Proyecto sobre cibercriminalidad
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Versión 30 Mayo 2007
[Reformat in March 2011]

Legislación sobre cibercriminalidad

REPÚBLICA DOMINICANA

Este perfil se ha preparado en el marco de la capacidad del Consejo de Europa sobre el delito cibernético de compartir información y evaluar el estado actual de la aplicación de la Convención sobre el delito cibernético en virtud de la legislación nacional de proyectos de construcción. No refleja necesariamente posiciones oficiales del país cubierto o del Consejo de Europa.

Comentarios deberán ser mandados a:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe, Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

País	**República Dominicana**
Firma de la Convención:	No
Ratificación:	No
Disposiciones de la Convención	**Disposiciones correspondientes o soluciones en la legislación nacional** Ley No. 53-07, del 23 de abril de 2007, contra Crímenes y Delitos de Alta Tecnología.
Capitulo I Terminología	
Artículo 1 – Definiciones A los efectos del presente Convenio: a.por "sistema informático" se entenderá todo dispositivo aislado o conjunto	**Artículo 4.- Definiciones.** Para los fines de esta ley, se entenderá por: **Acceso Ilícito:** El hecho de ingresar o la intención de ingresar sin autorización, o a través del acceso de un tercero, a un sistema de información, permaneciendo o

de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa; b. por "datos informáticos" se entenderá 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 informático ejecute una función; c. por "proveedor de servicios" se entenderá: i. toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y ii. cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo; d. por "datos relativos al tráfico" se entenderá todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.	no en él. **Afectar:** Alterar, provocar anomalías en cualquiera de las operaciones a realizar por un programa, software, sistema, red de trabajo, o a la computadora misma, impidiendo su uso normal por parte del usuario. **Clonación:** Duplicación o reproducción exacta de una serie electrónica, un número o sistema de identificación de un dispositivo o un medio de acceso a un servicio. **Código de Acceso:** Información o contraseña que autentica a un usuario autorizado en un sistema de información, que le permite el acceso privado y protegido a dicho sistema. **Código de Identificación:** Información, clave o mecanismo similar, que identifica a un usuario autorizado en un sistema de información. **Código Malicioso:** Todo programa, documento, mensaje, instrucciones y/o secuencia de cualquiera de éstos, en un lenguaje de programación cualquiera, que es activado induciendo al usuario quien ejecuta el programa de forma involuntaria y que es susceptible de causar algún tipo de perjuicio por medio de las instrucciones con las que fue programado, sin el permiso ni el conocimiento del usuario. **Computadora:** Cualquier dispositivo electrónico, independientemente de su forma, tamaño, capacidad, tecnología, capaz de procesar datos y/o señales, que realiza funciones lógicas, aritméticas y de memoria por medio de la manipulación de impulsos electrónicos, ópticos, magnéticos, electroquímicos o de cualquier otra índole, incluyendo todas las facilidades de entrada, salida, procesamiento, almacenaje, programas, comunicación o cualesquiera otras facilidades que estén conectadas, relacionadas o integradas a la misma. **Criptografía:** Rama de las matemáticas aplicadas y la ciencia informática que se ocupa de la transformación de documentos digitales o mensajes de datos, desde su presentación original a una representación ininteligible e indescifrable que protege su confidencialidad y evita la recuperación de la información, documento o

	mensaje original, por parte de personas no autorizadas. **Datos:** Es toda información que se transmite, guarda, graba, procesa, copia o almacena en un sistema de información de cualquiera naturaleza o en cualquiera de sus componentes, como son aquellos cuyo fin es la transmisión, emisión, almacenamiento, procesamiento y recepción de señales electromagnéticas, signos, señales, escritos, imágenes fijas o en movimiento, video, voz, sonidos, datos por medio óptico, celular, radioeléctrico, sistemas electromagnéticos o cualquier otro medio útil a tales fines. **Datos Relativos a los Usuarios:** Se entenderá toda información en forma de datos informáticos o de cualquiera 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: a) El tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el período de servicio; b) 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; c) 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. **Delito de Alta Tecnología:** Aquellas conductas atentatorias a los bienes jurídicos protegidos por la Constitución, las leyes, decretos, reglamentos y resoluciones relacionadas con los sistemas de información. Se entenderán comprendidos dentro de esta definición los delitos electrónicos, informáticos, telemáticos, cibernéticos y de telecomunicaciones. **Desvío de Facilidades Contratadas:** Se produce cuando se contratan facilidades de transmisión de tráfico de gran capacidad para uso privado y posteriormente, se les emplea con fines comerciales sin la autorización de la prestadora de servicios.

