LUIS ABINADER

PRESIDENTE DE LA REPÚBLICA DOMINICANA

CÁMARA DE DIPUTADOS DE LA REPÚBLICA DOMINICANA
Secretaría General
RECIBIDO
03 MAY 2023
POR JM HORA 5:50 P.M.
09531

Núm. 10679

03 MAY 2023

Sr. Alfredo Pacheco Osoria
Presidente de la Cámara de Diputados
Palacio del Congreso Nacional
Su despacho

Honorable presidente de la Cámara de Diputados:

En ejercicio de las atribuciones que me confiere el artículo 96, numeral 2, de la Constitución de la República, proclamada el 13 de junio de 2015, someto por su digna mediación a ese honorable Congreso Nacional el proyecto de ley contra la ciberdelincuencia.

El objeto de esta ley es lograr la protección integral de los sistemas que utilizan tecnologías de la información y comunicación, así como la prevención, persecución y sanción de dos tipos de delitos, por un lado, los cometidos en detrimento de tales sistemas, sus componentes o sus contenidos y, por otro lado, los cometidos mediante el uso de esas tecnologías de la información y comunicación en contra de personas físicas o jurídicas.

El proyecto de ley establece su propio ámbito de aplicación, sus principios rectores y las definiciones que para su aplicación corresponden. En su parte central, el proyecto tipifica cada uno de los ciberdelitos y los clasifica de la siguiente manera:

i) Ciberdelitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas de información.

ii) Ciberdelitos contra las personas.

iii) Ciberdelitos financieros y de sustracción.

iv) Ciberdelitos contra la propiedad intelectual.

v) Ciberdelitos contra las telecomunicaciones.

vi) Ciberdelitos contra la nación y ciberterrorismo.

Particularmente sobre los ciberdelitos contra las personas, deseo hacer las siguientes aclaraciones:

a) El 14 de junio de 2022, mediante mensaje núm. 13818, remití a esa Cámara de Diputados una primera propuesta del proyecto de ley contra la ciberdelincuencia.

b) Sin embargo, mediante instrucción núm. 15395, del 29 de junio de 2022, dispuse que el consultor jurídico del Poder Ejecutivo retirara del Congreso Nacional el referido proyecto, con el propósito de que este fuera estudiado por la comisión consultiva creada mediante el decreto núm. 333-22, del 23 de junio de 2022, para la revisión y actualización de la legislación sobre la libertad de expresión.

c) En consecuencia, el consultor jurídico del Poder Ejecutivo procedió a solicitar el retiro, de manera provisional, del referido proyecto de ley, mediante su oficio núm. 0637, del 4 de julio de 2022.

d) Desde ese momento quedó apoderada la comisión consultiva para la revisión y actualización de la legislación sobre la libertad de expresión, la cual recomendó eliminar de la versión original los artículos 17, 18 y 19, referentes a los ciberdelitos de discriminación, difamación e injuria, por lo que esta nueva versión que ahora someto al Congreso Nacional no contempla esas disposiciones.

El proyecto de ley que ahora se somete también dispone los organismos competentes para la persecución y enjuiciamiento de tales delitos, dentro de los cuales se incluyen el Ministerio Público, la Comisión Interinstitucional contra el Ciberdelito, el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) y la División de Investigación de Delitos Informáticos (DIDI).

Por otro lado, el proyecto define las reglas de derecho procesal, las cuales regulan aspectos diversos, tales como las medidas de investigación, la recopilación y control de evidencias, el decomiso de bienes, la competencia jurisdiccional y la acción pública. También son contempladas de manera particular la sostenibilidad del sistema y la cooperación internacional.

Para la aplicación de las disposiciones de la ley, de conformidad con su propio texto, en un plazo de seis meses, la Comisión Interinstitucional contra el Ciberdelito deberá presentar al Poder Ejecutivo, para su aprobación, un reglamento de aplicación.

Esta ley derogaría de manera total la ley núm. 53-07 sobre crímenes y delitos de alta tecnología, la cual regula la materia en el presente. Es oportuno actualizar este marco normativo dado que muchas de las nuevas conductas ciberdelictivas que afectan hoy en día a la sociedad no cuentan con una tipificación penal.

En consecuencia, espero que los honorables legisladores impartan su voto favorable sobre este importante proyecto de ley que someto a su consideración.

LUIS ABINADER

PROYECTO DE LEY CONTRA LA CIBERDELINCUENCIA

CONSIDERANDO: Que la Constitución de la República Dominicana establece los derechos y deberes fundamentales de los ciudadanos entre los que se encuentra la libertad de expresión, la integridad e inviolabilidad de la correspondencia y demás documentos privados;

CONSIDERANDO: Que la Ley General de las Telecomunicaciones No. 153-98, del 27 de mayo de 1998, estatuye la obligación de respetar la inviolabilidad de las telecomunicaciones y prohíbe el uso de las telecomunicaciones contrario a las leyes o que tenga por objeto cometer delitos o entorpecer la acción de la justicia;

CONSIDERANDO: Que las tecnologías de la información y de la comunicación han experimentado un desarrollo impresionante, con lo que brindan un nuevo soporte para la comisión de delitos tradicionales y crean nuevas modalidades de infracciones y hechos no incriminados, afectando los intereses patrimoniales y extrapatrimoniales de las personas físicas y morales, así como del Estado y las instituciones que lo representan;

CONSIDERANDO: Que estos crímenes y delitos relacionados a las tecnologías de información y comunicación están previstos en la legislación penal dominicana mediante la ley 53-07, no obstante, por los constantes avances de las tecnologías y el incremento en el uso de servicios digitales, resulta necesaria su actualización y modificación, para asegurar la protección de los usuarios, y fortalecer los mecanismos del Estado para la detección, investigación y sanción de estos nuevos tipos de delitos;

CONSIDERANDO: Que la tipificación y prevención de los actos delictivos a sancionar han adquirido gran relevancia a nivel internacional, debido a que con el desarrollo de las tecnologías de la información y comunicación se continúan produciendo grandes retos de seguridad que inciden en la ciberdelincuencia y el ciberterrorismo.

CONSIDERANDO: Que el uso de las tecnologías de la información y comunicación se han vuelto trascendentales en los procesos de desarrollo, competitividad y cambios estructurales registrados en las vertientes económicas, políticas, sociales, culturales y empresariales del país, lo cual ha expuesto a la población a las amenazas que se producen a través de las mismas.

VISTA: La Constitución de la Republica Dominicana;

VISTA: La Declaración Universal de Derechos Humanos de 1948 y la Convención Americana sobre Derechos Humanos, suscrita en San Jose de Costa Rica, el 22 de noviembre de 1969;

VISTO: El Convenio sobre la Ciberdelincuencia del Consejo de Europa, del 23 de noviembre del 2001;

VISTA: La ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología, del 17 de enero de 2007.

VISTA: La Ley núm. 1-12, del 25 de enero de 2012, que establece la Estrategia Nacional de Desarrollo 2030;

VISTA: La Ley General de Telecomunicaciones No.153-98, del 27 de mayo de 1998;

PROYECTO DE LEY CONTRA LA CIBERDELINCUENCIA

VISTA: La Ley No.126-02, del 4 de septiembre del 2002, de Comercio Electrónico, Documentos y Firmas Digitales;

VISTO: El Código Penal de la República Dominicana, aprobado por la Cámara de Diputados de la Republica, el 26 de julio del año 2006;

VISTO: El Código Procesal Penal de la Republica Dominicana, Ley No.76-02, del 19 de julio del 2002;

VISTA: La Ley No.20-00, del 8 de mayo del 2000, de Propiedad Industrial;

VISTA: La Ley No.65-00, del 21 de agosto del 2000, del Derecho de Autor;

VISTA: La Ley No.136-03, del 7 de agosto del 2003, Código del Menor;

VISTA: La Ley No.96-04, del 28 de enero del 2004, Institucional de la Policía;

VISTA: La Ley No.137-03, del 7 de agosto del 2003, sobre Tráfico Ilícito de Migrantes y Trata de Personas;

VISTA: La ley núm. 133-11, Orgánica del Ministerio Público, del 7 de junio del 2011;

VISTA: La Ley No.50-88, del 30 de mayo de 1988, sobre Drogas y Sustancias Controladas de la Republica Dominicana;

VISTA: La Resolución AG/RES.2004 (XXXIV-0/04) del 8 de junio del 2004 de la Asamblea General de la Organización de Estados Americanos (OEA);

VISTO: El Convenio sobre la Ciberdelincuencia del Consejo de Europa, del 23 de noviembre del 2001.

