Consideraciones jurídicas sobre la creación del consejo nacional de ciberseguridad

ALEJANDRO FUENMAYOR ESPINA

El presente ensayo nos ofrece un análisis, desde una perspectiva jurídica, sobre la creación del Consejo Nacional de Ciberseguridad que se oficializó el 12 de agosto de 2024. El artículo tiene dos partes; la primera, una revisión acerca de las nociones doctrinarias aplicables a lo que fue la creación del referido Consejo Nacional de Ciberseguridad, así como unas notas acerca de la importancia que tiene la ciberseguridad en el ámbito de la jurisprudencia internacional. La segunda parte es el análisis jurídico del Decreto de creación de este Consejo.

Es un hecho público y comunicacional la situación surgida con motivo de las elecciones presidenciales realizadas el 28 de julio de 2024, donde el presidente del Consejo Nacional Electoral, en lo adelante CNE, al momento de anunciar los resultados electorales, denunció ante el país un hackeo o acceso no autorizado al sistema informático de dicha institución, el cual hasta la fecha no ha sido explicado de manera satisfactoria ante la opinión pública nacional e internacional. En los días subsiguientes a esta elección presidencial el Poder Ejecutivo nacional decidió crear, mediante decreto presidencial, el Consejo Nacional de Ciberseguridad, que en lo adelante denominamos como CNC, publicado en la *Gaceta Oficial* no. 42.939 de fecha 12 de agosto de 2024.

En el presente trabajo nos abocaremos a analizar en una primera parte, las nociones doctrinarias aplicables a la creación de este Consejo, sus fundamentos constitucionales y los considerandos que motivan su creación. Igualmente haremos énfasis en la importancia que tiene el ámbito jurídico internacional en todos los asuntos referentes a la ciberseguridad.

En la segunda parte del trabajo nos referiremos al análisis jurídico del articulado que conforma este Decreto de creación y a las normas legales sobre las cuales debe versar el campo de aplicación del CNC como organismo de consulta del presidente de la República.

NOCIONES DOCTRINARIAS SOBRE EL DECRETO DE CREACIÓN DEL CNC Y LA CIBERSEGURIDAD

Antes de entrar en el análisis de la creación del CNC observamos que nuestro país cuenta con una legislación en materia de la cibernética, la electrónica y las telecomunicaciones en general desde el año 2000. Sin embargo, se puede apreciar que existe un tratamiento jurídico-político descoordinado y contradictorio, configurándose una situación de laberinto legislativo confuso. Si bien se refleja por una parte, una adecuación normativa en la materia al mundo económico digital, con sus aciertos y desaciertos en las transacciones financieras; por otra parte, la libre comunicación de las ideas y de las informaciones a través de las tecnologías electrónicas tienden a restringirse cada vez con mayor auge, con una intolerancia legislativa que tipifica la disidencia ideológica como delito, creando una verdadera confusión entre lo que entendemos como alteración al orden público y el ejercicio de la libertad de expresión de las ideas e informaciones. Tampoco existe un tratamiento jurídico idóneo que se ajuste a las nuevas plataformas tecnológicas que se han convertido en el transporte mundial de los mensajes informativos y de ideas.

En este contexto, abordaremos el análisis sobre el entorno doctrinario de los significados sobre cibernética, telemática, ciberespacio y ciberseguridad; así como sobre los fundamentos constitucionales y considerandos del Decreto de creación del CNC.

Fundamentos constitucionales y considerandos del Decreto de creación del CNC

En relación a los fundamentos constitucionales y los considerandos o criterios político-administrativos invocados por autoridades públicas del Gobierno nacional creadoras del CNC, observamos que se invocan los artículos 15, 110, 226, y 322 de la Constitución. De estos postulados podemos citar los artículos 110 y 322 que son del tenor siguiente:

> Artículo 110. El Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional. Para el fomento y desarrollo de esas actividades, el Estado destinará recursos suficientes y creará el sistema nacional de ciencia y tecnología de acuerdo con la ley. El sector privado deberá aportar recursos para las mismas. El Estado garantizará el cumplimiento de los principios éticos y legales que deben regir las actividades de investigación científica, humanística y tecnológica. La ley determinará los modos y medios para dar cumplimiento a esta garantía
>
> Artículo 322. La seguridad de la Nación es competencia esencial y responsabilidad del Estado, fundamentada en el desarrollo integral de ésta y su defensa es responsabilidad de los venezolanos y venezolanas; también de las personas naturales y jurídicas, tanto de derecho público como de derecho privado, que se encuentren en el espacio geográfico nacional.

Del artículo 110 se desprende que las aplicaciones tecnológicas se consideran instrumentos fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional. Del artículo 322, que la defensa integral de la seguridad de la Nación es responsabilidad de las personas naturales y jurídicas, tanto de derecho público como de derecho privado que se encuentran en el espacio geográfico nacional.

Seguidamente, respecto a los considerandos invocados por las autoridades públicas que han suscrito este Decreto citamos sus contenidos.

> Primer Considerando
> Que el Ciberespacio es de interés público y estratégico para la República Bolivariana de Venezuela, que requiere por parte del Estado el desarrollo de políticas de seguridad, administración y control en su acceso y uso, para asegurar el bien común, la soberanía y la institucionalidad en beneficio de la Nación,

Segundo Considerando
Que aun cuando las tecnologías de la información y las comunicaciones actualmente representan herramientas para el desarrollo de las sociedades, también pueden ser utilizadas para incurrir en la comisión de una diversidad de actividades delictivas que ocasionan un efecto adverso en todos los ámbitos de la sociedad, instituciones, operaciones y sistemas de información,

Tercer Considerando
Que la República Bolivariana de Venezuela ha sido y será víctima de repetidas agresiones telemáticas que han pretendido afectar la industria petrolera (2002), el suministro eléctrico nacional (2019) y las decisiones soberanas del pueblo Venezolano durante los comicios electorales, entre otras, por parte de grandes magnates, dueños de empresas fabricantes de tecnología que han demostrado su parcialidad por intereses económicos, políticos e injerencistas, usando las tecnologías de información y comunicación como herramienta de operación de la delincuencia organizada transnacional, ciberterrorismo y la desestabilización política,

Cuarto Considerando
Que los riesgos actuales que se generan del uso indebido de las tecnologías de comunicación e información representan un gran peligro a la preservación de la paz, la estabilidad y la seguridad de la nación, lo que requiere un mayor esfuerzo para el cumplimiento de las responsabilidades que tiene el Estado, de conformidad con el artículo 14 del Decreto con Rango, Valor y Fuerza de Ley de Reforma de la Ley Orgánica de Seguridad de la Nación.

Quinto Considerando
Que existe la necesidad de definir y aplicar, con carácter prioritario, una política con el objetivo de proteger a la sociedad de la ciberdelincuencia a través de la adopción de la delegación adecuada, el establecimiento de delitos y facultades procesales comunes y el fomento de la cooperación internacional para prevenir y combatir más eficazmente esas actividades en todos los ámbitos de la vida y en el espacio nacional, regional e internacional,…"

Comentaremos –en una primera parte– el primero, segundo, cuarto y quinto considerandos; y en una segunda parte, el tercero, visto que requiere un enfoque analítico distinto, por los graves conceptos acusatorios contenidos en el mismo.

Según el primer considerando, el ciberespacio es de interés público y estratégico para la República Bolivariana de Venezuela y requiere por parte del Estado el desarrollo de políticas de seguridad, administración y control en su acceso y uso, para asegurar el bien común, la soberanía y la institucionalidad en beneficio de la Nación.

Según el segundo considerando, aun cuando las tecnologías de la información y las comunicaciones, que en lo adelante denominamos las TIC, representan herramientas para el desarrollo de las sociedades, también pueden ser utilizadas para incurrir en la comisión de actividades delictivas que ocasionan un efecto adverso en todos los ámbitos de la sociedad, instituciones, operaciones y sistemas de información.

Según el cuarto considerando, los riesgos actuales que se generan del uso indebido de las TIC representan un gran peligro a la preservación de la paz, la estabilidad y la seguridad de la nación, lo que requiere un mayor esfuerzo para el cumplimiento de las responsabilidades que tiene el Estado. Este considerando lo fundamentan en el artículo 14 del *Decreto con rango, valor y fuerza de Ley de reforma de la Ley orgánica de seguridad de la nación*, el cual es del tenor siguiente:

> Artículo 14. El Conocimiento, la ciencia y la tecnología son recursos estratégicos para lograr el desarrollo sustentable, productivo y sostenible de nuestras generaciones. El Estado tiene la obligación de vigilar que las actividades tecnológicas y científicas que se realicen en el país no representen riesgos para la seguridad de la Nación.