	Desvío de Servicios: Se produce cada vez que se conectan irregularmente las facilidades internacionales a la red pública conmutada para terminar tráfico. **Dispositivo:** Objeto, artículo, pieza, código, utilizado para cometer delitos de alta tecnología. **Dispositivo de Acceso:** Es toda tarjeta, placa, código, número, 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. **Documento Digital:** Es la información codificada en forma digital sobre 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. **Interceptación:** Apoderar, utilizar, afectar, detener, desviar, editar o mutilar, de cualquier forma un dato o una transmisión de datos perteneciente a otra persona física o moral, 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. **Internet:** Es un sistema de redes de computación ligadas entre sí por un protocolo común especial de comunicación de alcance mundial, que facilita servicios de comunicación de datos como contenido Web, registro remoto, transferencia de archivos, correo electrónico, grupos de noticias y comercio electrónico, entre otros. **Pornografía Infantil:** Toda representación, por cualquier medio, de niños, niñas y adolescentes, dedicados a actividades sexuales explícitas, reales o simuladas o toda representación de las partes genitales de niños, niñas y adolescentes con fines primordialmente sexuales. Se considera niño o niña, a toda persona desde su nacimiento hasta los doce años, inclusive, y adolescente, a toda persona desde los trece años hasta alcanzar la mayoría de edad. **Red Informática:** Interconexión entre dos o más sistemas informáticos o entre sistemas informáticos y terminales remotas, incluyendo la comunicación por microondas medios ópticos, electrónicos o cualquier otro medio de comunicación, que permite el intercambio de archivos, transacciones y datos, con el fin de

	atender las necesidades de información y procesamiento de datos de una comunidad, organización o un particular. **Salario Mínimo:** Para los fines de la presente ley, se entenderá como el salario mínimo nacional más bajo percibido por los trabajadores del sector privado no sectorizado de empresas industriales, comerciales y de servicios, fijado por el Comité Nacional de Salarios de la Secretaría de Estado de Trabajo de la República Dominicana. **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. **Sin Autorización:** Sin facultad o autoridad legal, estatutaria, reglamentaria o de cualquier otra índole para poseer, usar o hacer algo, sin tener poder legítimo. Esto incluye la falta o carencia total de autorización, expresa o tácita, y la transgresión del límite de la autorización que se posee. **Sistema de Información:** Dispositivo o conjunto de dispositivos que utilizan las tecnologías de información y comunicación, así como cualquier sistema de alta tecnología, incluyendo, pero no limitado a los sistemas electrónicos, informáticos, de telecomunicaciones y telemáticos, que separada o conjuntamente sirvan para generar, enviar, recibir, archivar o procesar información, documentos digitales, mensajes de datos, entre otros. **Sistema Electrónico:** Dispositivo o conjunto de dispositivos que utilizan los electrones en diversos medios bajo la acción de campos eléctricos y magnéticos, como semiconductores o transistores. **Sistema Informático:** Dispositivo o conjunto de dispositivos relacionados, conectados o no, que incluyen computadoras u otros componentes como mecanismos de entrada, salida, transferencia y almacenaje, además de circuitos de comunicación de datos y sistemas operativos, programas y datos, para el procesamiento y transmisión automatizada de datos. **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. **Sistema Telemático:** Sistema que combina los sistemas de telecomunicaciones e informáticos como método para transmitir la información. **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 la presente 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 hechos. **Sujeto Pasivo:** Es todo aquel que se sienta afectado o amenazado en cualquiera de sus derechos por la violación de las disposiciones de la presente ley. **Transferencia Electrónica de Fondos (T.E.F):** Es toda transferencia de fondos iniciada a través de un dispositivo electrónico, informático o de otra naturaleza que ordena, instruye o autoriza a un depositario o institución financiera a transferir cierta suma a una cuenta determinada. **Usuario:** Persona física o jurídica que adquiere de manera, legítima bienes o servicios de otra.
Capítulo II – Medidas que deberán adoptarse a nivel nacional **Sección 1 – Derecho penal sustantivo**	
Título 1 – Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos	
Artículo 2 – Acceso ilícito Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con	**Artículo 6.- Acceso Ilícito.** El hecho de acceder a un sistema electrónico, informático, telemático o de telecomunicaciones, o a sus componentes, utilizando o no una identidad ajena, o excediendo una autorización, se sancionará con las penas de tres meses a un año de prisión y multa desde una vez a doscientas veces el salario mínimo. **Párrafo I.- Uso de Datos por Acceso Ilícito.** Cuando de dicho acceso ilícito