HA DADO LA SIGUIENTE LEY CONTRA LA CIBERDELINCUENCIA:

TÍTULO I
DISPOSICIONES GENERALES

CAPÍTULO I
OBJETO Y ÁMBITO DE APLICACIÓN DE LA LEY

Artículo 1. Objeto. Esta ley tiene por objeto la tutela de los derechos fundamentales, a partir de la protección integral de los sistemas que utilicen tecnologías de la información y comunicación o su contenido, así como la prevención, persecución y sanción de los delitos cometidos contra éstos o cualquiera de sus componentes, o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas físicas o jurídicas en los términos previstos en esta ley. A tales fines, se consideran bienes jurídicos protegidos la integridad, confidencialidad y disponibilidad de los sistemas de información o cualquiera de sus componentes, así como la información o los datos objeto de tratamiento a través de estos.

Artículo 2. Ámbito de aplicación. Esta ley es de aplicación en el territorio de la República Dominicana a toda persona física o jurídica, nacional o extranjera, para proteger derechos fundamentales que pudiesen ser vulnerados mediante el uso de sistemas informáticos o cualquiera de sus componentes, aplicándose en las circunstancias siguientes:

a) Cuando el sujeto activo origina u ordena la acción delictiva dentro del territorio de la República Dominicana;

b) Cuando el sujeto activo origina u ordena la acción delictiva desde el extranjero, produciendo efectos en el territorio de la República Dominicana;

c) Cuando el origen o los efectos de la acción se produzcan en el extranjero, utilizando medios que se encuentran en el territorio de la República Dominicana;

d) Cuando se caracterice cualquier tipo de complicidad desde el territorio de la República Dominicana;

e) Cuando el sujeto pasivo se localice, o los efectos de la acción se produzcan en el territorio de la República Dominicana a través de servicios que se ofrezcan utilizando medios que se encuentren en el extranjero; y

f) En ocasión de las solicitudes de asistencia legal mutua o cooperación jurídica internacional.

CAPÍTULO II
PRINCIPIOS GENERALES Y DEFINICIONES

Artículo 3. Principios generales. La presente ley tendrá como principios:

Principio de Territorialidad. La jurisdicción de los delitos contenidos en la presente ley se aplicará conforme a las disposiciones del Código Procesal Penal Dominicano. En los casos de infracciones cometidas de forma remota desde el extranjero, será competente el tribunal de primera instancia del Distrito Nacional.

Principio de Razonabilidad y Proporcionalidad. Las restricciones y prohibiciones deben ser proporcionales a los fines y medios del peligro que se intenta evitar, ponderándose con prudencia las consecuencias sociales de la decisión.

Artículo 4. Definiciones. Para los fines de esta ley, se entenderá por:

a) **Afectar:** Alterar, provocar anomalías en cualquiera de las operaciones realizadas por un sistema de información o cualquiera de sus componentes, impidiendo su uso normal.

b) **Clonación:** Duplicación, copia o reproducción exacta de una serie electrónica, un número o sistema de identificación de un dispositivo, un medio de acceso a un servicio o de un sistema, o cualquiera de sus componentes.

c) **Código de Acceso:** Información o contraseña que permite autenticar y dar acceso a un individuo, dispositivo o componente del sistema de información a dicho sistema o cualquiera de sus componentes.

d) **Código de Identificación:** Información que permite identificar a un individuo, dispositivo o componente del sistema de información.

e) **Datos Informáticos:** toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema de información ejecute una función.

f) **Datos Relativos a los Usuarios:** Se entenderá toda información en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y que esté relacionada con los usuarios a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, y que permita determinar:

1) El tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el período de servicio;

2) La identidad, la dirección postal o geográfica y el número de teléfono del usuario, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios;

3) Cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios.

g) **Ciberdelito:** Aquellas conductas perjudiciales a los bienes jurídicos protegidos por la Constitución, las leyes, decretos, reglamentos y resoluciones relacionadas con los sistemas de información. Esto comprende los delitos electrónicos, informáticos, telemáticos, cibernéticos y de telecomunicaciones.

h) **Ciberpatrullaje:** Técnica de investigación ejecutada para rastrear y localizar elementos de prueba del ciberdelito y sus responsables en fuentes accesibles al público.

i) **Dispositivo:** Objeto, artículo, pieza o componente de un sistema de información.

j) **Dispositivo de Acceso:** Es toda tarjeta, placa, código, número, dispositivo electrónico, u otros medios o formas de acceso, a un sistema o parte de éste, que puedan ser usados independientemente o en conjunto con otros dispositivos, para lograr acceso a un sistema de información o a cualquiera de sus componentes.

k) **Documento Digital:** Es la información codificada en forma digital, con o sin un soporte lógico o físico, en el cual se usen métodos electrónicos, fotolitográficos, ópticos o similares, que se constituyen en representación de actos, hechos o datos jurídicamente relevantes.

l) **Fuentes Abiertas o Accesibles al Público:** Son aquellas fuentes de datos cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa. Los datos provenientes de fuentes abiertas o accesibles al público pueden ser usados, reusados y redistribuidos libremente por cualquier persona, nacional o internacional. A los fines de esta ley se consideran datos de fuentes abiertas o accesibles al público cualquiera que no requiera ningún tipo de técnica de recolección clandestina para obtenerse y que puede ser obtenida por cualquier medio, sean estos públicos o privados, de manera física o digital.

m) **Interceptación:** Apoderar, utilizar, afectar, desviar o editar de cualquier forma, un dato o una transmisión de datos perteneciente a otra persona física o jurídica, por su propia cuenta o por encargo de otro, para utilizar de algún modo o para conocer su contenido, a través de un sistema de información o de cualquiera de sus componentes.

n) **Infraestructura Crítica:** Un sistema de información que es necesario para la prestación continua de un servicio esencial, y la pérdida o el compromiso del sistema de información tendrá un efecto debilitante en la disponibilidad del servicio esencial en el país.

o) **Proveedor de Servicios:** Toda entidad pública o privada, que ofrezca a los usuarios de sus servicios la posibilidad de comunicarse a través de una plataforma o un sistema de información o cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo; o cualquier entidad que registre y gestione nombres de dominios de internet.

p) **Salario mínimo del sector público:** Se entenderá como el salario mínimo nacional más bajo percibido por los trabajadores del sector público.

q) **Señal de Disparo:** Señal generada a una plataforma la cual devuelve el tono de marcar, ya sea proveniente de un sistema de información o a través de un operador.

r) **Sistema de Información:** Dispositivo o conjunto de dispositivos que utilizan las tecnologías de información y comunicación, así como cualquier sistema, incluyendo, pero no limitado a los sistemas electrónicos, informáticos, telemáticos y de telecomunicaciones, que separada o conjuntamente sirvan para generar, enviar, recibir, archivar o procesar información, documentos digitales, mensajes de datos, entre otros.

s) **Sistema de Telecomunicaciones:** Conjunto de dispositivos relacionados, conectados o no, cuyo fin es la transmisión, emisión, almacenamiento, procesamiento y recepción de señales, señales electromagnéticas, signos, escritos, imágenes fijas o en movimiento, video, voz, sonidos, datos o informaciones de cualquier naturaleza, por medio óptico, celular, radioeléctrico, electromagnético o cualquiera otra plataforma útil a tales fines. Este concepto incluye servicios

de telefonía fija y móvil, servicios de valor agregado, televisión por cable, servicios espaciales, servicios satelitales y otros.

t) **Sujeto Activo:** Es aquel que intencionalmente viole o intente violar, por acción, omisión o por mandato, cualquiera de las actuaciones descritas en la presente ley. A los fines de esta ley se reputa como sujeto activo a los cómplices, los cuales serán pasibles de ser condenados a la misma pena que el actor principal de los delitos que tipifica.

u) **Sujeto Pasivo:** Es todo aquel que resulte afectado o amenazado en cualquiera de sus derechos por la violación de las disposiciones de esta ley.

v) **Emergencia**: Es una situación en la que existe un riesgo significativo e inminente a la vida, integridad fisica o la seguridad de cualquier persona física.

TÍTULO II
CIBERDELITOS

CAPÍTULO I
CIBERDELITOS CONTRA LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE DATOS Y SISTEMAS DE INFORMACIÓN

Artículo 5. Obtención ilícita de códigos de identificación o acceso. El hecho de divulgar, generar, copiar, grabar, capturar, alterar, traficar, desencriptar, decodificar o de cualquier modo descifrar los códigos de acceso, información o mecanismos similares, a través de los cuales se logra acceso a un sistema, de información o cualquiera de sus componentes, o falsificar cualquier tipo de dispositivo de acceso al mismo, se sancionará con la pena de dos a cinco años de prisión y multa de cincuenta a doscientas veces el salario mínimo del sector público.

