1980; *Moet & Chandon* del 27 de noviembre de 1987; *AEG* del 6 de enero de 1982 y *Zinc Producer Group* del 6 de agosto de 1984. En cuanto al principio de intrascendencia de las penas debe precisarse que el mismo dispone que la pena no se transfiere, no comprende a terceros; de esta manera las penas son personales e intransferibles; excluyendo así la responsabilidad penal por acciones u omisiones de otros y hechos cometidos sin los presupuestos subjetivos de la responsabilidad penal; de allí que la Sala observa que la disposición normativa impugnada no consagra en su texto ni tampoco puede inferirse la imposición de penas a terceros ajenos a la actividad o servicio propio de las

[25] Para acceder al texto completo de la sentencia ir a: http://historico.tsj.gob.ve/decisiones/scon/junio/834-18609-2009-03-0296.HTML

telecomunicaciones, pues la sanción está destinada al prestador del servicio de telecomunicaciones una vez que se ha comprobado la infracción administrativa o penal según sea el caso».

- SSCP/TSJ Sentencia N° 240/2000, de 29 de febrero, Procter & Gamble de Venezuela, S.A.[26]

«… No puede negarse que las personas jurídicas tienen capacidad para realizar acciones jurídicamente relevantes. Y si se les considera susceptibles de ser sujetos activos de delitos, pese a que sus "actos" son discutibles en principio, por fuerza se les considerará dueñas de una reputación: si sus "actos" causan el efecto mayor de que se les pueda considerar "criminales", "a fortiori" podrán lograr el efecto menor y puramente pasivo de que se forje una reputación en torno a esos mismos actos. No es posible desconocer la capacidad de dichas personas jurídicas para "actuar" válidamente y en el marco de la ficción que les dio "vida" y dotó de "personalidad"; pero ese actuar guarda más relación con los hechos naturales o acontecimientos mecánicos propios del famoso y así denominado "acto acromático". Aun acogiendo la tesis organicista (que atribuía voluntad a las personas jurídicas) es forzoso reconocer que tal "voluntad" sería como la del autómata o como la energía que permite moverse a quienes duermen...».

2.8. Responsabilidad penal de la persona jurídica por ciberdelitos

En Venezuela el legislador se vio motivado a dictar la LECDI (2001) ante el escenario nacional de frecuentes actos de fraude y suplantación de identidad de tarjetahabientes, usuarios del sector bancario, para extraer dinero efectivo de los cajeros automáticos entre otras modalidades, aunado a la influencia internacional sobre la necesidad de dictar leyes que tipificaran penalmente este tipo de conductas para facilitar la persecución y la aplicación de una sanción persuasiva como política criminal tanto a las personas naturales como jurídicas involucradas en conductas antijurídicas y culpables, para proteger la propiedad, el patrimonio y los datos personales, como bienes jurídicos fundamentales que gozan de un gran valor para la sociedad y el derecho. De allí que resulta pertinente conocer el estado actual de la

[26] Para acceder al texto completo de la sentencia ir a: http://historico.tsj.gob.ve/decisiones/scp/febrero/240-290200-971971.html

ciberdelincuencia en Venezuela para abordar el estudio de esta legislación especial y comprender el alcance de los riesgos penales a los cuales pueden enfrentarse las personas jurídicas en su giro comercial y que de ocurrir podría causar un perjuicio económico y reputacional a la organización, por mencionar sólo algunos.

2.8.1. Incidencia de la ciberdelincuencia en Venezuela

En el estudio «Actividades rutinarias y cibervictimización en Venezuela» (RODRIGUEZ, ODUBER y MORA 2017) se expuso que las actividades ilícitas asociadas al ciberespacio en el país presentaban un patrón similar a los países de América Latina y el Caribe. Los referidos investigadores señalaron que la empresa Symantec en el 2013 identificó que el 4.2% de los ataques cibernéticos ocurridos en la región provenían de Venezuela. Por su parte, en 2015 el Sistema Nacional de Gestiones de Incidentes Telemáticos, publicó el Gráfico 1, donde se aprecia el crecimiento sostenido de los incidentes asociados a las TIC con un incremento del 2.220 % entre el 2008 y el 2014.

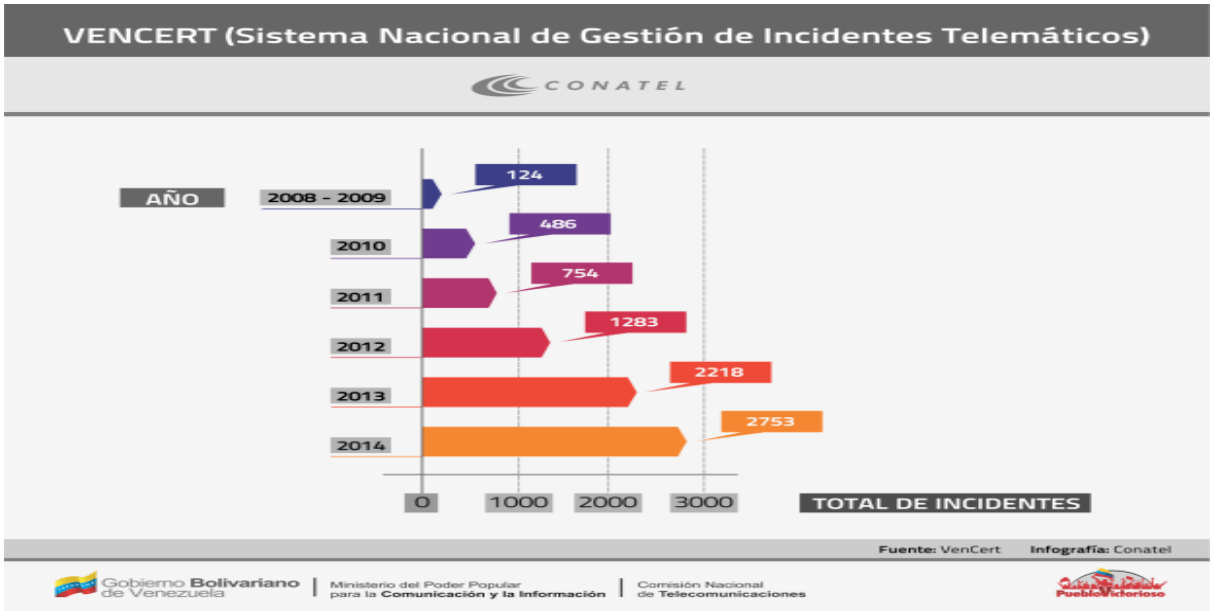


Gráfico 1. Incremento de los incidentes telemáticos en Venezuela 2008-2014
Fuente: VenCert

Igualmente, en el 2015 el laboratorio del antivirus ESET identificó una *bonet* en Latinoamérica denominada *liberpy* y Venezuela fue escogida por los cibercriminales como objetivo para su desarrollo delincuencial, de los 2.047 *bots*, 1.953 *bots* se encontraban en el país (RODRÍGUEZ,

et al 2017), este evento, no trascendió judicialmente, tampoco hubo respuesta gubernamental que permitiera alertar a la ciudadanía de los riesgos presentes en ese momento en el ciberespacio.

En 2017, Venezuela tuvo una tasa de incidencia de *malware* del 23.13% de las computadoras que disponían del antivirus PANDALABS y fue uno de los países más afectados por el phishing al contabilizar el 5% de los ataques sufridos en Latinoamérica y el Caribe (RODRÍGUEZ *et al* 2017). En el 2018, la División Contra Delitos Informáticos del CICPC, señaló la detención de 108 ciberdelincuentes (CICPC 2018), sin que esta información se pudiera relacionar con los responsables de la *bonet liberpy* u otras actividades de ciberdelincuencia realizadas en el país. En ese año, la conflictividad política reinante en el país se tradujo en diferentes ataques cibernéticos, la organización de derechos humanos Transparencia Venezuela, había denunciado que en contra de su página web se ejecutaron ataques DDoS, intrusión, sabotaje, robo de información, borrado de datos y, en esa oportunidad, el ataque se enfocó en eliminar un artículo intitulado «Venezuela la información en libertad condicional», el ciberdelincuente, dejó su firma «*Mister Spy Bot V3*» (FRONT LINE DEFENDERS 2018). De igual forma, para el 31 de julio de 2018, los portales de información «Armando.info» y «Crónica.uno», fueron objeto de ataques distribuidos de denegación de servicios (DDoS).

En febrero de 2019, se produjeron dos interrupciones del sistema eléctrico a nivel nacional, algunos medios de comunicación digital difundieron la hipótesis de que ese *Blackout* fue producto de un ataque cibernético contra el sistema SCADA, es decir, contra el control informático de la Central Hidroeléctrica Simón Bolívar ubicada a 576 kilómetros de Caracas, en el Estado Bolívar (CUBADEBATE 2019). El 21 de agosto de 2019, el presidente del Centro de Tecnologías de la Información (CNTI) denunció que Venezuela estaba bajo un ataque cibernético desmedido con el *malware* conocido como «Machete», en su opinión diseñado para el robo de la información del gobierno venezolano y estrategias militares de la Fuerza Armada Nacional Bolivariana (REINA 2019). Ahora bien, a nivel mundial en el 2020-2021, la prevalencia del fenómeno de la ciberdelincuencia respondió a la ecuación pandemia COVID-19 más la necesidad de producción, lo que incrementó la actividad digital y visualizó las vulnerabilidades del ciberespacio, fatídicamente, así como se extendió la pandemia, una ola sin precedentes de ciberdelincuencia siguió su estela (CONNER en SONICWALL 2021).

La situación global en el 2020 se agravó con los ciberataques y, en ese sentido, según el

National Institute of Standars and Technology (NIST) se identificaron 18.353 vulnerabilidades en el 2020 expuestas en el programa *Common Vulnerabilities and Exposures* (CVE)[27], superando en un 300% las vulnerabilidades identificadas en el quinquenio 2015-2019 (SONICWALL 2021). Por su parte, se señaló que el trabajo desde los lugares externos a la sede de la empresa e instituciones generó una superficie de ataque exponencialmente mayor en el ciberespacio, creando un incalculable número de vectores e infinitas oportunidades de disrupción para la comisión de cibercrímenes (SONICWALL 2021). También aprovecharon los ciberdelincuentes las aplicaciones de seguimiento para el COVID-19, documentos PDF asociados a la pandemia, en ambos vectores de ataque se incrustaron *malware*. Asimismo, se observó una tendencia clara en el 2021 del crecimiento en un 62% de los *ransomware* (SONICWALL 2021).