la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.	resulte la supresión o la modificación de datos contenidos en el sistema, o indebidamente se revelen o difundan datos confidenciales contenidos en el sistema accesado, las penas se elevarán desde un año a tres años de prisión y multa desde dos hasta cuatrocientas veces el salario mínimo. **Párrafo II.- Explotación Ilegítima de Acceso Inintencional.** El hecho de explotar ilegítimamente el acceso logrado coincidencialmente a un sistema electrónico, informático, telemático o de telecomunicaciones, se sancionará con la pena de un año a tres años de prisión y multa desde dos a cuatrocientas veces el salario mínimo.
Artículo 3 – Interceptación ilícita Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos. Las Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.	**Artículo 9.- Interceptación e Intervención de Datos o Señales.** El hecho de interceptar, intervenir, injerir, detener, espiar, escuchar, desviar, grabar u observar, en cualquier forma, un dato, una señal o una transmisión de datos o señales, perteneciente 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 electrónico, informático, telemático o de telecomunicaciones, o de las emisiones originadas por éstos, materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas físicas o morales, se sancionará con la pena de uno a tres años de prisión y multa de veinte a cien veces el salario mínimo, sin perjuicio de las sanciones administrativas que puedan resultar de leyes y reglamentos especiales.
Artículo 4 – Ataques a la integridad de los datos 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos. 2. Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.	**Artículo 10.- Daño o Alteración de Datos.** El hecho de borrar, afectar, introducir, copiar, mutilar, editar, alterar o eliminar datos y componentes presentes en sistemas electrónicos, informáticos, telemáticos, o de telecomunicaciones, o transmitidos a través de uno de éstos, con fines fraudulentos, se sancionará con penas de tres meses a un año de prisión y multa desde tres hasta quinientas veces el salario mínimo. **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, las penas se elevarán desde uno a tres años de prisión y multa desde seis hasta quinientas veces el salario mínimo.
Artículo 5 – Ataques a la integridad del sistema Cada Parte adoptará las medidas legislativas y de otro tipo que resulten	**Artículo 11.- Sabotaje.** El hecho de alterar, maltratar, trabar, inutilizar, causar mal funcionamiento, dañar o destruir un sistema electrónico, informático, telemático o de telecomunicaciones, o de los programas y operaciones lógicas que

necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.	lo rigen, se sancionará con las penas de tres meses a dos años de prisión y multa desde tres hasta quinientas veces el salario mínimo.
Artículo 6 – Abuso de los dispositivos 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos: a. la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: i. cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los artículos 2 a 5 del presente Convenio; ii. una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer cualquiera de los delitos contemplados en los artículos 2 a 5; y b. la posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a) del presente artículo con intención de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Las Partes podrán exigir en su derecho interno la posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal. 2. No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión o cualquier otra forma de puesta a disposición mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos previstos de conformidad con los artículos 2 a 5 del presente Convenio, como en el caso de las pruebas autorizadas o de la protección de un sistema informático. 3. Las Partes podrán reservarse el derecho a no aplicar el párrafo 1 del presente artículo, siempre que dicha reserva no afecte a la venta,	**Artículo 8.- Dispositivos Fraudulentos.** El hecho de producir usar, poseer, traficar o distribuir, sin autoridad o causa legítima, programas informáticos, equipos, materiales o dispositivos cuyo único uso o uso fundamental sea el de emplearse como herramienta para cometer crímenes y delitos de alta tecnología, se sancionará con la pena de uno a tres años de prisión y multa de veinte a cien veces el salario mínimo