Según el quinto considerando existe la necesidad de definir y aplicar, con carácter prioritario, una política con el objetivo de proteger a la sociedad de la ciberdelincuencia a través de la adopción de la delegación adecuada, el establecimiento de delitos y facultades procesales comunes y el fomento de la cooperación internacional para prevenir y combatir más eficazmente

esas actividades en todos los ámbitos de la vida y en el espacio nacional, regional e internacional.

En este orden de ideas, amerita citarse el artículo 11 constitucional, no invocado por el Decreto, el cual establece lo siguiente:

> Artículo 11. Corresponden a la República derechos en el espacio ultraterrestre suprayacente y en las áreas que son o puedan ser patrimonio común de la humanidad, en los términos, extensión y condiciones que determinen los acuerdos internacionales y la legislación nacional.

Es muy importante precisar la armonía jurídica que debe coexistir entre lo que se entiende por estos derechos de la República y los términos y condiciones de los acuerdos y tratados internacionales en la materia que son vinculantes para el Estado venezolano.

De conformidad con la hermenéutica jurídica que consagra el artículo 4 de nuestro Código Civil, interpretamos el sentido literal de las palabras que conforman estos considerandos, y la intención del constituyente, observando que los derechos de la República en el espacio ultraterrestre suprayacente y en las áreas que son o puedan ser patrimonio común de la humanidad, le corresponden en los términos y condiciones de los acuerdos internacionales y la legislación nacional. Es muy importante precisar la armonía jurídica que debe coexistir entre lo que se entiende por estos derechos de la República y los términos y condiciones de los acuerdos y tratados internacionales en la materia que son vinculantes para el Estado venezolano. El contenido de este artículo forma parte regulatoria del concepto del ciberespacio en lo que respecta al traspaso de las fronteras del Estado venezolano.

Precisando el significado jurídico del vocablo ciberespacio, se debe tener presente en su descripción que el espacio ultraterrestre y las áreas que son o puedan ser patrimonio común de la humanidad, forman parte del concepto de ciberespacio que también comprende el espacio terrestre por aire o por fibra óptica, pero entendiendo que bien sea por hilos o por aire, traspasan las fronteras del Estado interconectándolo a nivel mundial. El ciberespacio, obligatoriamente, aplica tanto en el derecho nacional de cada Estado como en el derecho internacional que regula sus relaciones entre los Estados. Su descripción no se agota en la jurisdicción nacional.

En este sentido, la expresión "ciber" se entiende como el elemento creado por acortamiento del adjetivo cibernético, relacionado con el mundo de las computadoras, dispositivos móviles y de la realidad virtual. A su vez, la cibernética se entiende como la ciencia que estudia los sistemas de comunicación y regulación automática de los seres vivos con los sistemas electrónicos; estructurándose el lenguaje cibernético-digital que se produce y difunde a través de los medios electrónicos.

Desde una óptica cronológica, constatamos que como resultado de los avances tecnológicos ocurridos desde el descubrimiento de las telecomunicaciones y de las invenciones científicas de la informática, la cibernética y las telecomunicaciones se han fusionado en lo que hoy conocemos como la telemática, que es la unión entre la informática y las telecomunicaciones, entendiendo por informática, las técnicas que hacen posible la información por medio de ordenadores y dispositivos móviles, y por telecomunicaciones toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza, por hilo, radioelectricidad, medios ópticos u otros medios electromagnéticos afines, inventados o por inventarse[1]. La informática hace referencia al *hardware*, *software* y demás componentes tecnológicos y las telecomunicaciones a su transporte por hilos o por aire, donde de manera vertiginosa el incremento de mensajes y datos que se transportan es cada vez mayor gracias a la tecnología del *streaming* o compresión digital.

Precisada esta fusión entre las telecomunicaciones y la informática; el vocablo ciberespacio contenido en el primer considerando alude a los mensajes cibernéticos o digitales; al entorno digital que se define como un espacio de comunicación e interacción donde se comparten, almacenan producen y transmiten datos e informaciones. Podríamos decir que el ciberespacio está regulado por un conjunto de normas y principios

jurídicos que tienen como objetivo mantener la estabilidad y seguridad en el entorno digital por aire (en la esfera terrestre y ultraterrestre donde orbitan los satélites de comunicación) y por la fibra a nivel nacional de los Estados y a nivel internacional por los cables submarinos.

De esta forma, la ciberseguridad la podemos describir como las estrategias, prácticas, tecnologías y acciones dirigidas a proteger de manera integral a los datos, sistemas de información, equipos, redes, aplicaciones de *software*, sistemas operativos, *hardware*, arquitectura de redes, puntos de acceso inalámbricos, *hosts*, servidores, archivos digitales de las personas naturales y jurídicas usuarias de estas tecnologías, contra conductas indeseadas como son, entre otras: 1) el acceso no autorizado y ataques a la data y archivos de los usuarios, 2) el ataque a la seguridad de las comunicaciones digitales y la comisión de delitos en general; 3) las interrupciones en las operaciones de la comunicación masiva e interpersonal que se genera en estas tecnologías. Estas estrategias y acciones tienen por finalidad fundamental, optimizar la defensa digital en forma integral entre las personas, los procesos y las tecnologías, para mantener la confianza en los usuarios. Los tipos principales de ciberseguridad son: la seguridad de la red, la seguridad de la nube y la seguridad física. Debemos tener presente que las conductas indeseadas aquí descritas son cambiantes y mutantes en el tiempo como los virus en el ser humano, lo cual exige una supervisión y monitoreo constante sobre las mismas por parte de estos mecanismos de protección. En esta descripción doctrinaria de la ciberseguridad, todo parece indicar que su ámbito de aplicación jurídica va enfocado a la protección tecnológica contra las amenazas y delitos informáticos contra las TIC, y no al control regulatorio de los contenidos que pueden ser transmitidos por ellas. Precisamos esto porque es importante advertir que existe el peligro latente según el cual la ciberseguridad se utilice como un mecanismo de censura en lugar de utilizarse como como un mecanismo de protección.

En este sentido podemos referirnos a información de la agencia de noticias *EFE* sobre la reciente Ley de Ciberseguridad aprobada por Birmania, la cual citamos a continuación:

> Bangkok, 2 ene (EFE).- La junta militar de Birmania (Myanmar) promulgó la polémica Ley de Ciberseguridad, criticada por vulnerar derechos y limitar la libertad en Internet, según publicó este jueves el medio oficialista 'Global New Light of Myanmar. Con casi tres años de retraso, la ley entró en vigor el 1 de enero, según la orden del Consejo de Administración del Estado, nombre oficial de la junta que tomó el poder en un golpe de Estado en 2021 que ha sumido al país en una espiral de violencia y conflicto. El medio birmano no ofrece detalles sobre las partes más polémicas de la ley, pero filtraciones del proyecto presentado en 2022 contenían numerosos artículos que fueron criticados por expertos de Naciones Unidas y organizaciones no gubernamentales como Human Rights Watch (HRW) y Access Now. Expertos de la ONU dijeron entonces que la ley da a las autoridades la posibilidad de interrumpir el servicio de internet sin necesidad de permiso judicial y además prohíbe el uso sin autorización previa de redes privadas virtuales (VPN, por sus siglas en inglés), un software utilizado para sortear la censura[2]

Precisamos esto porque es importante advertir que existe el peligro latente según el cual la ciberseguridad se utilice como un mecanismo de censura en lugar de utilizarse como como un mecanismo de protección.

Esta misma noticia fue difundida por la agencia de noticias *AP*.

> BANGKOK (AP) - Myanmar, un país gobernado por militares y notorio por reprimir la libertad de expresión, promulgó una nueva ley de ciberseguridad con amplios controles sobre el flujo de información, según el texto de la medida publicado el viernes en periódicos estatales. Las restricciones existentes a la libertad de expresión bajo el gobierno militar generalmente han impuesto acusaciones de acuerdo con leyes de seguridad nacional definidas de manera imprecisa y que se relacionan con el contenido en línea. También se han producido acciones para bloquear sitios web y aplicaciones a nivel de red, impidiendo que los

> usuarios finales accedan al contenido que el ejército no quiere que vean. Se utiliza tecnología de China y Rusia, principales aliados del gobierno militar, para fines de monitoreo y censura. La nueva ley, que entró en vigor el miércoles, tiene amplias disposiciones que apuntan principalmente a medios de comunicación y proveedores de servicios como redes privadas virtuales (VPN, por sus siglas en inglés) que pueden ayudar a evadir bloqueos de red. Las VPN conectan a los usuarios con los sitios que desean visitar a través de computadoras de terceros, ocultando el contenido a los proveedores de servicios de internet y a los gobiernos entrometidos[3].