A la sazón, en el informe global de seguridad de noviembre de 2021, la empresa Kaspersky, identificó una reducción de los ataques a los nodos de acceso remoto, mientras que en el 2020 fue del 55.6% en el 2021 se redujo al 44.4%, tendencia a la baja que es relacionada con el levantamiento del confinamiento por la pandemia de COVID-2019 y el retorno al trabajo en las sedes empresariales e institucionales. En este orden, Kaspersky avizora para el 2022 que en toda Latinoamérica se consolidarán los ataques con troyanos bancarios sofisticados y el uso de los troyanos *infostealers* cuya funcionalidad es recopilar datos confidenciales de la computadora que ha sido comprometida para remitirlo a los ciberdelincuentes involucrados. De igual manera explica el informe de Kaspersky que los ataques con ransomware serán posiblemente en el 2022 mucho más selectivos y estratégicos debido a que, por temas culturales propios de la región, hay una alta resistencia de las ciber víctimas a ser persuadidas a pagar. En esta modalidad, los cibercriminales regionales tienden a vender los datos sustraídos a plataformas internacionales para su negociación con otros cibercriminales, quienes podrían en un fututo explotar la información con diferentes recursos. Por otro lado, para Kaspersky el 2022, será el año del retorno progresivo a la normalidad después de la pandemia del COVID-19 y llevará, muy probablemente, a que la ciberdelincuencia se enfoque en los puntos de pagos, puesto que los de última generación están habilitados para el uso con criptomonedas, pero adolecen de altos controles de seguridad.

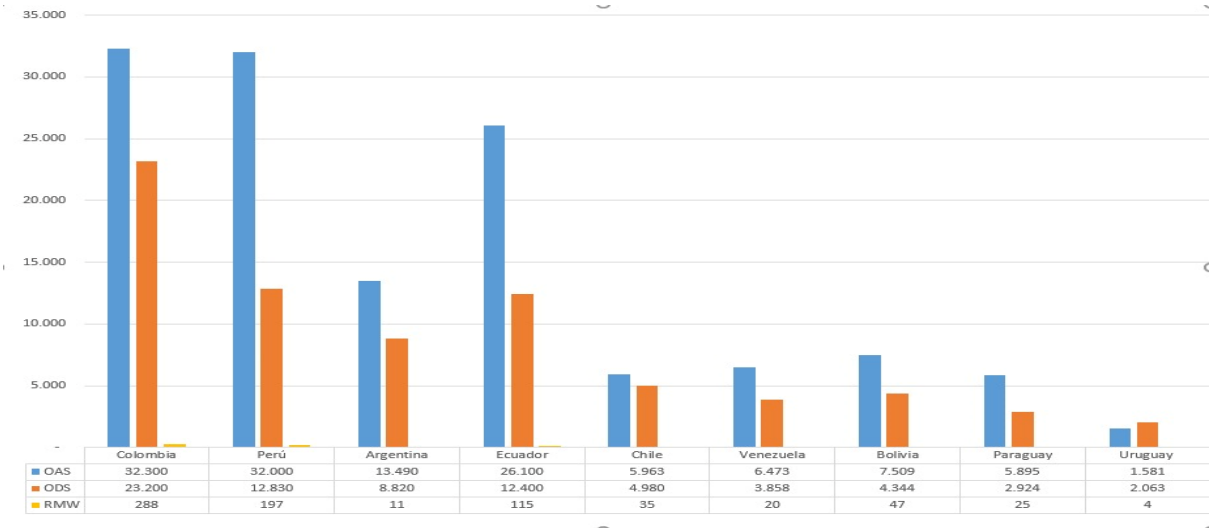
[27] Para conocer el Programa de vulnerabilidades comunes, véase la página web: www.cve.org

El recrudecimiento de los ataques dirigidos avanzados entre países, en especial a estructuras críticas entre países con gobiernos políticamente rivales en la región, aunado a esto, se buscará la legitimación de *trolls* en las redes sociales en períodos de elecciones, crisis sociales o en sucesos relevantes en la región, son otras de las previsiones de Kaspersky para el 2022. De igual manera señala que, para el próximo año, se intensificaran las estafas con las criptomonedas, dado que en las sociedades de Latinoamérica la tasa de analfabetismo sobre el uso y manejo de los criptoactivos es elevado; y, por último, la referida empresa considera altamente probable que se extenderán los ataques mediante el uso del código de QR, en el cual se incrustan *malware* o en las direcciones a páginas *web* que, aunados a la utilización de ingeniería social, así como técnicas de phishing, se pondrán en riesgo las credenciales de los usuarios de los códigos QR.

Bajo este panorama mundial, el Informe del Banco Interamericano de Desarrollo y la Organización de los Estados Americanos (2021) confirman que Latinoamérica y los países que conforman la región no son una excepción al fenómeno de la ciberdelincuencia; y que, en este sentido, la realidad vivida entre 2020-2021 evidenció las vulnerabilidades de su espacio digital, por eso la razón de implementar un modelo de madurez de la capacidad de ciberseguridad para las naciones con la finalidad de que los Estados miembros tengan herramientas defensivas ante las amenazas existentes en el ciberespacio.

Conforme a la visión anterior sobre el estado actual y futuro inmediato de la ciberdelincuencia en Latinoamérica, inexorablemente esta modalidad delictual se aprecia con mucha intensidad en Venezuela como en otros países de la región y, en efecto, en el Gráfico N°2, se exponen tres indicadores fundamentales con los que se construyen el concepto de ciberataques a los cuales está sometido un país determinado según Kaspersky, en este orden, tenemos: (i) *On-Access Scan* (OAS) el cual visibiliza la detección de malware cuando los usuarios realizan operaciones de abrir, copiar, ejecutar o guardar objetos provenientes del ciberespacio. (ii) *On Demand Scanner* (ODS) Se evidencia la detección de un programa maligno por solicitud del usuario en el software de antivirus. (iii) *Ransomware* (RMW) Muestra la detección de ransomware identificados por el software de antivirus. Desde esta perspectiva, entre los países que no superan los diez mil OAS (Bolivia, Chile, Uruguay Paraguay y Venezuela), Venezuela corresponde al segundo más atacado, con respecto a ODS ocupa el tercer lugar y con respecto a RMW corresponde al cuarto país con más ataques de ransomware.

Esta información valida indirectamente la observación de que, en Venezuela, la ciberdelincuencia presenta un patrón similar a los países de Latinoamérica (RODRIGUEZ *et al* 2017) y, de igual manera, las referencias periodísticas muestran un panorama similar a los países de la región sobre cibercriminalidad ante la cual deben estructurarse las definiciones de los ciber riesgos a que se enfrentan las personas jurídicas con asiento en el país, como se observa en el siguiente gráfico.



	Colombia	Perú	Argentina	Ecuador	Chile	Venezuela	Bolivia	Paraguay	Uruguay
OAS	32.300	32.000	13.490	26.100	5.963	6.473	7.509	5.895	1.581
ODS	23.200	12.830	8.820	12.400	4.980	3.858	4.344	2.924	2.063
RMW	288	197	11	115	35	20	47	25	4

Gráfico 2. Incidencia de ciberataques en Latinoamérica. Fuente: Kaspersky, 2021.

Ahora bien, con respecto a Venezuela, el informe *Digital 2021 Global Overview Report* detalló el contexto del país y su situación digital correspondiente al 2020 y 2021. En este sentido, destaca que el 79.6% de los venezolanos (28.57 millones de personas) poseen algún dispositivo asociado a las TIC como: móviles, *tablets* o *laptops* conectados a internet. De igual manera el 72% son usuarios de internet, con un aumento del 0.3% en el periodo 2020-2021 (KEMP 2021). De igual forma, se determinó que el 49% de los venezolanos mantienen un perfil activo en las redes sociales, con un incremento en el referido lapso del 16.7%. Refiere el estudio que, a pesar de la lentitud del internet, Venezuela se caracteriza por ser un mercado de redes sociales con una alta tasa del 96% de penetración en relación con Latinoamérica. Queda claro que las redes sociales son un vehículo expedito, eficiente y con gran potencial para el comercio electrónico que se hace exponencial en un mercado altamente atractivo para bienes y servicios, así como para el tráfico de criptoactivos.

Bajo el anterior panorama del ciberespacio en Venezuela, en el período 2020-2021, podemos

conocer las incidencias de la ciberdelincuencia por estadísticas parciales de empresas de ciberseguridad y no por datos oficiales. En este contexto, según Kaspersky para noviembre de 2021, Venezuela se ubicaba como el país número 59, víctima de ciberataques a nivel mundial y número 8 entre los 10 países más ciber atacados en Latinoamérica; por su parte, los ciberataques registraron un aumento del 29% en Venezuela (DIAZGRANADO 2021). Paralela y esporádicamente, los medios de comunicación publicaron noticias[28] de conductas delictuales como el acceso indebido, sabotaje o daño a sistemas, fraude informático, violación a la privacidad de la información de carácter personal, difusión de pornografía de niños y adolescentes, oferta engañosa, entre otras.

Ante esta realidad de acontecimientos relacionados con la ciberdelincuencia a nivel nacional, el CICPC en el mes de julio de 2021 exhortó a los ciudadanos a denunciar los delitos cibernéticos, en el marco de una alta prevalencia de ofertas engañosas, tipología prevista en el artículo 26 de la Ley especial contra los delitos informáticos, que utilizan como vector de ataque a las redes sociales y a las plataformas intermediarias de venta de productos y servicios (MercadoLibre y Marketplace, entre otras).

En este orden, los datos recabados por los autores expuestos en el Gráfico 3, se exponen las investigaciones policiales iniciadas en Caracas, entre el año 2019 y 2021. Es muy probable que la disminución de las investigaciones en el año 2021 se deba al retorno a las actividades laborales a las sedes empresariales, la apertura del comercio físico y a los casos de asesinatos de las víctimas que se han visto involucradas en ofertas engañosas en las plataformas intermediarias de venta de productos y servicios[29].