Artículo 6. Clonación de dispositivos de acceso. La clonación, para la venta, distribución o cualquier otra utilización de un dispositivo de acceso a un servicio o sistema de información, mediante el copiado o transferencia, de un dispositivo a otro similar, de los códigos de identificación, serie electrónica u otro elemento de identificación y/o acceso al servicio, que permita la operación paralela de un servicio legítimamente contratado o la realización de transacciones financieras fraudulentas en detrimento del usuario autorizado del servicio, se castigará con la pena de cuatro a diez años de prisión y multa de cien a quinientas veces el salario mínimo del sector público.

Artículo 7. Acceso ilícito. El hecho de acceder de forma ilegítima y deliberada a la totalidad o a una parte de un sistema de información, o cualquiera de sus componentes, utilizando o no una identidad ajena, o excediendo una autorización, se sancionará con las penas de dos a cuatro años de prisión y multa desde cien a quinientas veces el salario mínimo del sector público.

Párrafo I. Uso de datos por acceso ilícito. Cuando de dicho acceso ilícito resulte la supresión, adición, copiado o la modificación de datos contenidos en el sistema, o indebidamente se revelen o difundan datos confidenciales contenidos en el sistema accedido, las penas se elevarán de cuatro a siete años de prisión y multa de doscientas a quinientas veces el salario mínimo del sector público.

Párrafo II. Explotación ilegítima de acceso involuntario. El hecho de explotar ilegítimamente el acceso logrado coincidencialmente a un sistema de información o cualquiera de sus componentes, se sancionará con la pena de dos a cinco años de prisión y multa desde doscientas a quinientas veces el salario mínimo.

Artículo 8. Explotación de acceso ilícito para servicios a terceros. El hecho de utilizar un equipo, material o dispositivo, sistema de información o cualquiera de sus componentes, para ofrecer productos o servicios que estos sistemas proveen a terceros, sin que estos sean pagados a los proveedores de servicios legítimos, se sancionará con la pena de seis meses a cuatro años de prisión y multa de cien a quinientas veces el salario mínimo del sector público.

Párrafo. Beneficio de actividades de un tercero. El hecho de aprovechar las actividades fraudulentas de un tercero descritas en este artículo, a sabiendas de su ilicitud, para recibir directa o indirectamente beneficio pecuniario o de cualquier otra índole, ya sea propio o para terceros, o para gozar de los servicios ofrecidos a través de cualquiera de estos sistemas, se sancionará con pena de seis meses a cuatro años de prisión y multa de cien a quinientas veces el salario mínimo del sector público.

Artículo 9. Dispositivos fraudulentos. El hecho de producir, usar, poseer, traficar o distribuir, sin autorización o causa legítima, programas o sistemas de información, equipos, materiales o dispositivos cuyo único uso o uso fundamental sea el de emplearse como herramienta para cometer ciberdelitos, se sancionará con la pena de dos a cinco años de prisión y multa de doscientas a quinientas veces el salario mínimo del sector público.

Artículo 10. Inscripción en registro de servicios. Toda persona física o jurídica dedicada a ofrecer la provisión, desbloqueo y reparación de equipos de telecomunicaciones, deberá estar inscrita en el registro que a tales fines llevará el Ministerio de Interior y Policía a partir de la publicación de la presente ley y enviar a este organismo reportes mensuales donde se consignen los datos de los aparatos y equipos que hayan requerido de sus servicios. El incumplimiento de esta disposición será sancionado con multa de cien a quinientos salarios mínimos del sector público.

Artículo 11. Manipulación de equipos con fines fraudulentos. Todo aquel que altere, duplique y/o borre la identidad de un sistema de información con fines fraudulentos ser sancionado con una pena de seis meses a cuatro años de prisión y multa entre cincuenta a doscientos salarios mínimos del sector público.

Artículo 12. Interceptación e intervención de datos o señales. El hecho de interceptar, intervenir, detener, espiar, escuchar, desviar, grabar u observar, en cualquier forma, un dato, una señal o una transmisión de datos o señales no públicas pertenecientes a otra persona por propia cuenta o por encargo de otro, sin autorización previa de un juez competente, desde, a través o dirigidas a un sistema de información, materializando voluntaria e intencionalmente la violación del secreto, la intimidad, la privacidad de las personas físicas, y demás derechos personales establecidos en la Constitución, se sancionará con la pena de dos a cinco años de prisión y multa de doscientas a quinientas veces el salario mínimo del sector público, sin perjuicio de las sanciones administrativas que puedan resultar de leyes y reglamentos especiales.

Artículo 13. Daño o alteración de datos. El hecho de borrar, afectar, introducir, copiar, mutilar, editar, alterar o eliminar datos y cualquiera de los componentes presentes en sistemas de información transmitidos a través de uno de éstos, de manera deliberada, se sancionará con penas de seis meses a cuatro años de prisión y multa desde doscientas a quinientas veces el salario mínimo del sector público.

Párrafo. Cuando este hecho sea realizado por un empleado, ex-empleado o una persona que preste servicios directa o indirectamente a la persona física o jurídica afectada, la pena será tres a siete años de prisión y multa desde doscientas a quinientas veces el salario mínimo del sector público.

Artículo 14. Sabotaje. El hecho de alterar, maltratar, trabar, obstruir, inutilizar, causar mal funcionamiento, dañar o destruir un sistema de información o de los programas y operaciones lógicas que lo rigen, se sancionará con las penas de dos años a cinco años de prisión y multa desde doscientas a quinientas veces el salario mínimo del sector público.

CAPÍTULO II
CIBERDELITOS CONTRA LAS PERSONAS

Artículo 15. Atentado contra la vida. Se sancionará con las mismas penas del homicidio voluntario e involuntario, el atentado contra la vida, o la provocación o instigación para causar la muerte de una persona cometido utilizando un sistema de información, o cualquiera de sus componentes.

Artículo 16. Amenaza. El hecho de advertir o anticipar la intención de inferir un daño a otro, a sus bienes o a un tercero en circunstancias que hacen parecer verosímil la materialización del hecho, utilizando un sistema de información o cualquiera de sus componentes, será sancionado con la pena de seis meses a cuatro años de prisión y multa de cien a doscientas veces el salario mínimo del sector público.

Artículo 17. Uso de sistemas para invasión de la privacidad. El uso, sin causa legítima o autorización de la entidad legalmente competente, de un sistema de información o cualquiera de sus componentes que puedan servir para realizar operaciones que atenten contra la privacidad en cualquiera de sus formas, se sancionará con la pena de seis meses a cuatro años de prisión y multa de doscientas a quinientas veces el salario mínimo del sector público.

Artículo 18. Ciberacoso. Constituye el ciberacoso el acto de apremiar, perseguir, hostigar o vigilar de forma insistente y reiterada, a una persona a través del uso de un sistema de información o cualquiera de sus componentes, alterando gravemente el desarrollo de su vida cotidiana, se sancionará con la pena de tres a meses a cinco años de prisión y multa de doscientas a quinientas veces el salario mínimo del sector público.

Artículo 19. Ciberhostigamiento. El acoso por parte de un menor de edad utilizando un sistema de información o cualquiera de sus componentes para infligir a otra persona menor de edad con un trato degradante, menoscabando gravemente su integridad, pudiendo o no instigar a otros a actuar de igual manera, será castigado con una pena de tres meses a cuatro años de prisión y multa de doscientas a quinientas veces del salario mínimo del sector público.

Artículo 20. Atentado sexual. El hecho de entregar o requerir el intercambio de imágenes o material audiovisual de contenido sexual de un niño, niña, adolescente mediante la utilización de un sistema de información o cualquiera de sus componentes, se sancionará con las penas de tres a diez años de prisión y multa doscientas a quinientas veces el salario mínimo del sector público.

Artículo 21. Engaño pederasta. La persona adulta que contacte a un niño, niña o adolescente a través de un sistema de información o cualquiera de sus componentes, con el fin de ganarse su confianza para obtener favores de índole sexual, será sancionada con la pena de tres a cinco años de prisión y multa de doscientas a quinientas veces el salario mínimo del sector público.

Artículo 22. Difusión no autorizada de imágenes o material audiovisual de contenido sexual. La revelación o difusión no autorizada a terceros de imágenes o material audiovisual de contenido sexual obtenidas con el consentimiento o no de la víctima a través de un sistema de información o cualquiera de sus componentes, se sancionará con la pena de dos a cinco años y multa de doscientas a quinientas veces el salario mínimo del sector público.

Párrafo. Cuando la acción descrita en el párrafo anterior sea cometida por una persona que tenga o haya tenido un vínculo personal o sentimental con la víctima, esta se sancionará con pena de cinco a siete años de prisión y multa de quinientas a ochocientas veces el salario mínimo del sector público.