Es necesario la coexistencia e integración que debe existir entre las legislaciones nacionales de los Estados en esta materia y el ámbito regulatorio internacional sobre ciberseguridad, a fin de que las legislaciones nacionales busquen un consenso internacional coherente para que la ciberseguridad no se convierta en un mecanismo de censura contra la libre circulación de las ideas y la información.

Ámbito jurídico internacional de la ciberseguridad y su incidencia en el Decreto de creación del CNC

Entre los organismos internacionales y sus respectivos acuerdos y tratados en ciberseguridad, con incidencia en la República Bolivariana de Venezuela observamos, en primer lugar, la Organización de las Naciones Unidas –en lo adelante, ONU–. Con relación a esta Organización podemos citar, en primer lugar, la aprobación del *Proyecto de convención internacional integral sobre la lucha contra la utilización de las TIC y las comunicaciones con fines delictivos* de fecha 9 de agosto de 2024, cuyo título es el siguiente: Fortalecimiento de la cooperación internacional para la lucha contra determinados delitos cometidos mediante sistemas de tecnología de la información y las comunicaciones y para la transmisión de pruebas en forma electrónica de delitos graves. Este Proyecto fue aprobado por la Asamblea General de la ONU el 26 de diciembre de 2024, que citamos a continuación:

Convención de las Naciones Unidas contra la Ciberdelincuencia. Fortalecimiento de la Cooperación Internacional para la Lucha contra Determinados Delitos Cometidos mediante Sistemas de Tecnología de la Información y las Comunicaciones y para la Transmisión de Pruebas en Forma Electrónica de Delitos Graves.

La Asamblea General de las Naciones Unidas adopta una convención histórica contra la ciberdelincuencia. Nueva York, 26 de diciembre 2024 - La Asamblea General de las Naciones Unidas adoptó el día de hoy una nueva convención legalmente vinculante para prevenir y combatir la ciberdelincuencia, culminando un proceso de negociación de cinco años. La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) actuó como secretaría de las negociaciones. La adopción de esta Convención histórica es una gran Víctoria para el multilateralismo, ya que constituye el primer tratado internacional contra el crimen en 20 años. Es un avance crucial en nuestros esfuerzos por hacer frente a delitos como los abusos sexuales a menores en línea, las estafas sofisticadas en línea y el lavado de activos, dijo la Directora Ejecutiva de UNODC, la Sra. Ghada Waly. En la era digital actual, la ciberdelincuencia es cada vez más omnipresente y destructiva, se aprovecha de las personas vulnerables y drena billones de nuestras economías cada año. UNODC está dispuesta a apoyar a los Estados Miembro en la firma, ratificación e implementación de este nuevo tratado, proporcionando a los países las herramientas, la asistencia y el apoyo para la creación de las capacidades que necesitan para proteger sus economías y salvaguardar la esfera digital de la ciberdelincuencia. La Asamblea General aprobó la resolución sin someterla a votación. Los Estados Miembro de las Naciones Unidas, con las aportaciones de la sociedad civil, las instituciones académicas y el sector privado, negociaron el texto durante cinco años, hasta finalizar un borrador el 9 de agosto de 2024. La Convención tiene por finalidad prevenir y combatir la ciberdelincuencia de manera más eficiente y eficaz, entre otras cosas, mediante el fortalecimiento de la cooperación internacional y la prestación de asistencia técnica y el apoyo para la creación de capacidades, en particular a los

países en desarrollo. La Convención se abrirá a la firma en una ceremonia oficial que se celebrará en Vietnam en 2025 y entrará en vigor 90 días después de su ratificación por el 40° signatario. UNODC seguirá desempeñando las funciones de secretaría del Comité Ad Hoc, encargado de negociar un proyecto de protocolo complementario de la Convención, así como de la futura Conferencia de los Estados partes[4].

En el contexto de la adopción de esta convención, el ministro del Poder Popular para Relaciones Exteriores, Iván Gil, en fecha 8 de octubre de 2024, en la sede de la ONU, denunció que el sistema electoral venezolano que es totalmente electrónico y automatizado desde el año 2004 ha sido víctima de más de treinta millones de ciberataques por minuto, cuestión esta que fue seguida de masivos ataques contra todos los portales gubernamentales de Venezuela. A continuación transcribimos parte de esta denuncia.

> La culminación de este proceso llega en un momento de especial relevancia, especialmente para nuestro país que el pasado domingo 28 de julio celebró un proceso electoral en el que eligió al Presidente de la República para el sexenio 2025-2031. Como es bien sabido a pesar del ambiente de paz y civismo que signó a tales comicios, el sistema electoral venezolano que es totalmente electrónico y automatizado desde el año 2004 ha sido víctima de más de treinta millones de ciberataques por minutos, cuestión esta que fue seguida de masivos ataques contra todos los portales gubernamentales de Venezuela. Tales acciones que denunciamos hoy una vez más se enmarcan en una clara operación de desestabilización que pretendía por una parte generar un black out informativo y por otra, consolidar un golpe de estado contra las autoridades e instituciones constitucionales de mi país. Esta situación de la que hoy Venezuela es víctima señora Presidenta pudiera mañana afectar a cualquier otro Estado. Y por ello, la importancia de abordar estos temas desde una perspectiva multilateral y bajo un enfoque de cooperación. Más aun ante las profundas asimetrías que persisten en esta materia. Señora Presidenta, la magnitud de esta nueva agresión contra Venezuela que incluye precisamente el uso malicioso de las TIC pone de relieve la importancia de esta Convención[5].

Como se puede observar, Venezuela denunció ante las Naciones Unidas un golpe cibernético en curso, en el contexto de la adopción de la Convención de las Naciones Unidas contra la Ciberdelincuencia.

…el ministro del Poder Popular para Relaciones Exteriores, Iván Gil, en fecha 8 de octubre de 2024, en la sede de la ONU, denunció que el sistema electoral venezolano que es totalmente electrónico y automatizado desde el año 2004 ha sido víctima de más de treinta millones de ciberataques por minuto, cuestión esta que fue seguida de masivos ataques contra todos los portales gubernamentales de Venezuela.

Ahora bien; dentro de los postulados aprobados en esta Convención podemos referirnos a los siguientes artículos:

> Artículo 1
> Finalidad
> La finalidad de la presente Convención es:
> a) Promover y fortalecer las medidas para prevenir y combatir más eficaz y eficientemente la ciberdelincuencia; b) Promover, facilitar y fortalecer la cooperación internacional para prevenir y combatir la ciberdelincuencia; y c) Promover, facilitar y apoyar la asistencia técnica y el fomento de la capacidad con el fin de prevenir y combatir la ciberdelincuencia, en particular en beneficio de los países en desarrollo.

> Artículo 5
> Protección de la soberanía
> 1. Los Estados partes cumplirán sus obligaciones derivadas de la presente Convención en consonancia con los principios de igualdad soberana e integridad territorial de los Estados, así como de no intervención en los asuntos internos de otros Estados. 2. Nada de lo dispuesto en la presente Convención facultará a un Estado parte para

ejercer, en el territorio de otro Estado, jurisdicción o funciones que el derecho interno de ese Estado reserve exclusivamente a sus autoridades.

Artículo 6
Respeto de los derechos humanos
1. Los Estados partes velarán por que el cumplimiento de sus obligaciones con arreglo a la presente Convención se ajuste a sus obligaciones en virtud del derecho internacional de los derechos humanos. 2. Nada de lo dispuesto en la presente Convención se interpretará en el sentido de que permita la supresión de los derechos humanos o las libertades fundamentales, incluidos los derechos relacionados con las libertades de expresión, de conciencia, de opinión, de religión o creencia, de reunión pacífica y de asociación, de conformidad y en consonancia con el derecho internacional de los derechos humanos aplicable.

Respecto a los organismos especializados de la ONU, con competencia internacional en materia de ciberseguridad y con incidencia en la República Bolivariana de Venezuela nos referimos a la Unión Internacional de Telecomunicaciones, que en lo adelante denominamos UIT…

Artículo 8
Interceptación ilícita
1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno la interceptación deliberada y sin derecho, por medios técnicos, de transmisiones no públicas de datos electrónicos a un sistema de tecnología de la información y las comunicaciones, desde él o dentro de él, incluidas las emisiones electromagnéticas provenientes de un sistema de tecnología de la información y las comunicaciones que transporten esos datos electrónicos. 2. Los Estados partes podrán exigir como requisito que el delito se cometa con intención deshonesta o delictiva o en relación con un sistema de tecnología de la información y las comunicaciones que esté conectado a otro sistema de tecnología de la información y las comunicaciones.

Artículo 9
Interferencia con datos electrónicos
1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno todo acto deliberado y sin derecho que dañe, borre, deteriore, altere o suprima datos electrónicos. 2. Los Estados partes podrán exigir como requisito que los actos descritos en el párrafo 1 del presente artículo comporten daños graves.