---

[28] Denuncias sobre ataques informáticos a PDVSA en donde se hablaba de robo de archivos electrónicos, información de cuentas en el exterior, en el marco del paro petrolero de 2002. http://oiprodat.com/2014/08/06/venezuela-frente-a-los-delitos-informaticos/ El CICPC, reveló un incremento en los delitos informáticos en Venezuela, y resaltó que uno de los más frecuentes es el que se registra ante el acceso indebido de la persona no autorizada a una cuenta digital y a los correos electrónicos. http://www.ultimasnoticias.com.ve/noticias/sucesos/cicpc-combate-delitos-cometidos-en-redes/ Advierten crecimiento de ciberdelitos durante la Pandemia https://www.vtv.gob.ve/advierten-crecimiento-ciberdelitos-pandemia/ Auge del fraude cibernético en Venezuela y otras tendencias delictivas https://eldiario.com/2020/07/05/auge-del-fraude-cibernetico-en-venezuela-y-otras-tendencias-delictivas/ Capturado Pederasta en Caracas https://www.diariosuspenso.com.ve/2020/12/capturado-pederasta-en-caracas-modus.html CICPC Cabimas desarticula banda de denominada "Luigi el Mago de las Redes" http://www.notiexpres24.com.ve/2018/11/cicpc-cabimas-desarticula-banda-de.html

[29] Véase la noticia: En la última semana de julio mataron a cinco personas que pretendían comprar vehículos publicados en Marketplace. https://www.todosahora.com/destacado/en-la-ultima-semana-de-julio-mataron-a-cinco-personas-que-pretendian-comprar-vehiculos-publicados-en-marketplace/

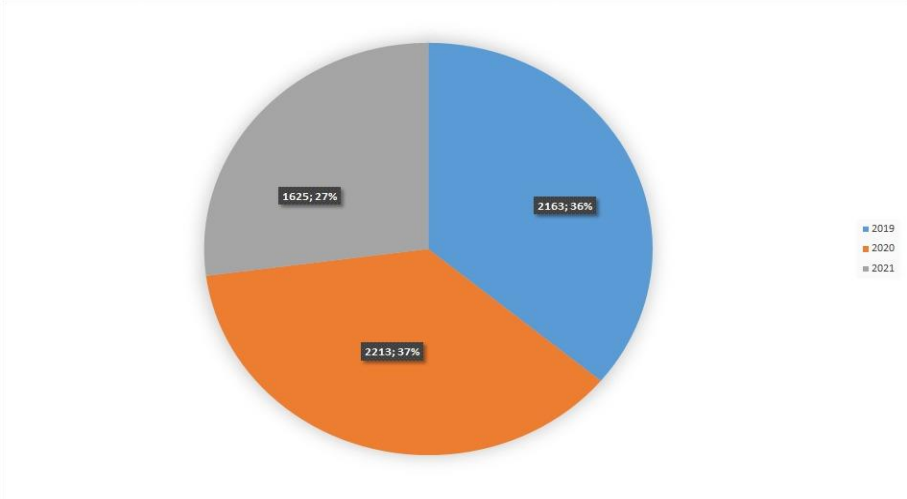


Gráfico 3. Investigaciones por ciberdelitos en Caracas 2019-2021
Adaptación Bautista y Perche, 2021.

En derivación podemos reafirmar, sin duda alguna, que Venezuela no se escapa de la incidencia de la ciberdelincuencia que impacta al mundo y a Latinoamérica; no obstante, poco se puede saber de la afectación a la economía, a la privacidad de las personas y a la seguridad de la información, ni de las tipologías delictuales más reiteradas así como de otras no contempladas en la LECDI (2001) que se estén suscitando por la ausencia de estadísticas oficiales que permitan el análisis y estudio criminológico, social y jurídico de la situación. Paralelamente en Venezuela, cada vez más, se transan operaciones con criptomonedas y, a la par, se ha desarrollado una estructura gubernamental representada por la Superintendencia Nacional de Criptoactivos y Actividades Conexas (SUNACRIP) cuya finalidad es organizar, planificar, regular, promover y coordinar la adopción y el uso del criptoactivo Petro[30], criptomonedas y activos digitales en el país, además, de evitar que los criptoactivos se conviertan en una forma de legitimación de capitales, financiamiento al terrorismo y financiamiento a propagación de armas de destrucción masiva.

No se puede dejar pasar por alto que los criptoactivos se han convertido en una válvula de escape de las sanciones internacionales impuestas al Gobierno de Venezuela, que ha afectado

[30] Creado mediante Decreto Constituyente de fecha 4 de abril de 2018, sobre criptoactivos y la criptomoneda soberana Petro, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 6.370 Extraordinario de 9 de abril de 2018.

de manera indiscriminada y desproporcionada a personas naturales y jurídicas, con domicilio en el país, que realizan actividades lícitas propias en el marco del desarrollo económico nacional no asociados al sector gubernamental. Pero a pesar de la ausencia de estadísticas y el empuje de los criptoactivos en el país, podemos inferir que la mayor tasa de incidentes relacionados con la ciberdelincuencia para el 2022 gravitará en relación con el comercio electrónico y, muy probablemente, por el uso de criptomonedas, esto sin desestimar la otra gama de tipologías delictuales asociadas a las TIC, dada la carencia de un programa de formación cultural de ciberseguridad para la ciudadanía.

2.9. Ley especial contra los delitos informáticos (LECDI, 2001)

Para finales del siglo XX en Venezuela, varios fenómenos criminológicos asociados a las TIC azotaban a la sociedad, entre otros, la clonación de tarjetas de crédito y de débito, el sabotaje informático, la falsificación de documentos electrónicos, la violación de los servicios de correo electrónico, así como su divulgación, venta de copias de software no originales al igual que cd de música. No menos escandaloso fue la venta de bases de datos de empresas privadas y públicas, como, por ejemplo, la base de datos de la empresa nacional de comunicaciones telefónicas en tiendas de economía informal ubicadas en calles y puentes de las principales ciudades del país (SEGUADMIN 2000). Este fenómeno criminológico asociados a las TIC, no conseguía consonancia desde la perspectiva judicial, la situación se había tornado frustrante para los órganos de investigación ya que si bien lograban identificar las vulnerabilidades, los vectores de ataques, las metodologías delincuenciales y en algunos casos a los ciberdelincuentes, no había una forma de procesarlos judicialmente por las conductas como «clonar» o «vaciar» los límites de una tarjeta de crédito que siempre estuvieron en disposición de sus titulares (DI TOTTO 2021).

Paralelamente a esta fenomenología criminológica, Venezuela se encontraba bajo la egida de una Asamblea Nacional Constituyente que, finalmente, promulgó la Constitución de la República Bolivariana de Venezuela de 1999, publicada en la Gaceta Oficial N° 5.453 de fecha 24 de marzo de 2000. Esta carta política, en su artículo 60 previó el mandato programático que la ley limitaría el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el ejercicio pleno de sus derechos, hasta hoy en nuestra opinión

el legislador está en deuda con la sociedad venezolana con respecto a este mandato. De igual manera, dos artículos más de la Constitución se refirieren a las TIC. Así, el artículo 108 constitucional, estableció la garantía estatal de crear redes informáticas con la finalidad de permitir el acceso universal a la información, así como, la aplicación de las nuevas tecnologías en los centros educativos y, el artículo 110 *eiusdem*, que estableció el interés público en los servicios de información para el desarrollo económico, social y político del país, como también, para la seguridad y soberanía nacional. Así las cosas, a la LECDI (2001) le antecedieron el Decreto Nº 825/2000 de 10 de mayo de 2000, mediante el cual se declaró el acceso y el uso de Internet como política prioritaria para el desarrollo cultural, económico, social y político de Venezuela; la Ley orgánica de ciencia y tecnología e innovación (2001); y, la Ley de mensaje de datos y firmas electrónicas (2001), cuyo objeto normativo es otorgar y reconocer eficacia y valor jurídico a la firma electrónica, al mensaje de datos y a toda información inteligible en formato electrónico.

2.9.1. Estructura de la Ley especial contra los delitos informáticos (2001)

La LECDI (2001) consta de treinta y tres artículos distribuidos en cuatro títulos: el **primer título**, contiene las disposiciones generales, objeto de la ley, definiciones, la extraterritorialidad, las sanciones y la responsabilidad de las personas jurídicas. En el **segundo título** se tipifican las conductas delictuales y las penas a imponer, subclasificando las tipologías en: (i) Delitos contra los sistemas que utilizan tecnologías de información, (ii) Delitos contra la propiedad, (iii) Delitos contra la privacidad de las personas y de las comunicaciones, (iv) Delitos contra niños, niñas o adolescentes, (v) Delitos contra el orden económico. El **tercer título** corresponde a las disposiciones comunes que regula las agravantes de las penas previstas en la ley, la agravante especial para las personas jurídicas, las penas accesorias, la divulgación de la sentencia condenatoria y la indemnización civil. Y, por último, el **cuarto título** referido a las disposiciones finales que estableció una *vacatio legis* de treinta (30) días y la derogación de aquellas disposiciones del ordenamiento penal que colidieran con este cuerpo normativo especial.

2.9.2. Objeto de la Ley especial contra los delitos informáticos (2001)

Esta ley fue concebida como una normativa previsiva y no reactiva, por eso en su redacción se tuvo presente que las definiciones fuesen funcionales, más no descriptivas, con la finalidad de procurar su intemporalidad (DI TOTTO 2021), lo que explicaría que luego de veinte años no haya sufrido ninguna reforma; en este sentido, al revisar el **objeto** de esta ley especial,

previsto en su artículo 1, observamos tres lineamientos fundamentales para prevenir y combatir la ciberdelincuencia: (i) Proteger los sistemas basados en tecnologías de la información, (ii) Prevenir y sancionar las conductas delictuales contra sistemas o componentes de las tecnologías, y (iii) Prevenir y sancionar las conductas que se sirvan de las tecnologías de la información para cometer dichos ilícitos.