Artículo 23. Material de explotación o abuso sexual contra niños, niñas y adolescentes. La producción, difusión, venta, puesta a disposición o cualquier tipo de comercialización; adquisición y posesión a través de un sistema de información o cualquiera de sus componentes de imágenes y representaciones de un niño, niña o adolescente, en actividades sexuales reales o simuladas o toda representación de las partes genitales de niños, niñas y adolescentes con propósitos primariamente sexuales, se sancionará de la forma siguiente:

a) Para los casos de adquisición o posesión de material de abuso sexual descrito, se aplicará la pena será de uno a cuatro años de prisión y multa de doscientas a quinientas veces el salario mínimo del sector público.

b) Para los casos de la producción, difusión, venta, puesta a disposición o cualquier tipo de comercialización de material de abuso sexual, la pena será de cuatro a siete años de prisión y multa de trescientas a quinientas veces el salario mínimo del sector público.

c) En los supuestos anteriores, cuando se trate de material de abuso sexual que incluya al menos la participación de un menor hasta los siete años de edad, la pena aplicable será de diez a quince años de prisión y multa de trescientas a quinientas veces el salario mínimo del sector público.

d) Cuando se trate de material audiovisual que contenga imágenes de violación sexual, violencia física y tortura a un menor, se aplicará la pena de diez a quince años de prisión y multa de trescientas a quinientas veces el salario mínimo del sector público.

Párrafo. Los proveedores de servicios deberán eliminar en un plazo de veinticuatro horas el material de explotación o abuso sexual contra niños, niñas y adolescentes que se les haya notificado. En caso de no cumplir con la orden de eliminar dicho contenido podrán sancionados con multas de doscientas veces el salario mínimo del sector público.

CAPÍTULO III
SUSTRACCIÓN Y CIBERDELITOS FINANCIEROS

Artículo 24. Sustracción. El que sustrae con fraude la cosa que no le pertenece por medio de la utilización de un sistema de información o cualquiera de sus componentes se sancionará con la pena de tres a veinte años de prisión y multa de cincuenta a quinientas veces el salario mínimo del sector público.

Artículo 25. Envío o recepción ilícita de fondos. Quien, con conocimiento de la acción e intención fraudulenta, producto de una operación ilícita o no autorizada, realice el envío o reciba fondos, créditos, valores o activos digitales a través de un sistema de información o cualquiera de sus componentes, será sancionado con pena de tres a diez años de prisión y multa de cien a quinientas veces el salario mínimo del sector público.

Párrafo I. No incurrirán en la comisión de este ilícito quien, desconociendo la acción e intención fraudulenta y previa a la disposición de fondos, créditos, valores o activos digitales, haya denunciado a Ministerio Público la transacción no reconocida por éste o que presuma ilegítima.

Párrafo II. Cuando el Ministerio Público haya recibido la reclamación indicada en el párrafo anterior, tendrá la obligación de informar sobre el particular a la Unidad de Análisis Financiero (UAF) para que esta última solicite a la entidad de intermediación financiera el congelamiento preventivo de estos fondos, créditos, valores o activos digitales, a fin de que no puedan ser dispuestos por el titular o cualquier otra persona, hasta la conclusión definitiva del caso objeto de denuncia.

Artículo 26. Estafa. Quien valiéndose de nombres o calidades que no posee o empleando manejos fraudulentos, a través del uso de un sistema de información, dando o no por cierta la existencia de empresas falsas, de créditos imaginarios o de poderes que no tienen, a fin de obtener capitales ajenos, haciendo o intentando hacer que se les entreguen o remitan fondos, billetes de bancos, activos digitales, muebles, datos o archivos digitales, se sancionará con la pena de cuatro a siete años de prisión y multa de cien a quinientas veces el salario mínimo del sector público.

Párrafo. La estafa realizada en perjuicio del Estado Dominicano o de sus instituciones, será sancionada con pena de cinco a diez años de prisión y multa de doscientas a quinientas veces el salario mínimo del sector público.

Artículo 27. Chantaje. El chantaje realizado a través del uso de un sistema de información o cualquiera de sus componentes, con el propósito de obtener fondos, valores, la firma o entrega de algún documento, imágenes o videos, sean digitales o no, un código de acceso o cualquier otra actuación en beneficio de la persona que comete el chantaje utilizando como medio la revelación de imágenes, videos, conversaciones, textos, voz o cualquier otro contenido se sancionará con pena de cuatro a siete años de prisión y multa de cien a quinientas veces el salario mínimo del sector público.

Artículo 28. Suplantación de identidad. El hecho de que una persona se valga a través de un sistema de información o cualquiera de sus componentes de una identidad ajena a la suya sin autorización, se sancionará con penas de tres meses a siete años de prisión y multa de doscientas a quinientas veces el salario mínimo del sector público.

Artículo 29. Falsedad de documentos y firmas. Todo aquel que falsifique, desencripte, suplante, decodifique o de cualquier modo descifre, divulgue o trafique, con documentos, firmas, certificados, sean digitales o electrónicos, será castigado con la pena de uno a cuatro años de prisión y multa de cincuenta a doscientas veces el salario mínimo del sector público.

Artículo 30. Comercio de bienes o servicios ilícitos. La comercialización no autorizada o ilícita de bienes o servicios, a través de un sistema de información o de cualquier dispositivo o mecanismo, se castigará con la pena de dos a cinco años de prisión y multa de doscientas a quinientas veces el salario mínimo del sector público.

CAPÍTULO IV
CIBERDELITOS CONTRA LA PROPIEDAD INTELECTUAL

Artículo 31. Delitos relacionados a la propiedad intelectual. Cuando las infracciones establecidas en la Ley Núm. 20-00, del 8 de mayo del año 2000, sobre Propiedad Industrial, y la Ley Núm. 65-00, del 21 de agosto del año 2000, sobre Derecho de Autor, y sus modificaciones, se cometan a través del empleo de un sistema de información, o de cualquiera de sus componentes, se sancionará con las penas establecidas en las respectivas legislaciones para estos actos ilícitos.

CAPÍTULO V
CIBERDELITOS CONTRA LAS TELECOMUNICACIONES

Artículo 32. Delitos de telecomunicaciones. Incurren en penas de tres meses a cuatro años de prisión y multa desde trescientas a quinientas veces el salario mínimo del sector público, los que cometan uno o varios de los siguientes hechos:

a) **Llamada de retorno de tipo fraudulento:** La generación de tráfico en sentido inverso al normal, con fines comerciales, mediante mecanismos y sistemas informáticos, afectando a las empresas prestadoras de servicios. Este hecho incluye, pero no se limita, a cualquier tipo de retorno de llamada a través de código, asistencia de operador, vía un sistema informático, dependiendo del mecanismo o sistema mediante el cual se transmita la señal de disparo;

b) **Fraude de proveedores de servicio de tarificación adicional:** La autogeneración de llamadas por parte del proveedor de servicio de información de líneas tipo 1-976, con el propósito de que la prestadora que le ofrece el servicio de telefonía tenga que pagarle las comisiones de estas llamadas será considerada un fraude, constituyendo un agravante, cuando los autores del delito se valgan de medios publicitarios o de cualquier otro tipo y precios reducidos, o de números telefónicos ordinarios para su redireccionamiento hacia líneas de servicio de información, u otros medios similares;

c) **Redireccionamiento de llamadas de larga distancia:** El fraude en el desvío o redirección del tráfico de larga distancia de la ruta utilizada por parte de las compañías portadoras de señal de larga distancia, para evadir el costo real de la misma, a través de conmutadores colocados en lugares distintos al de origen de la llamada;

d) **Robo de línea:** El uso de una línea existente, alámbrica o inalámbrica, de un cliente legítimo, para establecer cualquier tipo de llamadas mediante una conexión clandestina, física o de otra índole, en cualquier punto de la red;

e) **Desvío de tráfico:** El desvío de tráfico a través de rutas no autorizadas con el objeto de evitar o disminuir los pagos que corresponden a la naturaleza del tráfico desviado;

f) **Manipulación ilícita de equipos de telecomunicaciones:** El hecho de manipular ilícitamente, de cualquier forma, las centrales telefónicas u otros componentes de las redes de telecomunicaciones, con el objetivo de hacer uso de los servicios sin incurrir en los cargos correspondientes;

g) **Intervención de centrales privadas:** La utilización de medios para penetrar centrales privadas a través de los puertos de mantenimiento o especiales del contestador automático o cualquier otro medio, que conlleven la realización de llamadas no autorizadas en perjuicio del propietario de la central intervenida; y

h) **Uso ilegítimo de identificador de llamadas:** El hecho de alterar deliberadamente la información transmitida de identificación de llamadas para simular una identidad ajena.