Artículo 16
Difusión no consentida de imágenes de carácter íntimo
1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno la venta, distribución, transmisión, publicación o facilitación de otra manera, de forma deliberada y sin derecho, de una imagen de carácter íntimo de una persona por medio de un sistema de tecnología de la información y las comunicaciones, sin el consentimiento de la persona mostrada en la imagen. 2. A los efectos del párrafo 1 del presente artículo, por 'imagen de carácter íntimo' se entenderá un registro visual de una persona mayor de 18 años de edad captado por cualquier medio, con inclusión de un registro fotográfico o videográfico, que sea de carácter sexual, en el cual estén expuestas las partes íntimas de la persona o esta realice actividades sexuales, que fuera privado en el momento de captarse y respecto del cual la persona o personas mostradas tuvieran una expectativa razonable de privacidad en el momento de cometerse el delito. 3. Un Estado parte podrá ampliar la definición del término 'imagen de carácter íntimo', según proceda, a las representaciones de personas menores de 18 años de edad si han alcanzado la edad mínima legal para realizar actividades sexuales establecida en el derecho interno y la imagen no muestra abusos o explotación de niños. 4. A los efectos del presente artículo, una persona menor de 18 años de edad mostrada en una imagen de carácter íntimo no puede consentir la difusión de una imagen de carácter íntimo que constituya material que muestre abusos sexuales de niños o explotación sexual de niños en virtud del artículo 14 de esta

Convención. 5. Los Estados partes podrán exigir como requisito que exista el propósito de causar daños para que se considere que existe responsabilidad penal. 6. Los Estados partes podrán adoptar otras medidas en relación con los asuntos vinculados al presente artículo, de conformidad con su derecho interno y en consonancia con las obligaciones internacionales aplicables[6].

Respecto a los organismos especializados de la ONU, con competencia internacional en materia de ciberseguridad y con incidencia en la República Bolivariana de Venezuela nos referimos a la Unión Internacional de Telecomunicaciones, que en lo adelante denominamos UIT, encargado de regular las telecomunicaciones a nivel internacional entre los Estados miembros y las empresas operadoras[7].

Según la *Gaceta Oficial* de la República Bolivariana de Venezuela de fecha 3 de enero de 2005, No. Extraordinario 5.754 se publicó la *Ley aprobatoria de las enmiendas a la constitución y al convenio constitutivo de la UIT*, adoptadas por la Conferencia Plenipotenciaria en Mineapolis el 6 de noviembre de 1998.

Según esta Ley Aprobatoria, entre las estructuras que conforman la UIT está el sector de normalización de las telecomunicaciones incluida las Asambleas Mundiales de Normalización de las Telecomunicaciones. Este sector tiene por objeto cumplir parte de sus funciones a través de las Asambleas Mundiales de la Normalización de las Telecomunicaciones y la Oficina de Normalización de las Telecomunicaciones que es dirigida por un director de elección. Son miembros de este sector, por derecho propio, la administración de los Estados miembros, dentro de los cuales se encuentra la República Bolivariana de Venezuela.

También nos podemos referir a la *Gaceta Oficial* de la República Bolivariana de Venezuela de fecha 18 de abril de 2006 en la cual se publica otra *Ley aprobatoria de las enmiendas a la constitución y convenio de la UIT* (1992). Mediante esta Ley se aprueba en todas sus partes y para que surta efectos internacionales en cuanto a la República Bolivariana se refieren el Convenio de la UIT (1992), adoptadas en la reunión de Plenipotenciarios en la ciudad de Marrakech, Reino de Marruecos en el año 2002. En estas enmiendas se ratifican las Asambleas Mundiales de Normalización de las Telecomunicaciones, se incorpora el Grupo Asesor de Normalización de las Telecomunicaciones abierto a los representantes de las administraciones de los Estados miembros y la Oficina de Normalización de las Telecomunicaciones. Esta Asamblea de Normalización de las Telecomunicaciones referida en el artículo 13 de este Instrumento legal, en el año 2016, aprobó la Resolución No. 50 sobre ciberseguridad que analizaremos en lo adelante.

La Resolución No. 50 sobre ciberseguridad aprobada en la Asamblea Mundial de la UIT sobre la normalización de las telecomunicaciones, Hammamet (25 de octubre-3 de noviembre de 2016)

La Asamblea Mundial de la UIT sobre la Normalización de las Telecomunicaciones, Hammamet (25 de octubre-3 de noviembre de 2016) aprobó la Resolución No. 50 sobre Ciberseguridad[8], cuyos considerandos y resolución enunciamos a continuación:

Considerando

- La importancia vital de la infraestructura de las telecomunicaciones/TIC y sus aplicaciones para prácticamente todas los tipos de actividades sociales y económicas;
- Que si no se tiene el debido cuidado en el diseño y la gestión de la seguridad, las redes IP ofrecen una separación limitada entre los componentes de usuario y los componentes de red;
- Que si no se tiene especial cuidado en el diseño y la gestión de la seguridad, las redes heredadas y las redes IP convergentes son potencialmente más vulnerables a la intrusión;
- Que la seguridad es una cuestión intersectorial y que el panorama de la ciberseguridad es complejo y diverso, en el que intervienen distintos actores en los planos nacional, regional y mundial, que son responsables de identificar, examinar y reaccionar a las cuestiones relacionadas con la creación de confianza y seguridad en la utilización de las TIC;
- Que las pérdidas considerables y crecientes en que han incurrido los usuarios de sistemas de

telecomunicaciones/TIC, a consecuencia del problema cada vez mayor de la ciberseguridad, alarman a todos los países desarrollados y en desarrollo sin excepción;

- Que debido, entre otras cosas, a que las infraestructuras esenciales de telecomunicaciones/TIC están interconectadas a escala mundial, la seguridad insuficiente de la infraestructura de un país podría aumentar la vulnerabilidad y el riesgo en otros países, por lo que la cooperación es importante; que el número y métodos de ciberataques y los ciberataques están aumentando, del mismo modo que la dependencia de Internet y otras redes que son necesarias para acceder a servicios e información;

- Que, a fin de proteger las infraestructuras mundiales de telecomunicaciones/TIC contra las amenazas y los peligros del cambiante panorama de la ciberseguridad, es necesario tomar medidas coordinadas a escala nacional, regional e internacional que sirvan para prevenir, preparar, responder y recuperarse de incidentes de seguridad;

Resuelve

- Seguir atribuyendo gran prioridad a esta actividad en la UIT, de conformidad con sus competencias y conocimientos técnicos, en particular mediante la promoción del entendimiento común entre los gobiernos y otras partes interesadas acerca de la creación de confianza y seguridad en la utilización de las TIC en los planos nacional, regional e internacional;

- Seguir evaluando las recomendaciones de todas las Comisiones de Estudio del UIT-T tanto las existentes como las que están en curso de elaboración en lo que se refiere a la robustez de su diseño y a su posible explotación por grupos malintencionados y tengan en cuenta los nuevos servicios y aplicaciones que debe soportar la infraestructura mundial de telecomunicaciones TIC (por ejemplo, computación en la nube e Internet de las cosas, que se basan en redes de telecomunicaciones; necesidad de fortalecer y defenderlos de las ciberamenazas y ciberataques, y siga fomentando la cooperación entre las organizaciones internacionales y regionales correspondientes a efectos de aumentar el intercambio de información técnica en el campo de la seguridad de las redes de información y telecomunicaciones;

- Definir un plan de acción para evaluar las Recomendaciones del UIT-T, actuales, modificadas y nuevas en cuanto a las vulnerabilidades de seguridad y siga presentando informes periódicos sobre seguridad de las telecomunicaciones/TIC al Grupo Asesor de Normalización de las Telecomunicaciones (GANT); que las Comisiones de Estudio del UIT-T sigan estableciendo relaciones de coordinación con organizaciones de normalización y otros organismos activos en este campo;

- Tomar en cuenta los aspectos de seguridad en todos los procesos de elaboración de normas del UIT-T;

La Resolución No. 50 *in comento* asigna al director de la Oficina de Normalización de las Telecomunicaciones las siguientes funciones:

- Seguir manteniendo, a partir de la información asociada con el Plan de Normalización de Seguridad de las TIC y los trabajos del UIT-D en materia de ciberseguridad, y con la asistencia de otras organizaciones pertinentes, un inventario de iniciativas y actividades nacionales, regionales e internacionales dirigidas a fomentar, en la medida de lo posible, la armonización a escala mundial de las estrategias y enfoques adoptados en esta esfera fundamental;

- Contribuir en los informes anuales al Consejo de la UIT relativos a la creación de confianza y seguridad en la utilización de las TIC, según lo dispuesto en la Resolución 130 (Rev. Busán, 2014) de la Conferencia de Plenipotenciarios;