distribución o cualesquiera otras formas	
Título 2 – Delitos informáticos	
Artículo 7 – Falsificación informática Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las Partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal.	**Artículo 18.- De la Falsedad de Documentos y Firmas.** Todo aquel que falsifique, desencripte, decodifique o de cualquier modo descifre, divulgue o trafique, con
Artículo 8 – Fraude informático Las Partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: a. la introducción, alteración, borrado o supresión de datos informáticos; b. cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.	**Artículo 13.- Robo Mediante la Utilización de Alta Tecnología.** El robo, cuando se comete por medio de la utilización de sistemas o dispositivos electrónicos, informáticos, telemáticos o de telecomunicaciones, para inhabilitar o inhibir los mecanismos de alarma o guarda, u otros semejantes; o cuando para tener acceso a casas, locales o muebles, se utilizan los mismos medios o medios distintos de los destinados por su propietario para tales fines; o por el uso de tarjetas, magnéticas o perforadas, o de mandos, o instrumentos para apertura a distancia o cualquier otro mecanismo o herramienta que utilice alta tecnología, se sancionará con la pena de dos a cinco años de prisión y multa de veinte a quinientas veces el salario mínimo. **Artículo 14.- Obtención Ilícita de Fondos.** El hecho de obtener fondos, créditos o valores a través del constreñimiento del usuario legítimo de un servicio financiero informático, electrónico, telemático o de telecomunicaciones, se sancionará con la pena de tres a diez años de prisión y multa de cien a quinientas veces el salario mínimo. **Párrafo.- Transferencias Electrónica de Fondos.** La realización de transferencias electrónicas de fondos a través de la utilización ilícita de códigos de acceso o de cualquier otro mecanismo similar, se castigará con la pena de uno a cinco años de prisión y multa de dos a doscientas veces el salario mínimo. **Artículo 15.- Estafa.** La estafa realizada a través del empleo de medios electrónicos, informáticos, telemáticos o de telecomunicaciones, se sancionará con

	la pena de tres meses a siete años de prisión y multa de diez a quinientas veces el salario mínimo. **Artículo 16.- Chantaje.** El chantaje realizado a través del uso de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones, o de sus componentes, y/o con el propósito de obtener fondos, valores, la firma, entrega de algún documento, sean digitales o no, o de un código de acceso o algún otro componente de los sistemas de información, se sancionará con la pena de uno a cinco años de prisión y multa de diez a doscientas veces el salario mínimo.
Título 3 – Delitos relacionados con el contenido	
Artículo 9 – Delitos relacionados con la pornografía infantil 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos: a. la producción de pornografía infantil con la intención de difundirla a través de un sistema informático; b. la oferta o la puesta a disposición de pornografía infantil a través de un sistema informático; c. la difusión o la transmisión de pornografía infantil a través de un sistema informático; d. la adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático; e. la posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos. 2. A los efectos del párrafo 1 anterior, se entenderá por «pornografía infantil» todo material pornográfico que contenga la representación visual de: a. un menor adoptando un comportamiento sexualmente explícito; b. una persona que parezca un menor adoptando un comportamiento sexualmente explícito; c. imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito. 3. A los efectos del párrafo 2 anterior, se entenderá por «menor» toda persona menor de 18 años. Las Partes podrán, no obstante, exigir un límite de edad inferior, que deberá ser como mínimo de 16 años.	**Artículo 24.- Pornografía Infantil.** La producción, difusión, venta y cualquier tipo de comercialización de imágenes y representaciones de un niño, niña o adolescente con carácter pornográfico en los términos definidos en la presente ley, se sancionará con penas de dos a cuatro años de prisión y multa de diez a quinientas veces el salario mínimo. **Párrafo**.- **Adquisición y Posesión de Pornografía Infantil**. La adquisición de pornografía infantil por medio de un sistema de información para uno mismo u otra persona, y la posesión intencional de pornografía infantil en un sistema de información o cualquiera de sus componentes, se sancionará con la pena de tres meses a un año de prisión y multa de dos a doscientas veces el salario mínimo.

4. Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, los apartados d) y e) del párrafo 1 y los apartados b) y c) del párrafo 2.	
Título 4 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines	
Artículo 10 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual que defina su legislación, de conformidad con las obligaciones que haya contraído en aplicación del Acta de París de 24 de julio de 1971, por la cual se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Derecho de Autor, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático. 2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en su legislación, de conformidad con las obligaciones que haya asumido en aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas, a excepción de cualquier derecho moral conferido por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático. 3. En circunstancias bien delimitadas, toda Parte podrá reservarse el derecho de no imponer responsabilidad penal en virtud de los párrafos 1 y 2 del presente artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados	**Artículo 25.- Delitos Relacionados a la Propiedad Intelectual y Afines.** Cuando las infracciones establecidas en la Ley No.20-00, del 8 de mayo del año 2000, sobre Propiedad Industrial, y la Ley No.65-00, del 21 de agosto del año 2000, sobre Derecho de Autor, se cometan a través del empleo de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones, o de cualquiera de sus componentes, se sancionará con las penas establecidas en las respectivas legislaciones para estos actos ilícitos.

en los párrafos 1 y 2 del presente artículo.	
Título 5 – Otras formas de responsabilidad y de sanción	
Artículo 11 – Tentativa y complicidad 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier complicidad deliberada con vistas a la comisión de alguno de los delitos previstos en aplicación de los artículos 2 a 10 del presente Convenio, con la intención de que dicho delito sea cometido. 2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno toda tentativa deliberada de cometer alguno de los delitos previstos en aplicación de los artículos 3 a 5, 7, 8, 9.1.a) y 9.1.c) del presente Convenio. 3. Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, el párrafo 2 del presente artículo.	- Law 53-07 does not cover this aspect.-
Artículo 12 – Responsabilidad de las personas jurídicas 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos en aplicación del presente Convenio, cuando éstos sean cometidos por cuenta de las mismas por una persona física, ya sea a título individual o como miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en su seno, en virtud de: a. un poder de representación de la persona jurídica; b. una autorización para tomar decisiones en nombre de la persona jurídica; c. una autorización para ejercer funciones de control en el seno de la persona jurídica. 2. Además de los casos previstos en el párrafo 1 del presente artículo, Cada Parte adoptará las medidas necesarias para garantizar que pueda exigirse responsabilidad a una persona jurídica cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de un delito previsto en aplicación del presente Convenio por una persona física que actúe por cuenta de dicha persona	**Artículo 60.- Responsabilidad Civil y Penal de las Personas Morales.** Además de las sanciones que se indican más adelante, las personas morales son responsables civilmente 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 morales 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 morales no excluye la de cualquiera persona física, autor o cómplice de los mismos hechos. Cuando las personas morales sean utilizadas como medios o cubierta para la comisión de un crimen o un delito, o se incurra a través de ella en una omisión punible, las mismas 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 trate de un crimen o un delito sancionado en cuanto a las personas físicas se refiere con una pena privativa de libertad superior a cinco años;