CAPÍTULO VI
ACTOS DE CIBERTERRORISMO Y CIBERDELITOS CONTRA LA NACIÓN

Artículo 33. Ciberterrorismo. Se considerará ciberterrorismo el uso de sistemas de información o cualquiera de sus componentes para ejecutar cualquier acto con el fin de provocar en forma indiscriminada o atroz, muertes, heridas, lesiones físicas o psicológicas, en un número indeterminado de personas, o graves estragos materiales o funcionales a infraestructuras críticas y estratégicas nacionales, con la finalidad de:

a) Atemorizar a la población en general o determinados sectores de ésta obligando al gobierno nacional, a otro gobierno o a una organización internacional a realizar un acto o a abstenerse de hacerlo;

b) Ejercer retaliaciones fundadas por motivos políticos, étnicos, religiosos, o de cualquier otra índole; y

c) Afectar las relaciones del Estado dominicano con otros estados o su imagen exterior.

Párrafo I. La comisión de los actos aquí descritos será castigada con pena de veinte a treinta años de reclusión y multa de trescientos a mil salarios mínimos del sector público

Párrafo II. Se podrá ordenar la confiscación y destrucción del sistema de información o cualquiera de sus componentes utilizados para cometer el hecho.

Artículo 34. Ciberdelitos contra la Nación. Los actos que se realicen a través de un sistema de información o cualquiera de sus componentes, que atenten contra los intereses fundamentales, seguridad y defensa de la Nación, tales como el sabotaje, el espionaje o el suministro de información clasificada a personas no autorizadas, serán castigados con penas de quince a treinta años de reclusión y multa de trescientas a dos mil veces el salario mínimo.

TÍTULO III
ORGANÍSMOS COMPETENTES Y REGLAS DE DERECHO PROCESAL

CAPÍTULO I
ORGANISMOS COMPETENTES

Artículo 35. Ministerio Público. El Ministerio Público es el responsable de coordinar, a través de su dependencia especializada, la investigación y persecución de los delitos contenidos en esta ley.

Párrafo. El Ministerio Público contará con una dependencia especializada en la investigación y persecución de los ciberdelitos contenidos en la presente ley que se denominará la Procuraduría Especializada contra Ciberdelitos de la Procuraduría General de la República.

Artículo 36. Facultades del Ministerio Público. El Ministerio Público tiene a su cargo la dirección funcional de la investigación, pudiendo auxiliarse de los organismos de investigación del Estado, tales como el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología de la Policía Nacional; la División de Investigación de Delitos Informáticos del Departamento Nacional de Investigaciones; peritos; instituciones públicas o privadas. El Ministerio Público, siguiendo todas las formalidades establecidas por el Código Procesal Penal, podrá:

a) Ordenar a una persona física o jurídica la entrega de la información que se encuentre en un sistema de información o en cualquiera de sus componentes;

b) Ordenar a una persona física o jurídica la preservación de datos, mantenimiento e integridad de un sistema de información o de cualquiera de sus componentes, por un período de noventa (90) días a partir de su solicitud, renovable por períodos sucesivos;

c) Ordenar el acceso y preservación íntegra a dicho sistema de información o a cualquiera de sus componentes;

d) Ordenar a un proveedor de servicios suministrar información de los datos relativos a suscriptores, usuarios y de tráfico que pueda tener en su posesión o control;

e) Tomar en secuestro o asegurar un sistema de información o cualquiera de sus componentes, en todo o en parte;

f) Realizar y retener copia del contenido del sistema de información o de cualquiera de sus componentes;

g) Ordenar el mantenimiento de la integridad del contenido de un sistema de información o de cualquiera de sus componentes;

h) Hacer inaccesible o remover el contenido de un sistema de información o de cualquiera de sus componentes, que haya sido accedido para la investigación;

i) Ordenar a la persona que tenga conocimiento acerca del funcionamiento de un sistema de información o de cualquiera de sus componentes o de las medidas de protección de los datos en dicho sistema a proveer la información necesaria para realizar las investigaciones de lugar;

j) Recolectar o grabar los datos de un sistema de información o de cualquiera de sus componentes, a través de la aplicación de medidas tecnológicas;

k) Solicitar a un proveedor de servicios recolectar, extraer o grabar los datos relativos a un usuario, así como el tráfico de datos en tiempo real, a través de la aplicación de medidas tecnológicas;

l) Realizar la intervención o interceptación de las telecomunicaciones en tiempo real, según el procedimiento establecido en el Artículo 192 del Código Procesal Penal para la investigación de todos los hechos punibles en la presente ley; y

m) Ordenar cualquier otra medida aplicable a un sistema de información o cualquiera de sus componentes para obtener los datos necesarios y asegurar la preservación de los mismos.

Párrafo. El Ministerio Público al ejercer cualquiera de las funciones previamente indicadas en este artículo, deberá preservar el secreto de lo privado que no guarde relación con el correspondiente proceso.

Artículo 37. Comisión Interinstitucional contra el Ciberdelito. La Comisión Interinstitucional contra el Ciberdelito, la cual estará compuesta por un representante de las siguientes entidades:

a) La Procuraduría General de la República;

b) El Centro Nacional de Ciberseguridad;

c) El Ministerio de Defensa;

d) La Policía Nacional;

e) El Departamento Nacional de Investigaciones (DNI); y

f) El Instituto Dominicano de las Telecomunicaciones (INDOTEL).

Párrafo. La Comisión podrá auxiliarse de otras entidades públicas y privadas afines a las funciones desempeñadas por esta, para el reforzamiento de su gestión.

Artículo 38. Presidencia. La Comisión estará presidida por el Procurador General de la República o por un representante que se designe de la Procuraduría General de la República.

Artículo 39. Funciones. La Comisión Interinstitucional contra el Ciberdelito tendrá las funciones siguientes:

a) Coordinar y cooperar con autoridades policiales, militares, de investigación y judiciales, en sus esfuerzos comunes para mejorar y dar cabal cumplimiento a las disposiciones de la presente ley;

b) Gestionar proyectos de cooperación con gobiernos e instituciones nacionales y extranjeras para prevenir y reducir la comisión de ciberdelitos;

c) Establecer las directrices y elaborar propuestas de estrategias, normas y planes para someterlas al Poder Ejecutivo;

d) Promover la adopción de los convenios y tratados internacionales en esta materia y velar por la implantación y cumplimento de los mismos, cuando sean suscritos y ratificados por la República Dominicana;

e) Proponer la representación dominicana a través de la entidad nacional competente ante los diferentes organismos internacionales en el área de ciberdelito;

f) Garantizar mecanismos eficaces de financiamiento, sostenibilidad y buen funcionamiento de los organismos encargados de velar por la aplicación de esta ley;

g) Proponer y participar en la elaboración de protocolos interinstitucionales.

Artículo 40. Reuniones. La Comisión funcionará en pleno o por medio de comisiones delegadas. El pleno se reunirá por lo menos cuatro veces al año en reunión ordinaria o cuantas veces lo convoque su Presidente, por iniciativa propia o a propuesta de cualquiera de sus miembros.

Párrafo. Las decisiones adoptadas por la Comisión se acogerán con la votación de la mayoría simple de sus miembros.

Artículo 41. Secretaría general. La Comisión designará al representante que actuará como Secretario General de la Comisión de manera rotativa y por periodo de un (1) año, quien dentro de sus funciones convocará y fijará el orden del día de las reuniones de en coordinación con su Presidente; redactará las actas de las reuniones, llevando un registro de las mismas; y divulgará las decisiones aprobadas a los miembros de la Comisión, así como a las personas públicas y privadas que se estimen necesarias.

Artículo 42. Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT). El Departamento de Investigación de Crímenes y Delitos de Alta Tecnología es el cuerpo policial

especializado de la Policía Nacional cuyas funciones son las de prevenir, controlar, perseguir e investigar los distintos ciberdelitos tipificados en la presente ley.

Artículo 43. Funciones. El Departamento de Investigación de Crímenes y Delitos de Alta Tecnología tendrá las funciones siguientes:

a) Velar por el fiel cumplimiento y ejecución de las disposiciones de la presente ley;

b) Investigar todas las denuncias recibidas sobre ciberdelitos dentro del ámbito de su competencia;

c) Llevar a cabo las investigaciones de los ciberdelitos contra las infraestructuras críticas nacionales dentro del ámbito de su competencia;

d) Realizar las tareas de ciberpatrullaje;

e) Apoyar al Centro Nacional de Ciberseguridad en las labores de investigación que surjan como consecuencia de los incidentes de ciberseguridad;

f) Velar por el correcto entrenamiento del personal de la unidad de investigación;

g) Auxiliar en los procesos judiciales en los que sea necesario realizar investigaciones en entornos digitales afines con su competencia;

h) Ejercer la función de Punto de Contacto 24/7 de las distintas redes internacionales a las que pertenezca la República Dominicana, como son, entre otras, las de INTERPOL, G7 y el Convenio de Budapest;

i) Actuar en conjunto con las dependencias de la Procuraduría General de la República a los efectos de la implementación de estrategias eficaces para el abordaje de la ciberdelincuencia;

j) Elaborar informes y diagnósticos sobre esta clase de criminalidad; y

k) Cualquier otra que le faculte el Código procesal Penal.