- Informar sobre los progresos logrados en las actividades del "Plan de normalización de la seguridad de las TIC" al Consejo de la UIT;

- Seguir en la realización y seguimiento de las actividades pertinentes de la Cumbre Mundial de la Sociedad de la Información, en lo adelante CMSI sobre la creación de confianza y seguridad en el uso de las TIC, en colaboración con otros Sectores de la UIT y en cooperación con las partes interesadas correspondientes como manera de compartir a escala mundial la información sobre iniciativas de ciberseguridad nacionales, regionales, internacionales y no discriminatorias;

- Colaborar con la Agenda de Ciberseguridad Global (ACG) del Secretario General y con otros proyectos mundiales o regionales de ciberseguridad, según proceda, que entable relaciones y asociaciones, según el caso, con diversas organizaciones e iniciativas regionales e internacionales referentes a la ciberseguridad, e invite a todos los Estados Miembros, en especial a los países en desarrollo, a que tomen parte en las actividades, garantizando la cooperación y coordinación entre estas diversas actividades;
- Ayudar al Director de la Oficina de Desarrollo de las Telecomunicaciones a prestar asistencia a los Estados Miembros en el establecimiento de un marco adecuado entre los países en desarrollo, que permita reaccionar rápidamente en caso de incidentes importantes y que proponga un plan de acción destinado a reforzar la protección en estos países, teniendo en cuenta los mecanismos y asociaciones pertinentes;
- Ayudar en las actividades pertinentes de las Comisiones de Estudio del UIT-T relacionadas con el fortalecimiento y la creación de confianza y seguridad en la utilización de las TIC,

La Resolución No. 50 invita a los Estados miembros, a realizar las siguientes actividades:

- Colaborar estrechamente en el fortalecimiento de la cooperación regional e internacional, con el fin de mejorar la confianza y seguridad en la utilización de las TIC y mitigar los riesgos y las amenazas;
- Cooperar y participar activamente en la aplicación de la Resolución no. 50 y de las medidas asociadas;
- Trabajar en actividades pertinentes de las Comisiones de Estudio del UIT-T para desarrollar normas y directrices de ciberseguridad a fin de crear confianza y seguridad en la utilización de las TIC;
- Utilizar las Recomendaciones y Suplementos pertinentes del UIT-T.

La UIT, a través de la Resolución No. 50, exige a los Estados miembros de la unión colaboración y participación en el tratamiento jurídico de esta materia, buscando realizar un sistema estándar de protección contra los ciberataques en el mundo. No es una materia que se puede regular en forma aislada del resto de los países en el mundo.

La ciberseguridad, en su regulación jurídica, debe desarrollarse en coherencia y coexistencia con los acuerdos y tratados internacionales vinculantes para Venezuela. Por esta razón, El CNC debe canalizar sus recomendaciones dentro del contexto de la legislación nacional vigente en la materia y en coherencia y concordancia con la Resolución No. 50 de la UIT y con la Convención de la ONU contra la Ciberdelincuencia.

… la Resolución No. 50, exige a los Estados miembros de la unión colaboración y participación en el tratamiento jurídico de esta materia, buscando realizar un sistema estándar de protección contra los ciberataques en el mundo. No es una materia que se puede regular en forma aislada del resto de los países en el mundo.

La República Bolivariana de Venezuela estuvo presente en la reciente y última 24ª Asamblea Mundial de la Normalización de las Telecomunicaciones (WTSA-24), que se realizó entre los días 15 y 24 de octubre de 2024, en la ciudad de Nueva Delhi[9]

El jefe de Gobierno indio resaltó en esta Asamblea que ante la omnipresencia y la naturaleza sin fronteras de las herramientas y aplicaciones digitales, ningún país puede proteger de forma individual a sus ciudadanos de las amenazas cibernéticas.

En relación al tercer considerando del Decreto de creación del CNC, se observa que más allá de un considerando, estamos en presencia de una grave denuncia dirigida a los dueños y llamados magnates de las empresas fabricantes de tecnología. Dicho considerando es del tenor siguiente:

La República Bolivariana de Venezuela ha sido y será víctima de repetidas agresiones telemáticas que han pretendido afectar las decisiones soberanas del pueblo Venezolano durante los comicios electorales, entre otras, por parte de grandes magnates, dueños de empresas fabricantes de tec-

nología que han demostrado su parcialidad por intereses económicos, políticos e injerencistas, usando las tecnologías de información y comunicación como herramienta de operación de la delincuencia organizada transnacional, ciberterrorismo y la desestabilización política.

Consideramos que el lenguaje utilizado en este considerando no obedece a una sana técnica legislativa. De ser cierto lo afirmado, el mecanismo legal a utilizarse está contemplado en las disposiciones aprobadas por la Convención de las Naciones Unidas contra la Ciberdelincuencia.

Esta denuncia fue planteada por el ministro del Poder Popular para Relaciones Exteriores, Iván Gil, en fecha 8 de octubre de 2024, en el seno de la ONU, y en el contexto de la adopción de la Convención de las Naciones Unidas contra la Ciberdelincuencia[10].

Consideramos que el lenguaje utilizado en este considerando no obedece a una sana técnica legislativa. De ser cierto lo afirmado, el mecanismo legal a utilizarse está contemplado en las disposiciones aprobadas por la Convención de las Naciones Unidas contra la Ciberdelincuencia.

El Derecho Internacional, el ciberespacio y la ciberseguridad

En base a los argumentos legales expuestos ratificamos que el tratamiento jurídico sobre el ciberespacio y, por ende, de la ciberseguridad, no se puede desarrollar y regular en forma aislada, sino en forma coordinada e integrada con el resto de los países, buscando un entendimiento común.

En este sentido observamos que los países miembros de la Unión Europea, en el mes de noviembre de 2024 aprobaron una Declaración sobre un entendimiento común de la aplicación del Derecho Internacional en el ciberespacio el cual citamos a continuación:

> La Declaración indica que el Derecho internacional sigue siendo adecuado en ese ámbito digital y reitera que los Estados deben cumplir determinadas normas y obligaciones cuando llevan a cabo actividades en el ciberespacio. La Declaración reconoce que la escala, la gravedad, la sofisticación y las repercusiones de las actividades maliciosas en el ciberespacio, entre ellas los programas de secuestro, van en aumento, lo que supone un reto y una amenaza importantes para el funcionamiento de las sociedades, las economías y el modo de vida europeos. Sin embargo, el ciberespacio no es un ámbito sin ley. El respeto del marco de las Naciones Unidas para el comportamiento responsable de los Estados en el ciberespacio y la adhesión a él siguen siendo esenciales para mantener la paz, la seguridad y la estabilidad internacionales. Por consiguiente, la UE y sus Estados miembros reafirman su absoluta determinación de aplicar el marco de las Naciones Unidas para el comportamiento responsable de los Estados en el ciberespacio, adoptado por consenso y respaldado en varias ocasiones por la Asamblea General de las Naciones Unidas, que afirma, entre otras cosas, que el Derecho internacional, en particular la Carta de las Naciones Unidas, el Derecho internacional de los derechos humanos y el Derecho internacional humanitario, se aplica plenamente en el ciberespacio.
>
> La UE y sus Estados miembros seguirán trabajando con socios internacionales a fin de establecer el Programa de Acción, un mecanismo de las Naciones Unidas único, permanente, inclusivo, regular y orientado a la acción para poner en práctica y promover el comportamiento responsable de los Estados en el ciberespacio.
>
> Con esta Declaración, la UE y sus Estados miembros demuestran que es posible llegar a un entendimiento común sobre un conjunto de principios y normas fundamentales del Derecho internacional aplicables en el ciberespacio.
>
> Un mejor entendimiento común a nivel mundial sobre la manera en que se aplica el Derecho internacional en el ciberespacio contribuye a aumentar la ciberresiliencia mundial y a reforzar la transparencia, la previsibilidad y la rendición de cuentas en lo que se refiere a la conducta de los Estados en el ciberespacio. En este sentido, la UE y sus Estados miembros siguen apoyando a terceros países mediante formación y el desarrollo de capacidades sobre la aplicación del marco de las Naciones Unidas para el comportamiento responsable de los

> Estados en el ciberespacio, en particular sobre cómo desarrollar una posición regional, nacional o internacional relativa a la aplicación del Derecho internacional en el ciberespacio[11].

También amerita referirnos al Reglamento de Ciberresiliencia 2024/2847 del Parlamento Europeo y del Consejo de la Unión, de fecha 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales.