En efecto, el legislador nacional en la exposición de motivos justificó la promulgación de la ley en «la necesidad de tipificar en nuestro derecho interno una serie de conductas que, realizadas con el auxilio de medios informáticos, electrónicos, telemáticos, para utilizar el vocablo más actual en la materia, medios que supongan el uso de tecnologías de información puedan afectar, entre otros bienes jurídicos, la propiedad, el derecho a la información, a la inviolabilidad del secreto, a la intimidad, al honor, todo ello en consideración a que el bien protegido puede desaparecer o ser seriamente afectado sin que el sistema usado como medio de comisión, sufra menoscabo alguno».

2.9.3. Responsabilidad penal de la persona jurídica por delitos informáticos

Además del hito innovador de tipificar tipologías delictuales asociadas a las TIC en Venezuela, la LECDI (2001) estableció por primera vez, bajo la vigencia de la Constitución (1999), **la responsabilidad penal directa de la persona jurídica** por la comisión de hechos delictuales en su seno. Siguiendo este orden, declarada la responsabilidad penal de los sujetos mencionados en el artículo 5 de LECDI (2001) en los siguientes términos: «Responsabilidad de las personas jurídicas. Cuando los delitos previstos en esta ley fuesen cometidos por los gerentes, administradores, directores o dependientes de una PJ, actuando en su nombre o representación, éstos responderán de acuerdo con su participación culpable. La PJ 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.»

2.9.3.1. Modelos de atribución e imputación de la responsabilidad penal de la persona jurídica

Del artículo 5 de la LECDI (2001) se observa que la RPPJ es incorporada expresamente en la ley contra conductas delictivas informáticas, en atención al **modelo de atribución de responsabilidad ecléctico**, en tanto que, por una parte, la responsabilidad penal de las

personas naturales cuando actúan en nombre o representación de la PJ en condición de gerentes, administradores, directores o dependientes deviene directamente por su participación antijurídica y culpable en los hechos delictivos; y, por la otra, también asigna directamente a la PJ la responsabilidad penal como sujeto activo por la conducta delictiva que ejecute cuando se de al menos uno de los tres supuestos normativos previstos en el primer aparte del referido artículo, que son los siguientes:

- **La existencia inequívoca de la decisión del órgano**, contentiva de la instrucción, planificación o ejecución del hecho delictual. La voluntad del órgano, según la teoría organicista, manifiesta la voluntad de la PJ por la autoridad y competencia asignada en los estatutos sociales. Esa es una intención volitiva colectiva, por regla mayoritaria, que se distingue de la voluntad de cada una de las personas naturales, individualmente considerada que eventualmente puede formar parte del órgano decisor y estar de acuerdo o no, lo que es irrelevante a menos que se deje constancia en actas de las personas en desacuerdo y si ello las relevaría de responsabilidad considerando que forman parte del órgano y en conjunto son una unidad; sin embargo, si la posición de desacuerdo es mayoría, igualmente sería la voluntad de la PJ. Esta condición, plantea ciertas complicaciones cuando se trata de decisiones que rayan en una conducta delictiva, pues resulta obvio que no se deje referencia escrita de la voluntad de cometer un delito, siempre se desdibujará la intención real, de manera que ello quedaría sujeto a la pertinencia de otros medios de prueba.

  Otro aspecto tiene que ver con la personalidad de quien se desempeña como órgano de decisión, si es una o un grupo de personas, verbigracia: una junta directiva, un consejo de administración, una dirección general o una presidencia, o, si en contraste, se trata de una o varias personas jurídicas, caso en el cual, aunque pareciera complicar el asunto, la decisión del órgano sigue siendo la expresión de la voluntad de la PJ en nombre de quien actúan y representan. En este punto es interesante tener en cuenta que en estructuras complejas es posible que los órganos de decisión estén compuestos por personas jurídicas incluso extranjeras y deslocalizadas y aunque sean representadas por personas jurídicas, la individualidad no manifiesta la voluntad del órgano de esa PJ que forma parte del órgano de otra PJ, a menos, que no sea colegiado, lo que no es frecuente en ese tipo de organizaciones.

- **La conducta debe ejecutarse en el ámbito de la actividad de la empresa**. Necesariamente, según los supuestos normativos del mencionado artículo 5 de la LECDI, la

decisión constitutiva, preparativa o ejecutiva del hecho punible debe desarrollarse en el ámbito de la actividad de la empresa, es decir, que tiene relación directa con el objeto social de la empresa prevista en sus estatutos sociales, así como las tareas y proyectos que ejecuta para la consecución de sus propósitos comerciales o sociales, que son del conocimiento público.

- **Con recursos de la empresa y para su beneficio o de interés preferente.** Por último, el *inter criminis* debe desarrollarse con recursos de la empresa, esto es, que haya sido financiado con recursos económicos de la PJ en la ejecución de esa actividad disvaliosa o que, de no ser así, se patentice que el órgano de dirección involucrado haya establecido un mecanismo de recuperación del financiamiento mediante una práctica ficticia con la PJ, como por ejemplo, que el gerente haya financiado con criptoactivos la acción delictual con la condición de que la asamblea de accionista le recompensara con un bono correspondiente al doble de lo invertido, como si fuera un reconocimiento por su gestión o, que el hecho delictuoso hubiese sido autorizado, planificado o ejecutado por el órgano de la PJ con un interés exclusivo o ventajoso, bien sea monetario o de índole competencial, reputacional o aquel que nazca o que se desprenda del entorno donde se desarrolla la empresa.

En este sentido, consideramos que la exigencia de la RPPJ por los delitos previstos en la LECDI (2001) no requiere la concurrencia de los supuestos normativos previstos en el primer aparte del artículo 5, en *el inter criminis*, para que sea posible la exigencia de la responsabilidad penal. En efecto, si el órgano de decisión no intervino, pero sí conoció formalmente de la actividad delictual y lo toleró, supone la posibilidad de exigencia de la responsabilidad penal, independientemente de que ello concurra o no con la conducta individual del gerente, administrador, director o dependiente involucrado.

2.9.3.2. Naturaleza penal de la sanción

La promulgación de la LECDI (2001) supuso un hecho trascendental legislativo en Venezuela que, en efecto, superó el principio *societas delinquere non potest* al prever la RPPJ y sustentar en su exposición de motivo lo siguiente: «y, por cuanto algunos de los hechos punibles previstos en el Proyecto pueden ser perpetrados por intermedio de una PJ o con el fin de que ésta reciba sus efectos o beneficios, se establecen los supuestos que podrían hacer procedente su responsabilidad, la cual, en todo caso, sólo podría ser de orden pecuniario.»

En este orden, es preciso señalar que, si bien se hace referencia a la «responsabilidad de la

persona jurídica» sin el calificativo «penal», resulta evidente que la LECDI (2001) es una ley estrictamente punitiva, que prevé tipos penales y como consecuencia directa de la comisión de los delitos contempla penas corporales para las personas naturales y penas no corporales para las personas jurídicas[31]. De allí que, de modo alguno podría interpretarse que se trata de una responsabilidad de otra naturaleza como la administrativa, ni que la sanción que impone el juez penal lo hace en funciones de una autoridad administrativa y, mucho menos, que el proceso y régimen recursivo sea el de la jurisdicción contenciosa administrativa y no el contenido en el Código orgánico procesal penal (2021) norma aplicable ineludiblemente en materia de delitos informáticos, sean cometidos por personas naturales o jurídicas.

Así las cosas, conforme el artículo 4 de la LECDI (2001) las sanciones aplicables son penas principales y accesorias, tal como prevé el artículo 11 del Código penal (2005). Asimismo, establece que la única pena principal que se le aplicará a la PJ por los delitos cometidos es la pena de multa, conforme al artículo 28 (LECDI 2001) y al artículo 7 del Código penal (2005). Esta sanción tendrá una agravante por la condición de PJ y es que la multa será impuesta por el doble del monto previsto para el delito cometido. Como penas accesorias aplicables a la PJ, el artículo 29 de la LECDI (2001) prevé: (i) En el ordinal 1 el comiso de equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualquier otro objeto que hayan sido utilizados en el seno de la PJ para la comisión de los delitos previstos en el artículo 10 de la LECDI (2001): posesión de equipos o prestación de servicios de sabotaje, y en el artículo 19 *eiusdem*: posesión de quipos para falsificaciones; (ii) En el ordinal 2 (art. 29 LECDI), el trabajo comunitario hasta por tres años en el caso de la comisión de los delitos de acceso indebido (art. 6 de la LECDI) y favorecimiento culposo del sabotaje o daño (art. 8 de la LECDI); (iii) En el ordinal 3 (art. 29 LECDI) se considera que solo sería aplicable la inhabilitación para el ejercicio de la industria por un período de tres años cuando la sanción principal haya sido cumplida, en este caso, debió haber quedado en los hechos probados por el órgano jurisdiccional que impuso la sanción que el delito fue cometido con abuso de la posición de acceso a data o información reservada o el conocimiento privilegiado de contraseñas, que en efecto se haya

[31] Véase el anexo A, en el texto de la LECDI, los artículos del 6 al 26, en ellos se prevé un sistema doble de pena (corporal y pecuniaria) para las personas naturales, esto es, una pena de prisión más una pena de multa. Por otra parte, para las personas jurídicas se prevé una pena pecuniaria doble, esto es, de multa por el doble del monto que corresponda al delito en cuestión.

honrado la multa con su pago ante el sistema bancario nacional; (iv) En cuanto a las penas accesorias del ordinal 4 (art. 29 LECDI), se considera que sólo sería aplicable a las personas jurídicas la suspensión del permiso, registro o autorización que le hayan sido expedido para desarrollar su objeto social, por un período de tres años cuando la sanción principal haya sido cumplida, si para la comisión del delito la PJ hubiese utilizado a una tercera persona.