Artículo 44. Investigación y sometimiento. Las investigaciones de los casos y el sometimiento a la justicia de las personas involucradas serán dirigidas por el Ministerio Público, auxiliado por el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología, la División de Investigación de Delitos Informáticos del Departamento Nacional de Investigaciones, en los casos del ámbito de su competencia, pudiendo las instituciones involucradas tener oficiales de enlace para el desempeño de sus funciones.

Artículo 45. División de Investigaciones de Delitos Informáticos. La División de Investigaciones de Delitos Informáticos es una dependencia del Departamento Nacional de Investigaciones, encargada de investigar los ciberdelitos contra la humanidad, la Nación, el Estado y la paz pública; así como las

amenazas o ataques contra el Estado dominicano, la seguridad nacional o que involucren la figura del presidente de la República, ministros o funcionarios electos.

Artículo 46. Funciones de la División de Investigaciones de Delitos Informáticos. La División de Investigación de Delitos Informáticos (DIDI) tendrá como principales funciones:

a) Velar por el fiel cumplimiento y ejecución de las disposiciones de la presente ley;

b) Investigar todas las denuncias sobre ciberdelitos dentro del ámbito de su competencia;

c) Llevar a cabo las investigaciones de los ciberdelitos contra las infraestructuras críticas nacionales dentro del ámbito de su competencia;

d) Apoyar al Centro Nacional de Ciberseguridad en las labores de investigación que surjan como consecuencia de los incidentes de ciberseguridad;

e) Desarrollar análisis estratégicos de amenazas informáticas;

f) Velar por el correcto entrenamiento del personal de la unidad de investigación.

g) Trabajar en coordinación con los demás organismos nacionales e internacionales de investigación de ciberdelitos.

Artículo 47. Sostenibilidad operativa de los organismos competentes. El presupuesto de los organismos competentes para aplicar esta ley, estará conformado por:

a) La proporción de la asignación presupuestaria que cada año deberá otorgarles su respectiva institución;

b) Las asignaciones presupuestarias que les sean asignadas por el Gobierno Central;

c) Los fondos que puedan obtener por cualquier otro concepto legítimo;

d) La proporción de las multas y decomiso de bienes producto de la ejecución presente ley, según se describe a continuación:

   1. Un cuarenta por ciento (40%) a la Procuraduría Especializada en Ciberdelitos de la Procuraduría General de la República;

   2. Un cuarenta por ciento (40%) al Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional; y

   3. Un veinte por ciento (20%) a la División de Investigación de Delitos Informáticos (DIDI) del Departamento Nacional de Investigaciones.

CAPÍTULO II
MEDIDAS PROCESALES Y DE INVESTIGACIÓN

Artículo 48. Aplicación del Código Procesal Penal. Las reglas de la comprobación inmediata y medios auxiliares previstas en el Código Procesal Penal sus modificaciones y leyes especiales, se aplicarán para la obtención y preservación de los datos contenidos en un sistema de información o cualquiera de sus componentes, datos de tráfico, conexión, acceso o cualquier otra información de utilidad, en la investigación de los delitos tipificados en la presente ley y para todos los procedimientos establecidos en este Capítulo.

Artículo 49. Sobre medidas cautelares. Excepcionalmente, en aquellos casos en que exista peligro en la demora, el Ministerio Público podrá adoptar mediante resolución motivada las medidas cautelares contempladas en el presente artículo, con la obligación de informar a la jurisdicción competente dentro del plazo de veinticuatro horas.

Párrafo. Al investigarse una infracción prevista en esta ley, el juez de la instrucción competente, a solicitud del Ministerio Publico, emitirá por cualquier medio regulado por el Poder Judicial, las autorizaciones pertinentes.

Artículo 50. Equipos conjuntos de investigación. El Ministerio Público y los organismos de investigación del Estado podrán crear de común acuerdo con las autoridades competentes de dos o más Estados equipos conjuntos de investigación, con un fin determinado y por un período limitado que podrá ampliarse con el consentimiento de todas las partes, para llevar a cabo investigaciones penales en uno o más de los Estados que hayan creado el equipo. La composición del equipo se determinará en el acuerdo de constitución del mismo.

Párrafo I. Podrán crearse equipos conjuntos de investigación, en particular, en los siguientes casos:

a) Cuando la investigación de infracciones sancionadas por esta ley en un Estado requiera investigaciones que impliquen la movilización de medios considerables y afecten también a otros Estados; y

b) Cuando varios Estados realicen investigaciones sobre infracciones sancionadas por esta ley que, debido a las circunstancias del caso, requieran una actuación coordinada y concertada de los Estados afectados.

Párrafo II. Cuando el equipo conjunto de investigación necesite que se tomen medidas de investigación en uno de los Estados que hayan creado el equipo, los miembros destinados al mismo por ese Estado podrán pedir a sus propias autoridades competentes que tomen tales medidas. Estas medidas se examinarán en el Estado de que se trate en las mismas condiciones que si fueran solicitadas en el marco de una investigación nacional.

Párrafo III. Cuando el equipo conjunto de investigación necesite ayuda de un Estado afectado que no haya participado en la creación del equipo o de un tercer Estado, las autoridades competentes del Estado en el que actúe el equipo podrán formular la petición de ayuda a las autoridades competentes del otro Estado afectado, de conformidad con los instrumentos o disposiciones aplicables.

Párrafo IV. Para los fines de la investigación que esté realizando el equipo conjunto de investigación, cualquier miembro de éste podrá, de conformidad con su derecho interno de su país y dentro de los límites de las competencias que tenga atribuidas, compartir con el equipo información de la que disponga el Estado que le haya destinado al mismo.

Párrafo V. La información que obtenga legalmente un miembro de un equipo conjunto de investigación o un miembro destinado al mismo mientras forme parte de un equipo conjunto de investigación y a la que no tengan acceso de otro modo las autoridades competentes de los Estados miembros afectados podrán utilizarse para los siguientes fines:

a) Para los fines para los que se haya creado el equipo;

b) Condicionada a la autorización previa del Estado en que se haya obtenido la información, para descubrir, investigar y enjuiciar otras infracciones penales. Dicha autorización podrá denegarse únicamente en los casos en que esta utilización ponga en peligro las investigaciones penales en el Estado de que se trate o en que dicho Estado pueda denegar la asistencia judicial;

c) Para evitar una amenaza inmediata y grave para la seguridad pública, y sin perjuicio de lo dispuesto en la letra b) si ulteriormente se iniciara una investigación penal; y

d) Para otros fines, siempre y cuando hayan convenido en ello los Estados que crearon el equipo.

Artículo 51. Investigadores bajo reserva de identidad. Durante el curso de una investigación, el Ministerio Público puede solicitar a la autoridad judicial competente que autorice la reserva de identidad de uno o varios investigadores que puedan crear y hacer uso de uno o varios perfiles en uno o varios sistemas de información, que operen en redes públicas o privadas, cuando ello sea manifiestamente útil para el desarrollo de la investigación. A tales fines, la autoridad judicial competente fijará un plazo para la reserva de identidad y el desarrollo de tales operaciones, pudiendo ser prorrogado, sin que en ningún caso este plazo supere los dieciocho meses, y una vez vencido este plazo, el Ministerio Público deberá presentar a dicha autoridad un informe con el resultado de la investigación, revelando la identidad de los investigadores actuantes.

Párrafo I. Al término de esta actuación, los investigadores deberán emitir un informe con los resultados de la investigación, el cual puede ser incorporado al juicio por su lectura y exhibición, independientemente de que los investigadores puedan ser citados como testigo al juicio.

Párrafo II. Los investigadores autorizados podrán, bajo la dirección funcional del Ministerio Público y previa autorización judicial, participar en entregas vigiladas. A tal efecto, podrá recibir y/o entregar documentos, mensajes, archivos, softwares, imágenes, bienes, valores y cualquier elemento, físico o digital, que guarde relación con la investigación.