jurídica y bajo su autoridad. 3. Dependiendo de los principios jurídicos de cada Parte, la responsabilidad de una persona jurídica podrá ser penal, civil o administrativa. 4. Dicha responsabilidad se entenderá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido el delito.	c) La prohibición, a título definitivo o por un período no mayor de cinco años, de ejercer directa o indirectamente una o varias actividades profesionales o sociales; d) La sujeción a la vigilancia judicial por un período no mayor de cinco años; e) La clausura definitiva o 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, a título definitivo o por un período no mayor de cinco años; g) La prohibición, a perpetuidad o 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; i) La publicación por carteles de la sentencia pronunciada o la difusión de ésta, sea por la prensa escrita o por otro medio de comunicación. **Párrafo.- Negligencia u Omisión de la Persona Moral.** Asimismo, se considerará responsable civilmente a una persona moral cuando la falta de vigilancia o de control de su representante legal o empleado haya hecho posible la comisión de un acto ilícito previsto en la presente ley.
Artículo 13 – Sanciones y medidas 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que los delitos previstos en aplicación de los artículos 2 a 11 estén sujetos a sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad. 2. Las Partes garantizarán la imposición de sanciones o medidas penales o	- Each offence includes the corresponding sanction. -

no penales efectivas, proporcionadas y disuasorias, incluidas sanciones pecuniarias, a las personas jurídicas consideradas responsables de conformidad con el artículo 12.	
Sección 2 – Derecho procesal	
Artículo 14 – Ámbito de aplicación de las disposiciones de procedimiento 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos previstos en la presente Sección a los efectos de investigación o de procedimientos penales específicos. 2. Salvo que se establezca lo contrario en el artículo 21, cada Parte aplicará los poderes y procedimientos mencionados en el párrafo 1 del presente artículo: a. a los delitos previstos en aplicación de los artículos 2 a 11 del presente Convenio; b. a cualquier otro delito cometido por medio de un sistema informático; y c. a la obtención de pruebas electrónicas de cualquier delito. 3. a. Las Partes podrán reservarse el derecho a aplicar las medidas mencionadas en el artículo 20 únicamente a los delitos o categorías de delitos especificados en su reserva, siempre que el repertorio de dichos delitos o categorías de delitos no sea más reducido que el de los delitos a los que dicha Parte aplique las medidas mencionadas en el artículo 21. Las Partes tratarán de limitar tal reserva de modo que sea posible la más amplia aplicación de la medida mencionada en el artículo 20. b. Cuando, a causa de las restricciones que imponga su legislación vigente en el momento de la adopción del presente Convenio, una Parte no pueda aplicar las medidas previstas en los artículos 20 y 21 a las comunicaciones transmitidas dentro de un sistema informático de un proveedor de servicios: i. que se haya puesto en funcionamiento para un grupo restringido de usuarios, y	**Artículo 52.- Aplicación del Código Procesal Penal.** Las reglas de la comprobación inmediata y medios auxiliares del Código Procesal Penal, Ley No.76-02, se aplicarán para la obtención y preservación de los datos contenidos en un sistema de información o sus componentes, datos de tráfico, conexión, acceso o cualquier otra información de utilidad, en la investigación de los delitos penalizados en la presente ley y para todos los procedimientos establecidos en este Capítulo.

ii. que no emplee las redes públicas de telecomunicación y no esté conectado a otro sistema informático, ya sea público o privado, dicha Parte podrá reservarse el derecho a no aplicar dichas medidas a esas comunicaciones. Las Partes tratarán de limitar este tipo de reservas de modo que de modo que sea posible la más amplia aplicación de las medidas previstas en los artículos 20 y 21.	
Artículo 15 – Condiciones y salvaguardias 1. Cada Parte se asegurará de que la instauración, ejecución y aplicación de los poderes y procedimientos previstos en la presente Sección se sometan a las condiciones y salvaguardias previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, y en particular de los derechos derivados de las obligaciones que haya asumido cada Parte en virtud del Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) u otros instrumentos internacionales aplicables en materia de derechos humanos, y que deberá integrar el principio de proporcionalidad. 2. Cuando proceda, teniendo en cuenta la naturaleza del procedimiento o del poder de que se trate, dichas condiciones y salvaguardias incluirán una supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen su aplicación, así como la limitación del ámbito de aplicación y de la duración de dicho poder o procedimiento. 3. Siempre que sea conforme con el interés público, y en particular con la buena administración de la justicia, cada Parte examinará los efectos de los poderes y procedimientos mencionados en la presente Sección sobre los derechos, responsabilidades e intereses legítimos de terceros.	**Artículo 57.- 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 diez 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 crímenes o delitos establecidos por la presente ley; b) El tráfico y comercialización de los datos obtenidos durante la investigación; c) La divulgación de datos personales y comerciales del procesado distintos a la naturaleza de la investigación, así como el tráfico o comercialización de los mismos.
Artículo 16 – Conservación rápida de datos informáticos almacenados 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación rápida de datos electrónicos específicos,	**Artículo 53.- Conservación de los Datos.** Las autoridades competentes actuarán con la celeridad requerida para conservar los datos contenidos en un sistema de información o sus componentes, o los datos de tráfico del sistema, principalmente cuando éstos sean vulnerables a su pérdida o modificación.