2.9.4. Tipos penales en la Ley especial contra los delitos informáticos (2001)

El título segundo de la LECDI (2001), contempla veintiún tipos penales, con lo cual el legislador hace veinte años atrás buscó por un lado contener el auge delictual que imperaba para el 2001 y, en otro plano buscaba dejar las bases de cara al futuro y al avance tecnológico que le hizo avizorar que el fenómeno de la ciberdelincuencia no se detendría. Para la fecha de la promulgación de la LECDI (2001) en latinoamericana solo Chile y Perú disponían de textos legislativos sobre la materia. La Constitución (1999) y los preceptos constitucionales que se refieren a las TIC, son la base de este instrumento penal, que supuso un avance legislativo para hacer frente a la ciberdelincuencia del momento. Sin embargo, por alguna razón desconocida, la judicialización de hechos relacionados con los tipos penales previstos en la ley es hoy un misterio estadístico, empíricamente se sabe que la curva de delitos relacionados con las tarjetas de crédito y débito disminuyó drásticamente, no porque se contara con los tipos penales informáticos, sino porque la tecnología del chip incrustados en las tarjetas produjo un estándar de ciberseguridad que desalentó la comisión de las conductas delictuales que más azotaban a la población venezolana durante los años siguientes a la promulgación de la ley. No obstante, conocer hoy la magnitud del cibercrimen incluso las tipologías que pueden configurarse entorno a las organizaciones corporativas y su incidencia en la sociedad venezolana suponen que la mayoría de los tipos penales previstos en la LECDI (2001) permite hacerle frente a este fenómeno de la ciberdelincuencia para mitigar la impunidad.

Ahora bien, a partir de la construcción de la RPPJ por delitos informáticos prevista en el artículo 5 LECDI (2001), todos los tipos penales contemplados en el Titulo II de la ley, son susceptibles de ser cometidos por personas jurídicas, siempre que se materialice alguna de los supuestos previstos. Se debe advertir, que las construcciones de los contenidos normativos penales se inician en seis artículos con la palabra «persona» no diferenciando si es natural o jurídica, cinco artículos con el pronombre demostrativo masculino, femenino y neutro «aquel» y siete artículos con el pronombre relativo referido a personas.

De esta manera, la tipología de **acceso indebido** está prevista en el artículo 6 LECDI (2001). En este caso la acción típica corresponde a acceder, interceptar, interferir o usar un sistema que utilice tecnologías de información sin tener la debida autorización de su dueño o administrador, pero también quien teniendo unas credenciales determinadas en el sistema se extralimite en sus atribuciones para acceder, interceptar, interferir o usar más allá de lo autorizado. La pena base[1] aplicable a las personas jurídicas es de multa de diez a cincuenta unidades tributarias.

El **sabotaje o daño a sistemas** está contemplado en el artículo 7 LECDI (2001), en dicha norma penal se puede identificar que las acciones típicas atañen a la (i) Intención, destruir, dañar, modificar o realizar cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualesquiera de los componentes que lo conforman y (ii) Destruir, dañar, modificar o inutilizar la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualesquiera de sus componentes. La pena base aplicable a las personas jurídicas es de multa de cuatrocientas a ochocientas unidades tributarias y multa de quinientas a mil unidades tributarias si la acción típica se realiza mediante la creación, introducción o transmisión intencional de un «virus» o programa análogo. El favorecimiento culposo del sabotaje o daño, contenido en el artículo 8, tiene las siguientes acciones típicas: con imprudencia, negligencia o impericia, destruir, dañar, modificar o realizar cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualesquiera de los componentes que lo conforman, así como la acción típica: con imprudencia, negligencia o impericia, destruir, dañar, modificar o inutilizar la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualesquiera de sus componentes. La pena base aplicable a las personas jurídicas corresponderá a la multa calculada entre la mitad y dos tercios de la pena del artículo.

El **acceso indebido o sabotaje a sistemas protegidos**, está previsto en el artículo 9 (LECDI 2001) y la acción típica consiste en cometer los delitos tipificados en los artículos anteriores 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 o que contenga información personal o patrimonial de personas naturales o jurídicas. La pena base aplicable a las personas jurídicas corresponderá a la multa aumentada entre una tercera parte y la mitad cuando las acciones típicas de los

artículos 7 y 8 (LECDI 2001) cuando los sistemas de información estén destinados a funciones públicas o que las bases de datos contengan información patrimonial de personas naturales o jurídicas.

La **posesión de equipos o prestación de servicios de sabotaje**, contemplado en el artículo 10 (LECDI 2001), cuya acción típica es importar, fabricar, distribuir, vender o utilizar equipos, dispositivos o programas, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información; u ofrecer o prestar servicios destinados a cumplir los mismos fines. La pena base aplicable a las personas jurídicas es de multa de trescientas a seiscientas unidades tributarias.

El tipo penal **espionaje informático**, previsto en el artículo 11 (LECDI 2001), cuya acción típica es: indebidamente obtener, revelar o difundir la data o información contenidas en un sistema que utilice tecnologías de información o en cualesquiera de sus componentes. La pena base aplicable a las personas jurídicas es de multa de trescientas a seiscientas unidades tributarias. La pena será elevada de un tercio a la mitad si la comisión del tipo penal busca un beneficio para la PJ o para otra persona, sea natural o jurídica. La pena base aplicable a las personas jurídicas es de multa de trescientas a seiscientas unidades tributarias.

La conducta delictual correspondiente a la **falsificación de documentos** está prevista en el artículo 12 (LECDI 2001), cuyas acciones típicas son las siguientes: (i) Crear, modificar o eliminar un documento que se encuentre incorporado a un sistema que utilice tecnologías de información, (ii) Crear, modificar o eliminar datos un documento que se encuentre incorporado a un sistema que utilice tecnologías de información, (iii) Incorporar a un sistema un documento inexistente. La pena base aplicable a las personas jurídicas es de multa de trescientas a seiscientas unidades tributarias. Cuando se hubiese actuado para procurarse un beneficio para la PJ u otra PN o jurídica la multa se calculará entre un tercio y la mitad. En el supuesto que el hecho disvalioso resultare un perjuicio a otra persona el aumento de la multa será de la mitad a dos tercios.

El tipo penal referido al **hurto** está contenido en el artículo 13 (LECDI 2001), la acción típica: A través del uso de tecnologías de información, acceder, interceptar, interferir, manipular o usar de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro. La pena base aplicable a las

personas jurídicas es de multa de doscientas a seiscientas unidades tributarias.

El **fraude**, previsto en el artículo 14 (LECDI 2001), cuya acción típica: conseguir insertar instrucciones falsas o fraudulentas a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes, o en la data o información en ellos contenida, que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno. La pena base aplicable a las personas jurídicas es de multa de trescientas a setecientas unidades tributarias.

La **obtención indebida de bienes o servicios**, prevista en el artículo 15 (LECDI 2001), tiene como acciones típicas: (i) Utilizar sin autorización para portarlos, una tarjeta inteligente ajena o instrumento destinado a los mismos fines. (ii) Utilizar indebidamente tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio; o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida. La pena base aplicable a las personas jurídicas es de multa de doscientas a seiscientas unidades tributarias.

El **manejo fraudulento de tarjetas inteligentes o instrumentos análogos**, tipificado en el artículo 16 (LECDI 2001), tiene las siguientes acciones típicas: (i) Crear, capturar, grabar, copiar, alterar, duplicar o eliminar la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fine, (ii) Crear, capturar, duplicar o alterar la data o información en un sistema, con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos, (iii) Adquirir, comercializar, poseer, distribuir, vender o realizar cualquier tipo de intermediación de tarjetas inteligentes o instrumentos destinados al mismo fin o de la data o información contenidas en ellos o en un sistema. La pena base aplicable a las personas jurídicas es de multa de mil unidades tributarias.

La **apropiación de tarjetas inteligentes o instrumentos análogos**, esta descrita esta acción ilícita en el artículo 17 (LECDI 2001), su acción típica consiste en apropiarse, adquirir o recibir una tarjeta inteligente o instrumento destinado a los mismos fines, que se haya perdido, extraviado o que haya sido entregado por equivocación, con el fin de retenerlo, usarlo, venderlo o transferirlo a una persona distinta del usuario autorizado o entidad emisora. La pena base aplicable a las personas jurídicas es de multa de diez a cincuenta unidades tributarias.

La **provisión indebida de bienes o servicios**, prevista en el artículo 18 (LECDI 2001), cuya acción típica es proveer a quien presente dichos documentos, a sabiendas de su situación, de dinero, efectos, bienes o servicios, o cualquier otra cosa de valor económico. La pena base aplicable a las personas jurídicas es de multa de doscientas a seiscientas unidades tributarias.

La conducta delictual de **posesión de equipo para falsificaciones**, tipificada en el artículo 19 (LECDI 2001), cuya acción típica es: recibir, adquirir, poseer, transferir, comercializar, distribuir, vender, controlar o custodiar, sin autorización, cualquier equipo de fabricación de tarjetas inteligentes o de instrumentos destinados a los mismos fines, o cualquier equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o instrumentos. La pena base aplicable a las personas jurídicas es de multa de trescientas a seiscientas unidades tributarias.

La **violación de la privacidad de la data o información de carácter personal**, descrita es conducta criminal en el artículo 20 (LECDI 2001), siendo su acción típica apoderarse, utilizar, modificar o eliminar por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información. La pena base aplicable a las personas jurídicas es de multa de doscientas a seiscientas unidades tributarias.

La **violación de la privacidad de las comunicaciones**, contenida en el artículo 21 (LECDI 2001), la acción típica de este ilícito acceder, capturar, interceptar, interferir, reproducir, modificar, desviar o eliminar cualquier mensaje de datos o señal de transmisión o comunicación ajena, mediante el uso de tecnologías de información. La pena base aplicable a las personas jurídicas es de multa de doscientas a seiscientas unidades tributarias.

La revelación indebida de data o información de carácter personal, descrita en el artículo 22 (LECDI 2001), cuya acción típica es difundir o ceder, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos 20 y 21. La pena base aplicable a las personas jurídicas es de multa de doscientas a seiscientas unidades tributarias.

La **difusión o exhibición de material pornográfico**, contenido en el artículo 23 (LECDI 2001), acción típica: exhibir, difundir, transmitir o vender material pornográfico o reservado a

personas adultas, por cualquier medio que involucre el uso de tecnologías de información, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes. La pena base aplicable a las personas jurídicas es de multa de doscientas a seiscientas unidades tributarias. La **exhibición pornográfica de niños o adolescentes**, previsto en el artículo 24 (LECDI 2001), tiene como acción típica utilizar a la persona o imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos, por cualquier medio que involucre el uso de tecnologías de información. La pena base aplicable a las personas jurídicas es de multa de cuatrocientas a ochocientas unidades tributarias.