> Este Reglamento tiene por objeto fijar condiciones límite que permitan el desarrollo de productos con elementos digitales seguros, garantizando que los productos consistentes en equipos y programas informáticos se introduzcan en el mercado con menos vulnerabilidades y que los fabricantes se tomen en serio la seguridad a lo largo de todo el ciclo de vida de un producto. También aspira a crear condiciones que permitan a los usuarios tener en cuenta la Ciberseguridad a la hora de elegir y utilizar productos con elementos digitales, por ejemplo, mejorando la transparencia con respecto al período de soporte de los productos con elementos digitales comercializados[12].

ANÁLISIS JURÍDICO SOBRE EL ARTICULADO DEL DECRETO DE CREACIÓN DEL CNC Y SU ÁMBITO DE APLICACIÓN

En esta segunda parte del trabajo procedemos a analizar el conjunto de artículos que conforman el Decreto y su ámbito de aplicación, como organismo de consulta dependiente del presidente de la República. En este sentido esbozaremos la relación del Decreto con la Ley contra los Delitos Informáticos publicada en *Gaceta Oficial* de fecha 30 de octubre de 2001, bajo el No. 37.313 y la coexistencia que debe existir entre las normas nacionales especiales en la materia y la legislación internacional aplicable en la misma.

El CNC como organismo de consulta dependiente del presidente de la República y su campo de aplicación de consulta y asesoramiento

Según el artículo 1º del Decreto, se crea el CNC, con carácter permanente como órgano asesor y de consulta dependiente del presidente de la República Bolivariana de Venezuela en materia de la prevención de los usos delictivos de las TIC, cuyo funcionamiento se rige según dicho Decreto.

Como se puede apreciar, el CNC es un organismo de asesoría y consulta permanente dependiente del presidente de la República, el cual no tiene funciones ejecutivas. Su ámbito de aplicación como órgano administrativo de consulta va dirigido específicamente a la prevención de los usos delictivos de las TIC en el ciberespacio.

En este sentido, debemos referirnos a la Ley contra Delitos Informáticos que en lo adelante denominamos LCDI y que configura la materia legal especial en materia de delitos informáticos.

Como se puede apreciar, el CNC es un organismo de asesoría y consulta permanente dependiente del presidente de la República, el cual no tiene funciones ejecutivas. Su ámbito de aplicación como órgano administrativo de consulta va dirigido específicamente a la prevención de los usos delictivos de las TIC en el ciberespacio.

Partimos de la premisa según la cual, el ciberespacio está regulado por un conjunto de normas y principios jurídicos que tienen como objetivo mantener la estabilidad y seguridad en el entorno digital por aire (en la esfera terrestre y ultraterrestre donde orbitan los satélites de comunicación y por la fibra a nivel nacional de los Estados y a nivel internacional por los cables submarinos). En el entorno digital existen una serie de conceptos técnicos especiales, de obligatorio conocimiento, muchos de los cuales están definidos en el artículo 2 de la LCDI, que referimos continuación:

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

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

c) Data (datos): hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por seres humanos o por medios automáticos y a los cuales se les asigna o se les puede asignar un significado.

d) Información: significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas.

e) Documento: registro incorporado en un sistema en forma de escrito, video, audio o cualquier otro medio, que contiene data o información acerca de un hecho o acto capaces de causar efectos jurídicos.

f) Computador: dispositivo o unidad funcional que acepta data, la procesa de acuerdo con un programa guardado y genera resultados, incluidas operaciones aritméticas o lógicas.

g) Hardware: equipos o dispositivos físicos considerados en forma independiente de su capacidad o función, que conforman un computador o sus componentes periféricos, de manera que pueden incluir herramientas, implementos, instrumentos, conexiones, ensamblajes, componentes y partes.

h) Firmware: programa o segmento de programa incorporado de manera permanente en algún componente del hardware.

i) Procesamiento de datos o de información: realización sistemática de operaciones sobre data o sobre información, tales como manejo, fusión, organización o cómputo.

j) Seguridad: condición que resulta del establecimiento y mantenimiento de medidas de protección, que garanticen un estado de inviolabilidad de influencias o de actos hostiles específicos que puedan propiciar el acceso a la data de personas no autorizadas, o que afecten la operatividad de las funciones de un sistema de computación.

k) Virus: programa o segmento de programa indeseado que se desarrolla incontroladamente y que genera efectos destructivos o perturbadores en un programa o componente del sistema.

l) Tarjeta inteligente: rótulo, cédula o carnet que se utiliza como instrumento de identificación; de acceso a un sistema; de pago o de crédito, y que contiene data, información o ambas, de uso restringido sobre el usuario autorizado para portarla.

m) Contraseña (password): secuencia alfabética, numérica o combinación de ambas, protegida por reglas de confidencialidad, utilizada para verificar la autenticidad de la autorización expedida a un usuario para acceder a la data o a la información contenidas en un sistema.

n) Mensaje de datos: cualquier pensamiento, idea, imagen, audio, data o información, expresados en un lenguaje conocido que puede ser explícito o secreto (encriptado), preparados dentro de un formato adecuado para ser transmitido por un sistema de comunicaciones.

Consideramos necesario referirnos también al Decreto Nº 1.204 con Rango y Fuerza de Ley de Mensajes de Datos y Firmas Electrónicas publicado en la *Gaceta Oficial* de la República Bolivariana de Venezuela el 28 de febrero de 2001 bajo el no 37.148.

Dicho Decreto tiene por objeto otorgar y reconocer eficacia y valor jurídico a la firma electrónica, al mensaje de datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los proveedo-

res de servicios de certificación y los certificados electrónicos.

En su artículo 2, se consagran conceptos técnicos en la materia que amerita mencionarse y los cuales referimos a continuación:

> Persona: Todo sujeto jurídicamente hábil, bien sea natural, jurídica, pública, privada, nacional o extranjera, susceptible de adquirir derechos y contraer obligaciones.
> Mensajes de Dato: Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.
> Emisor: Persona que origina un Mensaje de Datos por sí mismo, o a través de terceros autorizados.
> Firma Electrónica: Información creada o utilizada por el Signatario, asociada al Mensaje de Datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado.
> Signatario: Es la persona titular de una Firma Electrónica o Certificado Electrónico.
> Destinatario: Persona a quien va dirigido el Mensaje de Datos.
> Sistema de Información: Aquel utilizado para generar, procesar o archivar de cualquier forma mensajes de datos.
> Usuario: Toda persona que utilice un sistema de información.

Enunciados estos conceptos tecnológicos del entorno digital del ciberespacio, y refiriéndonos a la prevención de los usos delictivos de las TIC que refiere el Decreto en su artículo 1, observamos en los artículos de la LCDI la tipificación de los siguientes delitos informáticos que se configuran en el entorno digital del ciberespacio y que se configuran como mecanismos de aplicación contra la ciberdelincuencia, los cuales mencionamos a continuación:

> Capítulo I. Delitos Contra los Sistemas que Utilizan Tecnologías de Información.
> Artículo 6. Acceso indebido.
> Artículo 7. Sabotaje o daño a sistemas.
> Artículo 8. Favorecimiento culposo del sabotaje o daño.
> Artículo 9. Acceso indebido o sabotaje a sistemas protegidos.
> Artículo 10. Posesión de equipos o prestación de servicios de sabotaje.
> Artículo 11. Espionaje informático.
> Artículo 12. Falsificación de documentos.
>
> Capítulo II. Delitos Contra la Propiedad.
> Artículo 13. Hurto.
> Artículo 14. Fraude.
> Artículo 15. Obtención indebida de bienes o servicios.
> Artículo 16. Manejo fraudulento de tarjetas inteligentes o instrumentos análogos.
> Artículo 17. Apropiación de tarjetas inteligentes o instrumentos análogos.
> Artículo 18. Provisión indebida de bienes o servicios.
> Artículo 19. Posesión de equipo para falsificaciones.
>
> Capítulo III. Delitos Contra la Privacidad de las Personas y de las Comunicaciones.
> Artículo 20. Violación de la privacidad de la data o información de carácter personal.
> Artículo 21. Violación de la privacidad de las comunicaciones.
> Artículo 22. Revelación indebida de data o información de carácter personal.
> Capítulo IV. Delitos Contra Niños, Niñas o Adolescentes.
> Artículo 23. Difusión o exhibición de material pornográfico.
> Artículo 24. Exhibición pornográfica de niños o adolescentes.
> Capítulo V. Delitos Contra el Orden Económico.
> Artículo 25. Apropiación de propiedad intelectual.
> Artículo 26. Oferta engañosa[13].

También debemos hacer referencia a la Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo[14] . Tanto en los tratados internacionales, como en los considerandos y el articulado del Decreto aquí analizados se hace referencia al ciberterrorismo como una de las actividades objeto de regulación de la ciberseguridad.