incluidos los datos relativos al tráfico, almacenados por medio de un sistema informático, en particular cuando existan motivos para creer que dichos datos son particularmente susceptibles de pérdida o de modificación. 2. Cuando una Parte aplique lo dispuesto en el párrafo 1 anterior por medio de una orden impartida a una persona de que conserve determinados datos almacenados que se encuentren en poder o bajo el control de esa persona, la Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a dicha persona a conservar y a proteger la integridad de los datos durante el tiempo necesario, hasta un máximo de noventa días, con el fin de que las autoridades competentes puedan obtener su revelación. Las Partes podrán prever la renovación de dicha orden. 3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a la persona que custodia los datos o a otra persona encargada de su conservación a mantener en secreto la ejecución de dichos procedimientos durante el tiempo previsto en su derecho interno. 4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.	
Artículo 17 – Conservación y revelación parcial rápidas de los datos relativos al tráfico 1. Con el fin de garantizar la conservación de los datos relativos al tráfico, en aplicación del artículo 16, cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para: a. garantizar la conservación rápida de los datos relativos al tráfico, ya sean uno o varios los proveedores de servicios que hayan participado en la transmisión de dicha comunicación; y b. asegurar la revelación rápida a la autoridad competente de la Parte, o a una persona designada por dicha autoridad, de un volumen suficiente de datos relativos al tráfico para que dicha Parte pueda identificar tanto a los proveedores de servicios como la vía por la que la comunicación se ha transmitido. 2. Los poderes y procedimientos mencionados en el presente artículo	**Artículo 56.- Proveedores de Servicios.** Sin perjuicio de lo establecido en el literal b) del Artículo 47 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 de noventa (90) días. 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 6 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.

estarán sujetos a lo dispuesto en los artículos 14 y 15.	
Artículo 18 – Orden de presentación 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar: a. a una persona presente en su territorio que comunique determinados datos informáticos que obren en su poder o bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento informático; y b. a un proveedor que ofrezca sus servicios en el territorio de dicha Parte, que comunique los datos que obren en su poder o bajo su control relativos a los abonados en relación con dichos servicios; 2. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15. 3. A los efectos del presente artículo, se entenderá por «datos relativos a los abonados» cualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido, y que permitan determinar: a. el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio; b. la identidad, la dirección postal o situación geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso y los datos relativos a la facturación y al pago, disponibles en virtud de un contrato o de un acuerdo de prestación de servicio; c. cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación, disponible en virtud de un contrato o de un acuerdo de prestación de servicio.	**Artículo 54.- Facultades del Ministerio Público**. Previo cumplimiento de las formalidades dispuestas en el Código Procesal Penal, el Ministerio Público, quien podrá auxiliarse de una o más de las siguientes personas: organismos de investigación del Estado, tales como el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional; la División de Investigación de Delitos Informáticos (DIDI) del Departamento Nacional de Investigaciones; peritos; instituciones públicas o privadas, u otra autoridad competente, tendrá la facultad de: a) Ordenar a una persona física o moral la entrega de la información que se encuentre en un sistema de información o en cualquiera de sus componentes;
Artículo 19 – Registro y confiscación de datos informáticos almacenados 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a registrar o a tener acceso de un modo similar:	**Artículo 54.- Facultades del Ministerio Público**. Previo cumplimiento de las formalidades dispuestas en el Código Procesal Penal, el Ministerio Público, quien podrá auxiliarse de una o más de las siguientes personas: organismos de investigación del Estado, tales como el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional; la División de Investigación de Delitos Informáticos (DIDI) del Departamento Nacional de