Artículo 52. Registros remotos. El Ministerio Público, previa autorización de la autoridad judicial competente, podrá acceder registrar y ocupar documentos, mensajes, archivos, imágenes y cualesquiera datos que sean manifiestamente útil y necesarios para la investigación y que se encuentren almacenados en cualquier sistema de información al cual se pueda acceder de manera remota haciendo conexión a

través del internet o de redes públicas o privadas de comunicación, así como con la instalación de programas que permitan de forma remota el examen a distancia y sin conocimiento de su titular o usuario del contenido de un sistema de información que persiga la investigación de alguno de los siguientes delitos:

a) Delitos cometidos por parte de grupos criminales organizados;

b) Delitos de terrorismo;

c) Delitos cometidos contra niños, niñas y adolescentes o personas en condiciones de vulnerabilidad; y

d) Delitos de traición y relativos a la defensa nacional;

Párrafo I. La orden judicial que autorice el registro remoto deberá especificar:

a) El alcance de la orden, la forma en que se procederá al acceso y registro y la ocupación o secuestro de los datos o archivos que sean útiles, relevantes y pertinentes para la investigación, así como el programa que se utilizará para lograr el acceso, registro, ocupación y secuestro de la información.

b) Los agentes autorizados para la ejecución de la medida.

c) El motivo preciso del registro, con indicación de los documentos, mensajes, archivos, imágenes y datos que se esperan encontrar.

d) La fecha y hora de expedición de la orden, con indicación del juez que la emite.

e) El plazo para la ejecución de la diligencia, que no puede superar de treinta (30) días, renovables por una única vez por treinta (30) días adicionales.

Párrafo II. Los investigadores autorizados para la ejecución de esta diligencia investigativa no pueden suprimir, alterar o modificar los datos almacenados en el sistema de información al cual se ha tenido acceso.

Artículo 53. Uso de información de fuentes abiertas o accesibles al público. Se permite el uso de datos e información obtenidos de fuentes abiertas sin la necesidad de una autorización judicial. En tal virtud, los investigadores podrán realizar búsquedas, captación y recolección de documentos, mensajes, archivos, imágenes, videos, programas y cualquier otro dato que se encuentre disponible en fuentes abiertas.

Artículo 54. Videoconferencia. Ante la imposibilidad de la presencia fisica de un testigo o perito en el tribunal, el juez podrá permitir que se tomen sus testimonios o declaraciones a través del mecanismo de videoconferencia

Párrafo. Cuando en el transcurso de la videoconferencia el testigo o perito cometa perjurio, se niegue a testificar o cometa otra falta tipifcada en el Codigo Procesal Penal, las mismas seran sancionables de igual manera que si se hubiesen cometido fisicamente en el tribunal.

TÍTULO IV
DE LA COOPERACIÓN INTERNACIONAL, RECOPILACIÓN Y CONTROL DE EVIDENCIAS, EL DECOMISO DE BIENES Y LA SOSTENIBILIDAD DEL SISTEMA

CAPÍTULO I
COOPERACIÓN INTERNACIONAL

Artículo 55. Alcance de las actuaciones de cooperación internacional. El Ministerio Público tiene la potestad para solicitar o realizar pesquisas u obtener información a nombre propio o de sus contrapartes extranjeras y formar equipos conjuntos de investigación, para facilitar la identificación de los sujetos activos del delito, la obtención de datos (o informaciones) y recabar elementos de prueba de utilidad y pertinencia para la investigación, pudiendo en este caso suscribir acuerdos bilaterales o multilaterales para posibilitar estas medidas investigativas de alcance transnacional.

Artículo 56. Medidas de identificación, localización e incautación de bienes. El Ministerio Público podrá realizar o responder con las medidas apropiadas, las solicitudes de asistencia mutua internacional, para identificar, localizar, detectar, incautar los bienes, productos o instrumentos relacionados con los delitos previstos en esta ley, de los sujetos activos y sus cómplices, incluyendo dentro de dichas medidas la distribución, repatriación y recuperación de activos de origen ilícito.

Párrafo II. Cuando entre el Estado requirente y el Estado requerido no se encuentre vigente un tratado de asistencia mutua o un acuerdo basado en legislación uniforme o recíproca, cada Parte designará una o varias autoridades centrales encargadas de enviar solicitudes de asistencia mutua y de dar respuesta a las mismas, de su ejecución o de su remisión a las autoridades competentes para su ejecución y posterior respuesta.

Artículo 57. Intercambio de información. El Ministerio Público tiene la potestad para intercambiar la información disponible en el ámbito nacional con contrapartes extranjeras y viceversa, para cumplir con los propósitos de investigación penal relativos al ciberdelito y la obtención de evidencia digital, incluyendo la identificación y el rastreo de los bienes que son producto o instrumento del delito, y el beneficiario final de las personas jurídicas o de las transacciones, según lo definido en esta ley.

Artículo 58. Solicitud de información sobre el registro de nombres de dominio. La autoridad que investigue, bajo la supervisión del Ministerio Público, podrá emitir una solicitud a una entidad que preste servicios de registro de nombres de dominio en Estados con los que la República Dominicana tenga convenios de cooperación para obtener la información que esté en posesión o bajo el control de la entidad, con el fin de identificar al titular de un nombre de dominio.

Párrafo I. De igual forma, se permitirá a las entidades que prestan servicios de registro de nombres de dominio en el territorio nacional a divulgar la información en su posesión o control sobre los titulares de nombres de dominio en respuesta a solicitudes de las autoridades competentes de los Estados con los

que la República Dominicana tenga convenios de cooperación, sujeto a las condiciones razonables previstas en nuestra legislación nacional.

Párrafo II. El reglamento de aplicación de la presente ley establecerá la información que deberán incluir las solicitudes.

Artículo 59. Divulgación de la información de los abonados. La autoridad competente podrá ordenar directamente a un proveedor de servicios en el territorio de Estados con los que la República Dominicana tenga convenios de cooperación, la divulgación de información especificada y almacenada del abonado que esté en posesión o bajo el control de dicho proveedor de servicios.

Párrafo I. De igual forma, se permitirá los proveedores de servicio en el territorio nacional divulgar la información de abonados en su posesión o control en respuesta a solicitudes de las autoridades competentes de Estados con los que la República Dominicana tenga convenios de cooperación, sujeto a las condiciones razonables previstas en nuestra legislación nacional.

Párrafo II. El reglamento de aplicación de la presente ley establecerá la información que deberán incluir las solicitudes.

Artículo 60. Dar efecto a las órdenes de otra Parte para la producción acelerada de información sobre los abonados y datos de tráfico. La autoridad competente podrá emitir una orden que se presentará como parte de una solicitud a la autoridad central de un Estado con el que la República Dominicana tenga convenios de cooperación con el fin de obligar a un proveedor de servicios en el territorio de dicho Estado a presentar información específica y almacenada sobre los abonados y datos de tráfico en posesión o control de dicho proveedor de servicios.

Párrafo I. De igual forma, la autoridad competente dará efecto a las órdenes de las autoridades competentes de Estados con los que la República Dominicana tenga convenios de cooperación.

Párrafo II. El reglamento de aplicación de la presente ley establecerá la información que deberán incluir las órdenes, así como la información de apoyo, proporcionada con el fin de ayudar a la Parte requerida a dar efecto a la orden y que no se divulgará al proveedor de servicios sin el consentimiento de la Parte requirente.

Artículo 61. Divulgación acelerada de datos informáticos almacenados en caso de emergencia. En caso de emergencia, el punto de contacto para las redes 24/7 podrá transmitir una solicitud a un punto de contacto de un Estado con el que la Repùblica Dominicana tenga convenios de cooperación, una solicitud de éste en la que se pida asistencia inmediata para obtener de un proveedor de servicios la divulgación acelerada de determinados datos informáticos almacenados que estén en posesión o control de dicho proveedor de servicios, sin necesidad de una solicitud de asistencia mutua.

Párrafo I. De igual forma se permitirá a un proveedor de servicios en el territorio nacional la divulgación acelerada de determinados datos informáticos almacenados que estén en posesión o control

de dicho proveedor de servicios, a solicitud de un Estado con el que la Repùblica Dominicana tenga convenios de cooperación a través de su punto de contacto 24/7.

Párrafo II. El reglamento de aplicación de la presente ley establecerá la información que deberán incluir las solicitudes.

Artículo 62. Asistencia mutua en caso de emergencia. Cuando se considere que existe una emergencia, la autoridad competente podrá solicitar y brindar asistencia mutua de forma rápida y expedita a un Estado con el que la República Dominicana tenga convenios de cooperación. Una solicitud en virtud del presente artículo deberá incluir, además de los demás elementos necesarios, una descripción de los hechos que demuestran que existe una emergencia y la forma en que la asistencia solicitada se relaciona con ella.

Párrafo I. Ante una solicitud de asistencia de un Estado con el que la República Dominicana tenga convenios de cooperación, la autoridad competente podrá solicitar, de forma rápida y expedita, información complementaria para evaluar la solicitud, debiendo responder dicha solicitud de forma rápida y expedita una vez que esté convencida de que existe una emergencia y de que se han cumplido los demás requisitos de asistencia mutua.