La **apropiación de propiedad intelectual**, descrito en el artículo 25 (LECDI 2001), acción típica: reproducir, modificar, copiar o divulgar un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información sin autorización de su propietario y con el fin de obtener algún provecho económico. La pena base aplicable a las personas jurídicas es de multa de cien a quinientas unidades tributarias. Así, la conducta delictual de **oferta engañosa**, tipificada en el artículo 26 (LECDI 2001) cuya acción típica es: ofrecer, comercializar o proveer de bienes o servicios, mediante el uso de tecnologías de información, y hacer alegaciones falsas o atribuir características inciertas a cualquier elemento de dicha oferta, de modo que pueda resultar algún perjuicio para los consumidores. La pena base aplicable a las personas jurídicas es de multa de cien a quinientas unidades tributarias.

3. Conclusiones

Tras la tendencia internacional de penalizar la vertiginosa criminalidad ejecutada incluso en entornos digitales por personas jurídicas, que cumplen un rol destacado en la sociedad como sujetos económicos cuya conducta antijurídica debe someterse inevitablemente al derecho penal y siendo que ese fenómeno que también ha tenido lugar en Venezuela, la Asamblea Nacional dictó la LECDI en 2001, un instrumento legal penal novísimo, no solo por los tipos penales referidos a las TIC, sino también porque incorporó la cláusula de la responsabilidad penal de la persona jurídica por delitos informáticos. En ese entonces la comunidad científica venezolana no estaba preparada para asimilar el alcance de esa norma ni el cambio de paradigma que representa respecto de un código penal de corte tradicional, por lo que

negaban la existencia de la responsabilidad penal de los entes morales con fundamento en el principio «societas delinquere non potest», al tiempo que perdían de vista su ineficiencia ante la delincuencia económica empresarial y menos para una ciberdelincuencia en auge y aún más letal. Ante la necesidad de sostener una posición clara sobre la responsabilidad penal de la persona jurídica por delitos informáticos en Venezuela, en esta investigación se propuso analizar de forma crítica y reflexiva el artículo 5 de la LECDI (2001) y estudiar la teorización internacional formulada sobre la problemática planteada para identificar cuál es el modelo de atribución de la responsabilidad penal de la persona jurídica escogido por el legislador venezolano, cuál es el modelo de imputación, esto es, si se le imputan hechos propios o hechos ajenos, así como determinar la naturaleza de la sanción aplicable que, en este caso, es pecuniaria, como esencia del aporte que ofrece frente aspectos fuertemente controvertidos. En atención a los conocimientos adquiridos durante el análisis de precepto legal señalado, del derecho comparado y de las teorías que se han formulado en relación con los aspectos indicados, pudo llegarse a las siguientes conclusiones:

PRIMERA. El Código penal venezolano (2005) no prevé un título destinado a la responsabilidad penal de las personas jurídicas ni existe una ley especial que desarrolle un estatuto completo como las codificaciones de España y Francia, entre otros. Sin embargo, el articulado del código sobre el sujeto activo del delito y las penas está redactado de una forma neutra tal, que deja abierta la posibilidad de abarcar a una persona natural, a una jurídica y hasta aquella que ahora denominan «persona artificial» para referirse a las IA con autonomía de decisión; igual pasa con las sanciones que, según está establecido, pueden ser penas corporales y no corporales. Puesto que no hay en el referido Código penal una disposición expresa que limite la aplicación de sus normas sólo a los individuos, resta en consecuencia hacer una interpretación de ellas y de las leyes especiales dictadas, en consonancia con las disposiciones de aquel, ajustada a la realidad actual de la dinámica social que así lo exige so pena de caducidad o desuso normativo. Con fundamento en lo anterior puede afirmarse que el Código Penal venezolano (2005) prevé una cláusula abierta de responsabilidad penal aplicable tanto a las personas naturales como a las jurídicas, en consonancia con la previsión de responsabilidad penal de las personas colectivas en la LECDI en materia de delitos informáticos, por lo que no es posible negar su fundamento jurídico.

SEGUNDA. La incidencia de la ciberdelincuencia en Venezuela ha alcanzado mayor auge en los últimos años, con certeza se puede aseverar que la verificación de las tres variables interdependientes de Cohen y Felson (1979), un ciberdelincuente motivado, una víctima apropiada y un guardián ausente, no se escapa de la realidad sobre la existencia de una ciberdelincuencia corporativa, principalmente por una realidad de doble anonimato, la que genera el amparo de una persona jurídica y la capa de invisibilidad otorgada por el ciberespacio, mutando de esta forma hacia una ciberdelincuencia económica, hoy opaca como fenómeno criminológico, pero no imposible de inferir, pues a nivel mundial la pandemia por el COVID-19 creó las condiciones perfectas para la expansión de la ciberdelincuencia, por esa razón la INTERPOL alertó sobre esa combinación letal para la sociedad; no obstante, en Venezuela, así como en la mayoría de los países de Latinoamérica, la comercialización de productos asociados a la salud es altamente regulada por el Estado, podemos entonces inferir que en parte de ese mercado clandestino de productos asociados al COVID-19 se hayan involucrado personas jurídicas. Por esta razón se requiere agilizar la operacionalización judicial de la responsabilidad penal de las personas jurídicas por la comisión de delitos informáticos previstos en la LECDI (2001). Por otra parte, el sector de las criptoactivos en Venezuela es altamente regulado, sin embargo, las predicciones para el 2022 por las empresas de ciberseguridad es la incidencia de cibercrímenes asociadas a este sector, siendo así, *ex profeso*, la captación de víctimas será ejecutada por personas jurídicas para cometer *a posteriori* un delito, por ejemplo, el de oferta engañosa, previsto en el artículo 26 de la LECDI (2001). De allí que se requiere aceptar que el derecho penal se ha expandido para reconocer y abarcar a las personas jurídicas como sujetos activos de delitos comunes y ciberdelitos e impedir la impunidad por sus conductas antijurídicas.

TERCERA. Comprender la funcionalidad de la responsabilidad penal de las personas jurídicas por delitos informáticos, prevista en el artículo 5 (LECDI 2001), es esencial para deslindarla de la responsabilidad penal de las personas naturales, por lo que se deben determinar de forma clara y coherente los modelos de atribución e imputación de la responsabilidad de la persona jurídica para que los operadores jurídicos conozcan su fundamento estructural y sea posible su aplicación efectiva por parte del órgano jurisdiccional en los casos planteados, con las garantías del debido proceso y tutela judicial efectiva, para que dimane la jurisprudencia como fuente de interpretación y creación del derecho en esta crucial materia, por demás compleja.

CUARTA. La investigación y los estudios realizados permitieron determinar que en el artículo 5 de la LECDI (2001), considerando el preciado valor de los bienes jurídicos protegidos como la seguridad e integridad de la información, la privacidad entre otros, el legislador adoptó un sistema cónsono con el modelo de atribución ecléctico de la responsabilidad penal de la persona jurídica, de manera que éstas son responsables directamente por los delitos que cometen por decisión de sus órganos o por haberlos financiado con sus recursos o por hacerlo en su beneficio o interés preferente (condiciones que no son concurrentes), con independencia de la responsabilidad penal de las personas naturales, en tanto que ellas responden por su participación culpable; asimismo, conforme a dicha norma se imputa la responsabilidad penal a la persona jurídica por el hecho propio que manifiesta la voluntad inequívoca a partir de la tesis organicista, excluyendo toda posibilidad de la transferencia del hecho ajeno; y finalmente, la sanción de multa que se aplica es de naturaleza estrictamente penal, en efecto, conforme lo señala el propio Código penal (art. 10 CP, 2005) se trata de una pena no corporal, consecuencia de la comisión de un delito previsto en la ley penal especial contra los delitos informáticos, impuesta y graduada por el juez en la sentencia condenatoria dictada en un proceso penal.

QUINTA. En una reforma futura la ley debería incorporar: (i) un título dedicado a las normas y garantías procesales propias para la investigación, imputación, prueba digital y juzgamiento de las personas jurídicas por delitos informáticos, así como la obligación de crear y mantener planes de cumplimiento normativo en el sector de las TIC o cibercompliance para gestionar los riesgos derivados de los ciberdelitos, como atenuante de la pena y eximente de responsabilidad. Además, es necesario agregar como tipología delictiva la receptación de datos informáticos para penalizar a quien conociendo el origen ilegal comercialice, transfiera o almacene los datos, a sabiendas de que provienen de las conductas delictuales de acceso ilícito, interceptación ilícita de datos o falsificación, tal como lo prevé la reforma de la Ley 19223 de Chile; asimismo, conviene añadir las conductas punibles de participación en la producción de material pornográfico con menores de 18 años y de almacenamiento digital de material pornográfico infantil; aunada la fórmula que asigne la competencia de los tribunales penales nacionales para conocer de las conductas punibles de comercialización, distribución y exhibición cuando se tenga acceso a un sistema informático desde el territorio nacional.

Referencias bibliográficas

Bibliografía básica

ABANTO M. «La Responsabilidad Penal de las Personas Jurídicas: ¿Un problema del derecho penal?» En: *Derecho & Sociedad 35 Asociación Civil, N° 35. 2010.* p. 191-211. [Consultada 4/11/2021] Disponible en: https://revistas.pucp.edu.pe/index.php/derechoysociedad/article/view/13300

ABANTO M. «La Responsabilidad Penal de los entes colectivos: una revisión crítica de las soluciones penales» En: Revista Penal México, N° 3 enero-junio 2012. p. 9-57. [Consultada 4/11/2021] Disponible en: http://rabida.uhu.es/dspace/bitstream/handle/10272/14257/responsabilidad_penal.pdf;jsessionid=EB064580DED61BE4D6D64FCFB29C5665?sequence=2

AGOUES MENDIZABAL, C. «La responsabilidad penal y/o sancionadora de las personas jurídicas en los distintos Estados miembros de la UE» EUROPEAN INLINKINGS (euI) ii Armonización Penal en Europa. ISBN: 978-84-7777-412-9. IVAP Herri Arduralaritzaren Euskal Erakundea 2012. P. 34-51. Disponible en: https://www.ehu.eus/documents/1736829/2010409/EyC+32+Armonizaci%C3%B3n+Penal+DIG.pdf

AGUSTINA, J.R. MONTIEL JUAN, I. y GÁMEZ-GUADIX. *Cibercriminología y victimización online*. 1ª edición. Madrid: Ed. Síntesis, 2020.