En este sentido el ciberterrorismo es una forma de terrorismo en la que los grupos agresores emplean medios digitales para atacar ordenadores, telecomunicaciones e información privada con el objetivo de intimidar o coaccionar a un Gobierno o población. Sus fines pueden ser políticos, sociales o religiosos. Es una amenaza en auge desde finales de los años noventa que crece conforme las sociedades aumentan su dependencia tecnológica. Cualquier fallo, intrusión o ataque en los sistemas informáticos puede causar daños irreparables en infraestructuras básicas de la comunidad, y los terroristas aprovechan esta vulnerabilidad como elemento de presión[15].

En este sentido es importante conocer la definición legislativa nacional sobre el terrorismo. Esta ley consagra en su artículo 4 la definición de "Acto terrorista" el cual citamos a continuación:

> Acto terrorista: es aquel acto intencionado que por su naturaleza o su contexto, pueda perjudicar gravemente a un país o a una organización internacional tipificado como delito según el ordenamiento jurídico venezolano, cometido con el fin de intimidar gravemente a una población; obligar indebidamente a los gobiernos o a una organización internacional a realizar un acto o a abstenerse de hacerlo; o desestabilizar gravemente o destruir las estructuras políticas fundamentales, constitucionales, económicas o sociales de un país o de una organización internacional.

Tanto en los tratados internacionales, como en los considerandos y el articulado del Decreto aquí analizados se hace referencia al ciberterrorismo como una de las actividades objeto de regulación de la ciberseguridad.

Podemos observar que estamos en presencia de una definición compleja impregnada de conceptos subjetivos indeterminados. Es un campo de apreciación donde la tolerancia y prudencia en la autoridad pública es pilar fundamental para apreciar y juzgar el hecho de manera justa sin perjudicar los derechos humanos del ciudadano. Para que se configure el acto terrorista se requiere:

1. Que el acto sea intencionado;
2. Que esté tipificado como delito en el ordenamiento jurídico venezolano;
3. Que sea cometido con el fin de intimidar gravemente a una población;
4. Que obligue indebidamente a los gobiernos o a una organización internacional a realizar un acto o a abstenerse de hacerlo;
5. Que obligue a desestabilizar gravemente; o destruir las estructuras políticas fundamentales, constitucionales, económicas o sociales de un país o de una organización internacional.

Así mismo, el legislador nacional define como actos terroristas los que se realicen o ejecuten a través de los siguientes medios:

a. atentados contra la vida de una persona que puedan causar la muerte;
b. atentados contra la integridad física de una persona;
c. secuestro o toma de rehenes;
d. causar destrucciones masivas a un gobierno o a instalaciones públicas, sistemas de transporte, infraestructuras, incluidos los sistemas de información, plataformas fijas o flotantes emplazadas en la zona económica exclusiva o en la plataforma continental, lugares públicos o propiedades privadas que puedan poner en peligro vidas humanas o producir un gran perjuicio económico;
e. apoderamiento de aeronaves y de buques o de otros medios de transporte colectivo, o de mercancías;
f. fabricación, tenencia, adquisición, transporte, suministro, desarrollo o utilización de armas de fuego, explosivos, armas nucleares, biológicas y químicas;
g. liberación de sustancias peligrosas, o provocación de incendios, inundaciones o explosiones cuyo efecto sea poner en peligro vidas humanas;
h. perturbación o interrupción del suministro de agua, electricidad u otro recurso natural fundamental cuyo efecto sea poner en peligro vidas humanas.

El literal d) antes citado se refiere al acto terrorista que se ejecuta a través de infraestructuras, sistemas de información, plataformas fijas o

flotantes emplazadas en la zona económica exclusiva o en la plataforma continental que puedan poner en peligro vidas humanas o producir un gran perjuicio económico. Es el acto terrorista cometido en el entorno digital del ciberespacio, el cual lo califica la ciberseguridad como ciberterrorismo.

Integrantes del CNC

El CNC está integrado por los representantes de los siguientes organismos públicos.

1. Vicepresidencia ejecutiva de la República Bolivariana de Venezuela.
2. Ministerio del Poder Popular para la Defensa.
3. Ministerio del Poder Popular para la Ciencia y Tecnología.
4. Ministerio del Poder Popular de Economía, Finanzas y Comercio Exterior.
5. Ministerio del Poder Popular para Relaciones Exteriores.
6. Ministerio del Poder Popular para Relaciones Interiores, Justicia y Paz.
7. Ministerio del Poder Popular para la Planificación.
8. Ministerio del Poder Popular de Comercio Nacional.

El CNC tendrá un coordinador designado por el presidente de la República, a cuyo cargo estará la convocatoria a las sesiones del Consejo, el levantamiento de las actas y demás documentos emanados este. El coordinador del CNC actuará de conformidad con las instrucciones que le imparta el ministro de la Presidencia y Seguimiento de la Gestión de Gobierno que es el organismo encargado de la ejecución del Decreto[16].

Eventualmente, el CNC debe convocar a sus reuniones a representantes de otros órganos y entes del Poder Público, del sector empresarial público y privado y de las diferentes instancias de base del Poder Popular para que las consultas coadyuven al logro de sus fines. Así mismo, el presidente de la República y el coordinador del CNC, tienen la facultad para integrar otros miembros al Consejo.

Funciones del CNC

Analizado el ámbito de aplicación sobre el cual consideramos debe actuar como órgano de consulta y asesoría el CNC, pasamos a enunciar las funciones que le asigna el Decreto de creación.

1. Asesorar al presidente de la República y al Consejo de Defensa de la Nación en la elaboración de la política nacional de ciberseguridad que contenga los planes y programas de seguridad informática, vigilancia tecnológica, supervisión y control de incidentes telemáticos.
2. Elevar propuestas de regulaciones, leyes y/o reglamentos en materia de prevención de uso de las TIC con fines delictivos. Como se puede apreciar, sus funciones de consulta y asesoría van dirigidas fundamentalmente a los usos delictivos que se cometen en el ciberespacio, lo cual coincide con los postulados internacionales analizados.
3. Verificar el grado de cumplimiento de la implementación de los planes y regulaciones adoptados en materia de ciberseguridad. En estos planes se debe considerar e implementar los de la ONU y los de la UIT antes analizados.
4. Formular propuestas y recomendaciones sobre la política de ciberseguridad, en armonía con los intereses y objetivos de la Nación para garantizar los fines supremos del Estado. Igualmente, en esta función se deben contemplar los postulados internacionales aprobados por la ONU y la UIT.
5. Realizar la valoración continua de riesgos y amenazas en materia de seguridad informática.
6. Impulsar la constitución de una red de vigilancia durante 24 horas de incidentes telemáticos, afiliada a los pares regionales para prevenir, mitigar y/o controlar los delitos informáticos transfronterizos, de conformidad con el artículo 41 del documento de Naciones Unidas para la prevención del ciberdelito. Esta función está directamente referida al artículo 41 de la Convención de las Naciones Unidas contra la Ciberdelincuencia. *Fortalecimiento de la cooperación internacional para la lucha contra determinados delitos cometidos mediante sistemas de TIC* y para la *Transmisión de pruebas en forma electrónica de delitos graves*. Este artículo es del tenor siguiente:

1. Cada Estado parte designará un punto de contacto que estará disponible las 24 horas del día, los siete días de la semana, a fin de garantizar la prestación de asistencia inmediata a efectos de investigaciones, acciones o procesos judiciales penales específicos en relación con delitos tipificados con arreglo a la presente Convención o de la recolección, obtención y conservación de pruebas en forma electrónica a los efectos del párrafo 3 del presente artículo y en relación con los delitos tipificados con arreglo a la presente Convención, así como con delitos graves.
2. Dicho punto de contacto se notificará al Secretario o Secretaria General de las Naciones Unidas, quien llevará un registro actualizado de los puntos de contacto designados a los efectos del presente artículo y transmitirá anualmente a los Estados partes la lista actualizada de puntos de contacto.
3. Esa asistencia comprenderá la facilitación o, si el derecho y la práctica internos del Estado parte requerido lo permiten, la aplicación directa de las medidas que figuran a continuación:
a) La prestación de asesoramiento técnico;
b) La conservación de los datos electrónicos almacenados con arreglo a los artículos 42 y 43 de la presente Convención, incluida, según proceda, información sobre la ubicación del proveedor de servicios, si el Estado parte requerido la conoce, a fin de ayudar al Estado parte requirente a formular una solicitud;
c) La recolección de pruebas y el suministro de información de carácter jurídico;
d) La localización de personas sospechosas; o
e) El suministro de datos electrónicos para evitar que se produzca una emergencia.
4. El punto de contacto de un Estado parte dispondrá de los medios necesarios para comunicarse de manera acelerada con el de otro Estado parte. Si el punto de contacto designado por un Estado parte no forma parte de la autoridad o autoridades de ese Estado parte responsables de la asistencia judicial recíproca o de la extradición, dicho punto de contacto se asegurará de poder actuar de manera acelerada en coordinación con esa autoridad o autoridades.
5. Cada Estado parte velará por que se disponga de personal capacitado y equipado para asegurar el funcionamiento de la red 24/7.
6. Los Estados partes también podrán utilizar y reforzar las redes autorizadas de puntos de contacto existentes, cuando proceda y dentro de los límites de su derecho interno, entre ellas las redes de funcionamiento continuo sobre delitos relacionados con computadoras de la Organización Internacional de Policía Criminal para una cooperación interpolicial rápida y otros métodos de cooperación mediante el intercambio de información.
7. Constituir comités de trabajo interinstitucionales y de emergencia, para la atención y prevención del uso de las TIC con fines delictivos.
8. Requerir de las personas naturales o jurídicas de carácter público y privado los datos, estadísticas e informaciones relacionados con la seguridad informática de la Nación, así como su necesario apoyo.
9. Impulsar programas de capacitación en materia de ciberseguridad con instituciones educativas, centros de investigación y entidades públicas y privadas.
10. Fomentar la formación de equipos multidisciplinarios especializados en ciberseguridad del sector público y privado.
11. Promover las inversiones necesarias para el fortalecimiento de la plataforma telemática del Estado.
12. Dictar el reglamento para su organización y funcionamiento.
13. Otras que sean decididas en el seno del Consejo, al menos por las dos terceras partes de sus miembros permanentes[17].