Párrafo II. De igual forma facilitará dicha información complementaria de forma rápida y expedita cuando le sea solicitada por un Estado con el que la República Dominicana tenga convenios de cooperación.

Párrafo III. Las autoridades responsables de responder a las solicitudes de asistencia mutua tendrán personal disponible las veinticuatro horas del día y los siete días de la semana para responder a una solicitud de conformidad con el presente artículo.

Párrafo IV. Los resultados de la ejecución de una solicitud en virtud del presente artículo, o una copia anticipada de los mismos, de común acuerdo con autoridades responsables de la asistencia mutua de la parte requirente, podrán facilitarse por una vía distinta de la utilizada para la solicitud.

Artículo 63. Formato de las solicitudes. Todas las solicitudes de cooperación internacional previstas en la presente ley serán aceptables en formato electrónico, siempre que las mismas contengan medidas adecuadas de seguridad y de autentificación.

CAPÍTULO II
RECOPILACIÓN Y CONTROL DE EVIDENCIAS

Artículo 64. Mejores prácticas de recopilación de evidencias. El Ministerio Público, el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología de la Policía Nacional, la División de Investigación de Delitos Informáticos del Departamento Nacional de Investigaciones, y demás instituciones auxiliares, deberán procurar el uso de mejores prácticas y métodos eficientes durante los procesos de investigación para la obtención, recuperación, conservación y presentación de las evidencias.

Párrafo. El Reglamento de aplicación de esta ley contendrá las especificaciones relativas a la cadena de custodia y control de evidencias del proceso de investigación.

Artículo 65. Proveedores de servicios. Sin perjuicio de lo establecido en el literal [b)] del Artículo [39] de la presente ley, los proveedores de servicio deberán conservar los datos de tráfico, conexión, acceso o cualquier otra información que pueda ser de utilidad a la investigación, por un período mínimo un (1) año.

Párrafo. El Instituto Dominicano de las Telecomunicaciones (INDOTEL) creará un reglamento para el procedimiento de obtención y preservación de datos e informaciones por parte de los proveedores de servicios, en un plazo de seis meses a partir de la promulgación de la presente ley. Dicha normativa deberá tomar en cuenta la importancia de preservación de la prueba, no obstante, la cantidad de proveedores envueltos en la transmisión o comunicación.

Artículo 66. Desnaturalización del proceso investigativo. La desnaturalización de los actos de investigación por parte de las autoridades competentes será castigada con la destitución inmediata del cargo, prisión de seis meses a cinco años y multa de no menos de cien salarios mínimos. Dentro de los actos de desnaturalización, se considerarán, entre otros:

a) El inicio o solicitud de medidas por cualquier otra razón que no sea la persecución real de uno de los delitos establecidos por en esta ley;

b) El tráfico y comercialización de los datos obtenidos durante la investigación;

c) La divulgación de datos personales o comerciales del procesado distintos a la naturaleza de la investigación, así como el tráfico o comercialización de los mismos;

d) La contaminación o alteración deliberada de las evidencias recopiladas; y,

e) El uso desviado o desproporcionado de las facultades de investigación para fines pecuniarios o con la intención de causar un daño cierto.

Artículo 67. Confidencialidad del proceso investigativo. Quien colabore con el proceso de investigación, sea o no parte del mismo, en la provisión, recolección, interceptación, intervención o preservación de datos sobre un sistema de información o cualquiera de sus componentes, u otra acción, incluyendo a los proveedores de servicios, mantendrá confidencial el hecho de la ejecución de los actos realizados por parte de la autoridad competente. La violación a esta disposición será castigada con la pena de seis meses a cinco años de prisión y multa de no menos de cien salarios mínimos del sector público.

Artículo 68. Decomiso de bienes. Los bienes, productos, activos o instrumentos decomisados que provengan de las infracciones a esta ley, serán destinados para los planes y programas tendentes a la prevención, investigación y persecución de la ciberdelincuencia por parte de los organismos competentes de aplicar la presente ley. Dichos bienes serán distribuidos de la manera siguiente:

a) Un cincuenta por ciento (50%) a la Procuraduría Especializada contra el Delito Cibernético de la Procuraduría de General de la República; y,

b) Un cincuenta por ciento (50%) a la Dirección de Policía Cibernética de la Policía Nacional.

TÍTULO V
DISPOSICIONES FINALES

Artículo 69. Responsabilidad civil y penal de las personas jurídicas. Además de las sanciones que se indican más adelante, las personas jurídicas son solidariamente responsables de las infracciones cometidas por sus órganos o representantes. La responsabilidad penal por los hechos e infracciones contenidas en esta ley se extiende a quienes ordenen o dispongan de su realización y a los representantes legales de las personas jurídicas que conociendo de la ilicitud del hecho y teniendo la potestad para impedirlo, lo permitan, tomen parte en él, lo faciliten o lo encubran. La responsabilidad penal de las personas jurídicas no excluye la de cualquiera persona física, autor o cómplice de los mismos hechos. Cuando las personas jurídicas sean utilizadas como medios o cubierta para la comisión de un delito, o se incurra a través de ellas en una omisión punible o negligencia, estas se sancionarán con una, varias o todas de las penas siguientes:

a) Una multa igual o hasta el doble de la contemplada para la persona física para el hecho ilícito contemplado en la presente ley;

b) La disolución, cuando se compruebe que la persona jurídica sea constituida o creada o sirva como medio para la comisión de ciberdelitos;

c) La prohibición, por un período no mayor de cinco años, de ejercer directa o indirectamente una o varias actividades profesionales o sociales que realizaba en ocasión del hecho delictivo;

d) La sujeción a la vigilancia judicial por un período no mayor de cinco años;

e) La clausura por un período no mayor de cinco años, de uno o varios de los establecimientos de la empresa, que han servido para cometer los hechos incriminados;

f) La exclusión de participar en los concursos públicos, por un período no mayor de cinco años;

g) La prohibición por un período no mayor de cinco años, de participar en actividades destinadas a la captación de valores provenientes del ahorro público;

h) La confiscación de la cosa que ha servido o estaba destinada a cometer la infracción, o de la cosa que es su producto; o

i) La difusión de la sentencia pronunciada en su contra a través de los medios de comunicación.

Artículo 70. Acciones administrativas. Lo establecido en esta ley, no impide ejercer las acciones administrativas que puedan resultar de leyes y reglamentos especiales aplicables.

Artículo 71. Pago de indemnizaciones. Sin perjuicio de las sanciones penales y administrativas que puedan resultar de leyes y reglamentos especiales, las personas físicas o jurídicas podrán ser condenadas al pago de indemnizaciones civiles a favor del sujeto pasivo o cualquier víctima del ciberdelito de que se trate.

Artículo 72. Circunstancias agravantes. Se consideran circunstancias agravantes para el sujeto activo sometido a la acción de la justicia por la comisión de los ciberdelitos contenidos en esta ley las siguientes:

a) La participación de grupos criminales organizados;

b) El hecho de haber cometido el delito en asociación de dos o más personas;

c) Cuando el agente autor del delito hubiese ingresado al territorio nacional con artificios o engaños o sin autorización legal, sin perjuicio del conjunto de delitos que puedan presentarse;

d) Cuando el que comete el delito ostenta un cargo público o fuese funcionario o servidor público;

Párrafo. Los agravantes contenidos en el presente artículo se sancionarán con la pena de dos a cinco años de prisión y multa de cincuenta a doscientas veces el salario mínimo del sector público.

Artículo 73. Acción pública. Las infracciones previstas en esta ley se consideran de acción pública, con las excepciones establecidas en su contenido.

Artículo 74. Tribunal competente. Los casos de ciberdelitos serán conocidos por la jurisdicción ordinaria o por el Tribunal de Niños, Niñas y Adolescentes, dependiendo del caso.

Artículo 75. Reglamento de aplicación. Para la aplicación de las disposiciones de esta ley se elaborará una propuesta de Reglamento de Aplicación, cuya elaboración estará a cargo de la Comisión Interinstitucional contra el Ciberdelito, auxiliado por las entidades involucradas en su ámbito de aplicación. Dicha propuesta será sometida al Poder Ejecutivo para su aprobación en un plazo de seis meses.

Artículo 76. Derogaciones. Con la promulgación de esta ley, queda derogada cualquier norma o disposición que le sea contraria a la misma en esta materia.

Párrafo. Con la promulgación de esta ley queda derogada la Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología, sustituyéndola en todas sus partes.

Artículo 77. Entrada en vigencia. Esta ley entrará en vigencia desde la fecha de su publicación.

DADA EN...