ARROYO HERNÁNDEZ, A. «Actualidad e importancia de la responsabilidad criminal de las personas jurídicas y su incorporación en el Anteproyecto del Código Penal», 93-116. En: BREZO

ARROYO ZAPATERO, L. «Personas jurídicas y responsabilidad penal en España» 125-131. En GARCÍA RIVAS, N. (Coord.) *Protección penal del consumidor en la Unión Europea*. Cuenca: Universidad Castilla La Mancha, 2005.

BAJO FERNÁNDEZ, M. «Concepto y contenido del derecho penal económico» 3-21. En MIR PUIG, S., MODOLLEL GONZÁLEZ, J., GALLEGO SOLER, J., BELLO RENGIFO, C. (Coords). Estudios de *Derecho penal económico*. Caracas: Livrosca, 2002.

BASIGALUPO, R. «La responsabilidad penal y sancionatoria de las personas jurídicas en el Derecho Europeo», 65-89. En BASIGALUPO R. (Director). *Derecho penal económico*. Buenos

Aires: Hammurabi, 2000.

CANDAU, J. *Ciberseguridad, evolución y tendencias*. Instituto Español de Estudios Estratégicos. 2021. Disponible en: http://www.ieee.es/Galerias/fichero/docs_marco/2021/DIEEEM11_2021_JAVCAND_Ciberseguridad.pdf

CASTELLS, A. *Diccionario de Internet. Todos los términos utilizados en la WWW.* España: Ed. DEUSTO, 2001.

CHOCLÁN MONTALVO, J. «La responsabilidad de la persona jurídica y d ellos Administradores por la actuación de los administradores por la actuación en su nombre» 14-46. En SOLER PASCUAL, L. *Responsabilidad de las personas jurídicas en los delitos económicos. Especial referencia a los consejos de administración. Actuar en nombre de otro*. Estudios de Derecho Judicial 91-2006. Madrid: Centro de documentación del Consejo General del Poder Judicial, 2006.

ESTEPA DOMINGUEZ, F. La responsabilidad penal de la persona jurídica. PF. Universidad Internacional de Andalucía. Córdoba: Ed. electrónica, 2012

FARALDO CABANA, P. ¿Es la multa una pena apropiada para las personas jurídicas? EUROPEAN INLINKINGS (eul) ii Armonización Penal en Europa. ISBN: 978-84-7777-412-9. IVAP Herri Arduralaritzaren Euskal Erakundea 2012. P. 53-77. Disponible en: https://www.ehu.eus/documents/1736829/2010409/EyC+32+Armonizaci%C3%B3n+Penal+DIG.pdf

FEIJOO SÁNCHEZ, B. *Derecho Penal de la Empresa e Imputación Objetiva.* 1ª edición. Madrid: Ed. Reus S.A., 2007.

FEIJOO SÁNCHEZ, B. «Imputación de hechos delictivos en estructuras empresariales complejas (1)» En *La Ley Digital 360,* 2243/2007, p.21, [Consulta: 29 noviembre 2021]. Disponible en: https://www.corporatedefense.com/pdf/Imputacion%20de%20hechos%20delictivos%20en%20estructuras%20em....pdf

FERNÁNDEZ, C. y CHANJAN, R. «La Responsabilidad Penal de las Personas Jurídicas: un estudio comparado entre España y el Perú». En Revista *Derecho PUCP*, N° 77, ISSN 0251-3420. Lima: Fondo Editorial de la Pontificia Universidad Católica, 2016. [en línea]. [Consulta: 20 noviembre 2021]. Disponible en: https://doi.org/10.18800/derechopucp.201602.014

FERNÁNDEZ SÁNCHEZ, M. «Responsabilidad penal de las personas jurídicas. Criminalidad de empresa. Tipos específicos del Anteproyecto de Código Penal del Tribunal Supremo de Justicia», 305-329. En: PARRA ARANGUREN, F. (ed.). *Anteproyecto Código Penal – comentarios.* Caracas: Ed. Tribunal Supremo de Justicia, 2004.

FERRAJOLI, L. Democracia y garantismo. Edición de Miguel Carbonell. Madrid: Ed. Trotta, 2008.

FIGUEROA RUBIO, S. y TORRES ORTEGA, I. «Dos tesis de H.L.A. Hart sobre responsabilidad y castigo: 50 años después». En Revista *Derecho PUCP*, N° 81, ISSN 0251-3420 / e-ISSN: 2305-2546. Lima: Fondo Editorial de la Pontificia Universidad Católica, 2018. [en línea]. [Consulta: 10 octubre 2021]. Disponible en: https://www.academia.edu/38729257/Dos_tesis_de_H_L_A_Hart_sobre_responsabilidad_y_castigo_50_a%C3%B1os_despu%C3%A9s

GÓMEZ MARTÍN, V. *La responsabilidad penal individual en estructuras empresariales. El caso del compliance officer.* 1ª edición. Buenos Aires: Ed. Hammurabi Digital, 2021. *La reforma penal en materia de investigación tecnológica.* 1ª edición. Coruña: Ed. Colex, Biblioteca Digital, 2020.

HERNÁNDEZ DÍAZ, l. El delito informático. EGUZKILORE San SebastiÆn: Nœmero 23, 2009.

HERNÁNDEZ QUITERO, H. Los delitos económicos en la actividad financiera. Séptima edición. Bogotá: Grupo Editorial Ibañez. 2015.

MAGRO SERVET, V. *Contenido necesario del plan de prevención jurídica de las empresas para evitar responsabilidades penales*. La Ley penal número 87, 2011. Disponible en:

https://biblioteca.cunef.edu/gestion/catalogo/index.php?lvl=notice_display&id=19481

MANSDÖRFE, M. «Responsabilidad e imputación individuales en la ejecución de tareas en grupo». En *InDret* 2/2007. Barcelona. [Consulta: 1 diciembre 2021] Disponible en: https://indret.com/wp-content/themes/indret/pdf/425_es.pdf

MARTÍNEZ – BUJÁN PÉREZ, C. *Derecho penal económico parte general.* 1ª edición. Valencia: Ed. Tirant lo Blanch, 1998.

MAYER LUX, Laura. *The object of legal protection in cybercrimes*. En *Revi Chil. Derecho* [online]. 2017, vol.44, n.1 [consultado el 09/11/2021], pp.261-285. Disponible en:

http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-34372017000100011&lng=en&nrm=iso>. ISSN 0718-3437. http://dx.doi.org/10.4067/S0718-34372017000100011.

MENDOZA TROCONIS, J. Curso de Derecho Penal Venezolano. Parte General. Tomo III. 7ª Ed. Caracas: Empresa El Cojo C.A., 1985.

MIR PUIG S., MODOLELL GONZÁLEZ J. L., GALLEGO SOLER J. I. y BELLO RENGIFO C. S. (coords.). *Estudios de Derecho Penal Económico.* 1ª edición. Caracas: Ed. Livrosca, 2002.

MIRÓ LINARES F., «La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen». *Revista Electrónica de Ciencia Penal y Criminología* (en línea). 2011, núm. 13-07, p. 07:1- 07:55. ISSN 1695-0194 [RECPC 13-07 (2011), 29 nov] [Consulta: 1 noviembre 2021]. Disponible en: http://criminet.ugr.es/recpc/13/recpc13-07.pdf.

MIRÓ LINARES F., «Reflexiones sobre el principio societas delinquere non potest y el artículo 129 del Código Penal». En SOLER PASCUAL, L. Magistrado (dir). *Responsabilidad de las personas jurídicas en los delitos económicos. Especial referencia a los consejos de administración. Actuar en nombre de otro.* Consejo General del Poder Judicial. Escuela Judicial. Estudios de Derecho Judicial N° 21, p. 190. ISSN: 1137 –3520, ISBN 978-84-96518-96-42006. Madrid: Centro de Documentación Judicial, 2006.

MONTEALEGRE LYNETT E. (coord.). *Libro Homenaje al Profesor Gunter Jakobs. El Funcionalismo en Derecho Penal.* Tomo II. 1ª edición. Colombia: Ed. Universidad Externado de Colombia, 2003.

NEWLANDS, G, LUTZ C, TAMO-LARRIEUX, A, FOSCH VILLARONG, E, HARASGAMA, R, SCHEITLIN, G. «Innovation under pressure: Implications for data privacy during the Covid-19pandemic». Big Data & Society. 2020. July- December. Disponible en: https://journals.sagepub.com/doi/full/10.1177/2053951720976680.

ORSE G. «Responsabilidad penal de las personas jurídicas» 368-386. En MONTEALEGRE LYNETTE., (Coord.). *El funcionalismo en derecho penal Libro Homenaje al profesor GÜNTER JACKOBS*. Tomo II, 1ra ed. Bogotá: Ed. Universidad Externado de Colombia, 2003.

PARRA ARANGUREN, F. (ed.). *Anteproyecto Código Penal – comentarios.* Caracas: Tribunal Supremo de Justicia, 2004.

STEEL, C, NAGAPPAN, R y LAI, R. *Core Security Patterns: Best Practices and Strategies for J2EETM, Web Services, and Identity Management*. Estados Unidos: Prentice Hall, 2005.

PETRO G., I., Mosquera R., J. y Torres M., L. *«La responsabilidad penal de personas jurídicas como omisión legislativa en Colombia»*. Revista Criminalidad, Vol.56, N°3, p 87-102 ISSN 1794-3108. Bogotá, 2014.

POLANSKY J. A. *Garantías constitucionales del procedimiento penal en el entorno digital*. 1ª edición. Buenos Aires: Ed. Hammurabi Digital, 2020.