Respecto a la función establecida en el numeral 6, observamos que esta función se consagra de conformidad con el artículo 41 de la Convención de la ONU contra la Ciberdelincuencia. Es una iniciativa importante para integrar la red de vigilancia durante 24 horas de incidentes telemáticos a un sistema internacional, que pueda combatir con mayor eficacia estos incidentes que, como ya dijimos, son cambiantes y mutantes.

RESUMEN Y CONCLUSION

En el desarrollo del análisis del Decreto de creación del CNC, así como de las nociones doctrinarias del entorno digital que conforma el ciberespacio, y de los ataques y amenazas constantes a

los cuales está sometido el mundo digital que impera en el planeta, se constata que la ciberseguridad cabalga en un ambiente internacional hostil donde el entendimiento entre los países aún sigue siendo un objetivo no logrado.

En este contexto podemos concluir:

- La Ciberseguridad es una materia que no puede interpretarse de manera aislacionista, ni puede esclavizarse a dogmas políticos nacionales de los Estados miembros de la ONU y de la UIT donde Venezuela es miembro, ya que se corre el riesgo de transformar la ciberseguridad en un mecanismo de censura tecnológica que termina afectando a los derechos humanos de los ciudadanos y beneficiando los virus tecnológicos que corroen la conectividad mundial de las TIC.
- Estamos viviendo una nueva guerra fría; en esta oportunidad cibernética, donde los grandes consorcios tecnológicos, tanto fabricantes de tecnologías como propietarios de las plataformas digitales mundiales, abogan por dominar los mercados sin percatarse, de manera acuciosa, que los ciberataques mundiales que acechan el entorno digital pueden provocar una anarquía sin control en perjuicio de ellos mismos.
- Las diferencias políticas e ideológicas siempre han existido y continuarán existiendo. La diversidad es una realidad que los Estados no pueden evadir y deben aceptar. Bajo esta realidad, se debe buscar un entendimiento en temas que amenazan la estabilidad de la humanidad como son, en el supuesto bajo análisis, la cibercriminalidad y el ciberterrorismo, que configuran conductas que desestabilizan al mundo. Por ello, es ineludible un entendimiento internacional.
- Venezuela cuenta con una legislación avanzada en la materia de las TIC y de las telecomunicaciones. En este sentido, la creación del CNC, como órgano de consulta gubernamental debe dar énfasis en el estudio del complejo análisis de la extraterritorialidad de la ciberseguridad.
- Uno de los temas de mayor complejidad que requiere un real asesoramiento integral, es el referente a la integración y debate de Venezuela en los acuerdos y tratados internacionales como es la Convención de las Naciones Unidas contra la Ciberdelincuencia de la ONU y la Resolución No. 50 sobre Ciberseguridad aprobada en la asamblea mundial de la UIT.
- Es deseable que la creación del CNC canalice sus actividades y funciones de asesoramiento y consulta en la dirección de contrarrestar los usos delictivos y ciberataques que afectan al ciberespacio a nivel nacional y a nivel extraterritorial, en armonía y coherencia con la garantía constitucional de los derechos humanos ciudadanos.

Notas

1 Artículo 4 de la Ley Orgánica de Telecomunicaciones vigente, *Gaceta Oficial de la República Bolivariana de Venezuela* no. 39.610 de fecha 07 de febrero de 2011.

2 https://www.swissinfo.ch/spa/birmania-promulga-la-pol%C3%A9mica-ley-de-ciberseguridad-criticada-por-vulnerar-derechos/88666522

3 https://es-us.noticias.yahoo.com/gobierno-militar-myanmar-promulga-ley-190443204.html

4 https://www.unodc.org/lpomex/es/noticias/diciembre-2024/la-asamblea-general-de-las-naciones-unidas-adopta-una-convencion-historica-contra-la-ciberdelincuencia.html

5 https://www.tiktok.com/@yvan.gilpinto/video/7401583732253232389

6 https://www.unodc.org/lpomex/es/noticias/diciembre-2024/la-asamblea-general-de-las-naciones-unidas-adopta-una-convencion-historica-contra-la-ciberdelincuencia.html

7 La UIT es el organismo de las Naciones Unidas especializado en las tecnologías de la información y la comunicación (TIC). La UIT atribuye el espectro radioeléctrico a los diferentes servicios y las órbitas de satélite a escala mundial, elabora normas técnicas que garantizan la interconexión de las redes y uso armonizado de las tecnologías, y aúna esfuerzos por mejorar el acceso a las TIC de las comunidades insuficientemente atendidas de cualquier parte del mundo.

8 Según el artículo 18 de la *Ley aprobatoria de las enmiendas a la constitución y al convenio constitutivo de la UIT*, adoptadas por la Conferencia Plenipotenciaria en Mineapolis el 6 de noviembre de 1998, publicada en la *Gaceta Oficial* de la República Bolivariana de Venezuela de fecha 3 de enero de 2005, No. Extraordinario 5.754 estas Asambleas

se celebran cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen recomendaciones sobre dichos temas.
La República Bolivariana de Venezuela estuvo presente en la última y reciente 24ª Asamblea Mundial de la Normalización de las Telecomunicaciones (WTSA-24), que se realizó entre los días 15 y 24 de octubre de 2024, en la ciudad de Nueva Delhi, India.

9 Esta Asamblea contó con la asistencia de Margalad Bencomo Noguera, directora ejecutiva de la Agencia Bolivariana para Actividades Espaciales (ABAE), quien participó en todas las jornadas del evento. La jefa de la misión diplomática venezolana en la República de la India, embajadora Capaya Rodríguez González, acompañó a la delegada nacional durante la mencionada Asamblea, siguiendo con gran interés la discusión de importantes temas en el campo de la elaboración de normas que rigen para todos los Estados miembros en el sector de las telecomunicaciones. El jefe de Gobierno indio resaltó la omnipresencia y la naturaleza sin fronteras de las herramientas y aplicaciones digitales, aseverando que ningún país puede proteger de forma individual a sus ciudadanos de las amenazas cibernéticas. Asimismo, recordó el notable progreso de la India en el campo de las telecomunicaciones. Al respecto, destacó que en tan solo diez años la India ha tendido una red de fibra óptica que abarca una distancia ocho veces mayor que la que hay entre la Tierra y la Luna.

10 Ver cita 3.

11 https://www.consilium.europa.eu/es/press/press-releases/2024/11/18/cyberspace-council-approves-declaration-to-promote-common-understanding-of-application-of-international-law/.

12 https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81720

13 Ver Ley contra los Delitos Informáticos publicada en *Gaceta Oficial* de fecha 30 de octubre de 2001, bajo el no. 37.313.

14 *Gaceta Oficial* No. 39.912 de fecha 30 de abril de 2012.

15 https://elordenmundial.com/que-es-ciberterrorismo/

16 Artículo 5 del Decreto de creación del CNC

17 Artículo 2 del Decreto de creación del CNC.

ALEJANDRO FUENMAYOR ESPINA

Doctor en Derecho por la Universidad de París I. Fue presidente del Consejo Nacional de la Cámara Venezolana de la Radiodifusión. Autor del libro *Régimen jurídico de las telecomunicaciones. Instituciones fundamentales.* Investigador Asociado del Instituto de Investigación de la Comunicación e Información de la Universidad Católica Andrés Bello.

Galería de Papel, Víctor Hugo Irazábal. Serie Libro de Artista.