ROBLES PLANAS R. «¿Delitos de las Personas Jurídicas? A propósito de la Ley austriaca de responsabilidad de las agrupaciones por hechos delictivos», *En InDret Revista para el Análisis del Derecho* 2.2006. Nº4 - 2021 - ISSN 1698-739X. Barcelona 2006. [Consultada: 20 octubre 2021] Disponible en: https://indret.com/delitos-de-personas-juridicas/.

RODRÍGUEZ MORALES, A.J. «Venezuela» 875-904. En Tratado Angloiberoamericano sobre Compliance Penal. RODRÍGUEZ GARCÍA, N. (dir.). Valencia: Tirant Lo Blanch. 2021.

RODRÍGUEZ, J., ODUBER, J., & MORA, E. «Actividades rutinarias y cibervictimización en Venezuela». 2017 *Revista Latinoamericana de Estudios de Seguridad*, (20), 63-79. [Consulta: 17 septiembre 2021]. Disponible en: https://doi.org/10.17141/urvio.20.2017.2583

SILVA S. J. *La Expansión del Derecho Penal. Aspectos de la política criminal en las sociedades postindustriales.* 3ra edición. Madrid: Marcial Pons, 2011.

TÉLLEZ VALDES J. *Derecho Informático.* 2ª edición. México: Ed. McGRAW – HILL, 1999.

TIEDEMANN K. (dir.), Nieto Martín, A. (coord.). *Eurodelitos. El Derecho Penal económico en la Unión Europea.* 1ª edición. La Mancha: Ediciones de la Universidad Castilla – La Mancha, 2004.

VALS J. «Nuevas formas de combatir el Crimen en internet y sus riesgos» *En Revista Electrónica de Ciencia Penal y Criminología.* ISSN 1695-0194. 2016, N°18-22, pp. 1-36 − ISSN 1695-0194 2016. [Consulta: 30 octubre 2021] Disponible en: http://criminet.ugr.es/recpc/18/recpc18-22.pdf

Bibliografía complementaria

AMONI G. Entrevista a Beatriz Di Totto: 20 años de la histórica Ley contra Delitos Informáticos. *Prodavinci* [en línea], 1 de diciembre de 2021. [Consulta: 7 diciembre 2021]. Disponible en: https://prodavinci.com/entrevista-a-beatriz-di-totto-20-anos-de-la-historica-

ley-contra-1/.

BANCO INTERAMERICANO DE DESARROLLO. «Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe». [en línea]. Julio 2020. S.l.: Banco interamericano de Desarrollo. [Consulta: 26 octubre 2021]. Disponible en: https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-seguir-en-america-latina-y-el-caribe.

CUBADEBATE. «Ataque cibernético en Venezuela prende las alarmas en el mundo». [en línea], 2019. [Consulta: 25 noviembre 2021]. Disponible en: http://www.cubadebate.cu/especiales/2019/03/31/ataque-cibernetico-en-venezuela-prende-las-alarmas-en-el-mundo/.

CUERPO DE INVESTIGACIONES CIENTÍFICAS PENALES Y CRIMINALÍSTICAS «CICPC a la vanguardia de la investigación científica de los delitos informáticos». *Revista CICPC* [en línea], 15 de junio de 2018. [Consulta: 7 agosto 2021]. Disponible en: https://revistacicpc.com/cicpc-a-la-vanguardia-de-la-investigacion-cientifica-de-los-delitos-informaticos/.

DIAZGRANADOS H. «Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021». [en línea], 31 de agosto de 2021. [Consulta: 26 noviembre 2021]. Disponible en: https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/.

DIAZGRANADOS H. «Pronóstico de ciberamenazas 2022 para América Latina». [en línea], 18 de noviembre de 2021. [Consulta: 20 de noviembre 2021]. Disponible en: https://latam.kaspersky.com/blog/pronostico-de-ciberamenazas-2022-para-america-latina/23426/.

FRONT LINE DEFENDERS «Transparencia Venezuela subjected to repeated cyber attacks». [en línea], 9 de julio de 2018. [Consulta: 25 noviembre 2021]. Disponible en: https://www.frontlinedefenders.org/es/case/transparencia-venezuela-subject-cyber-attacks.

KEMP, S. *DIGITAL 2021: LOCAL COUNTRY HEADLINES.* Data Reportal, [en línea], 27 de enero de 2021. [Consulta: 2 noviembre 2021]. Disponible en: https://datareportal.com/reports/digital-2021-local-country-headlines

PROYECTO de ley que establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest. Chile. 25 de octubre de 2018. [Consulta: 17 mayo 2020] Disponible en: https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=12715&prmBOLETIN=12192-25

REINA, O. «Venezuela está bajo un ataque cibernético desmedido». *CONATEL* [en línea], 2019. [Consulta: 25 noviembre 2021]. Disponible en: http://www.conatel.gob.ve/cnti-venezuela-esta-bajo-un-ataque-cibernetico-desmedido/.

SEGUADMIN. «Exposición del proyecto de ley sobre delitos informáticos» [en línea], 2000. [Consulta: 4 noviembre 2021]. Disponible en: https://segured.com/2000/01/01/exposicion-del-proyecto-de-ley-sobre-delitos-informaticos/.

SONICWALL. «Sonicwall Cyber Threat Report».[en línea], 2021.[Consulta: 5 noviembre 2021]. Disponible en: https://www.sonicwall.com/medialibrary/en/white-paper/2021-cyber-threat-report.pdf

Legislación citada

Carta de Naciones Unidas, 1945. Disponible en: https://www.un.org/es/about-us/un-charter/full-text

Código Orgánico Procesal Penal. Gaceta Oficial de la República Bolivariana de Venezuela de 15 de junio de 2012, N° 6.078, p. 64.

Código Penal. Gaceta Oficial de la República Bolivariana de Venezuela de 13 de abril de 2005, N° 5.768 Extraordinario, p. 32.

Constitución de la República Bolivariana de Venezuela. Gaceta Oficial de la República Bolivariana de Venezuela de 30 de diciembre de 1999, N° 36.860, p. 312.171.

Decreto Constituyente sobre criptoactivos y la criptomoneda soberana Petro. Gaceta Oficial de la República Bolivariana de Venezuela de 9 de abril de 2018, N° 6.370 Extraordinario.

Ley contra la delincuencia organizada y financiamiento al terrorismo. Gaceta Oficial de la República Bolivariana de Venezuela de 30 de abril de 2012, N° 39.912. p. 385.472.

Ley de acceso e intercambio electrónico de datos, información y documentos entre los órganos y entes del Estado. Gaceta Oficial de la República Bolivariana de Venezuela de 15 de junio de 2012, N° 39.945, p. 394.274.

Ley de corrupción. Gaceta Oficial de la República Bolivariana de Venezuela de 19 de noviembre de 2014, N° 6.155 Extraordinario, p. 48.

Ley de precios justos. Gaceta Oficial de la República Bolivariana de Venezuela de 23 de enero de 2014, N° 40.340, p 408.948.

Ley de simplificación de trámites administrativos. Gaceta Oficial de la República Bolivariana de Venezuela de 22 de octubre de 1999, N° 5.393 Extraordinario, p. 32.

Ley especial contra delitos informáticos. Gaceta Oficial de la República Bolivariana de Venezuela de 30 de octubre de 2001, N° 37.313, p. 320.852.

Ley penal del ambiente. Gaceta Oficial de la República Bolivariana de Venezuela de 02 de mayo de 2012, N° 39.913. p. 425.936.

Ley sobre Mensajes de Datos y Firma Electrónica. Gaceta Oficial de la República Bolivariana de Venezuela de 28 de febrero de 2001, N° 37.148. p. 317.499.

Pacto Internacional de derechos económicos, sociales y culturales. Asamblea General de las Naciones Unidas, Resolución 2200 A (XXI), de 16 de diciembre de 1966. Disponible en: https://www.ohchr.org/SP/ProfessionalInterest/Pages/CESCR.aspx

Pacto Internacional sobre derechos civiles y políticos. Asamblea General de las Naciones Unidas, Resolución 2200 A (XXI), de 16 de diciembre de 1966. Disponible en: https://www.ohchr.org/sp/professionalinterest/pages/ccpr.aspx

Jurisprudencia referenciada

Decisión N° 240 de 29 de febrero de 2020, Sala de Casación Penal del Tribunal Supremo de Justicia, caso Procter & Gamble de Venezuela, S.A. En: http://historico.tsj.gob.ve/decisiones/scp/febrero/240-290200-971971.htm

Decisión N° 834 de 18 de junio de 2009, Sala Constitucional del Tribunal Supremo de Justicia, caso GLOBOVISIÓN. En: http://historico.tsj.gob.ve/decisiones/scon/junio/834-18609-2009-03-0296.HTML.

Listado de abreviaturas

(Art) Artículo

(CE) Constitución Española

(CICPC) Cuerpo de Investigaciones Científicas, Penales y Criminalísticas

(CNTI) Centro de Tecnologías de la Información

(CP) Código Penal Venezolano

(CPE) Código Penal Español

(CPF) Código Penal Francés

(CRBV) Constitución de la República Bolivariana de Venezuela

(CSC) Convenio sobre la ciberdelincuencia

(DAM) Dispositivos de almacenamiento masivo

(DDOs) Ataque distribuido de denegación de servicios

(EC3) Centro Europeo de Ciberdelincuencia

(Europol) Agencia de la Unión Europea en Materia Policial

(GO) Gaceta Oficial de la República Bolivariana de Venezuela

(IA) Inteligencia artificial

(IoT) Internet de las cosas

(INTERPOL) Organización Internacional de Policía Criminal

(LECDI) Ley especial contra los delitos informáticos

(NT) Nuevas tecnologías

(OAS) On Access Scan

(OCDE) Organización para la Cooperación y el Desarrollo Económico y los Estados

(ODS) On demand scanner

(PJ) Persona jurídica

(PN) Persona natural

(RMW) Ransomware

(RPPJ) Responsabilidad penal de la persona jurídica

(RPPN) Responsabilidad penal de la persona natural

(SSC/TSJ) Sentencia de la Sala Constitucional del Tribunal Supremo de Justicia

(SSCP/TSJ) Sentencia de la Sala de Casación Penal del Tribunal Supremo de Justicia

(TIC) Tecnologías de la información y comunicación

(UE) Unión Europea