a. a todo sistema informático o a parte del mismo, así como a los datos informáticos en él almacenados; y b. a todo dispositivo de almacenamiento informático que permita almacenar datos informáticos en su territorio. 2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para asegurarse de que, cuando, de conformidad con el apartado 1.a), sus autoridades registren o tengan acceso de un modo similar a un sistema informático específico o a una parte del mismo y tengan motivos para creer que los datos buscados se hallan almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y que dichos datos son legítimamente accesibles a partir del sistema inicial o están disponibles por medio de dicho sistema inicial, puedan extender rápidamente el registro o el acceso de un modo similar al otro sistema. 3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a confiscar o a obtener de un modo similar los datos informáticos a los que se haya accedido en aplicación de los párrafos 1 o 2. Estas medidas incluirán las siguientes prerrogativas: a. confiscar u obtener de un modo similar un sistema informático o una parte del mismo, o un dispositivo de almacenamiento informático; b. realizar y conservar una copia de esos datos informáticos; c. preservar la integridad de los datos informáticos almacenados pertinentes; y d. hacer inaccesibles o suprimir dichos datos informáticos del sistema informático consultado. 4. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar a toda persona que conozca el funcionamiento de un sistema informático o las medidas aplicadas para proteger los datos informáticos que contiene, que proporcione toda la información necesaria, dentro de lo razonable, para permitir la aplicación de las medidas previstas en los párrafos 1 y 2. 5. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.	Investigaciones; peritos; instituciones públicas o privadas, u otra autoridad competente, tendrá la facultad de: b) Ordenar a una persona física o moral preservar y mantener la integridad de un sistema de información o de cualquiera de sus componentes, por un período de hasta noventa (90) días, pudiendo esta orden ser renovada por períodos sucesivos; e) Tomar en secuestro o asegurar un sistema de información o cualquiera de sus componentes, en todo o en parte; 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;

Artículo 20 – Obtención en tiempo real de datos relativos al tráfico 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes: a. a obtener o grabar con medios técnicos existentes en su territorio, y b. a obligar a cualquier proveedor de servicios, en la medida de sus capacidades técnicas: i. a obtener o a grabar con medios técnicos existentes en su territorio, o ii. a ofrecer a las autoridades competentes su colaboración y su asistencia para obtener o grabar en tiempo real los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático. 2. Cuando una Parte no pueda adoptar las medidas enunciadas en el apartado 1.a) por respeto a los principios establecidos en su ordenamiento jurídico interno, podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en dicho territorio. 3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto. 4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.	**Artículo 54.- Facultades del Ministerio Público**. Previo cumplimiento de las formalidades dispuestas en el Código Procesal Penal, el Ministerio Público, quien podrá auxiliarse de una o más de las siguientes personas: organismos de investigación del Estado, tales como el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional; la División de Investigación de Delitos Informáticos (DIDI) del Departamento Nacional de Investigaciones; peritos; instituciones públicas o privadas, u otra autoridad competente, tendrá la facultad de: k) Solicitar al 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,
Artículo 21 – Interceptación de datos relativos al contenido 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes en lo que respecta a un repertorio de delitos graves que deberá definirse en su derecho interno a: a. obtener o grabar con medios técnicos existentes en su territorio, y b. obligar a un proveedor de servicios, en la medida de sus capacidades	**Artículo 54.- Facultades del Ministerio Público**. Previo cumplimiento de las formalidades dispuestas en el Código Procesal Penal, el Ministerio Público, quien podrá auxiliarse de una o más de las siguientes personas: organismos de investigación del Estado, tales como el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional; la División de Investigación de Delitos Informáticos (DIDI) del Departamento Nacional de

técnicas, a: i. obtener o grabar con medios técnicos existentes en su territorio, o ii. prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar, en tiempo real los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio por medio de un sistema informático. 2. Cuando una Parte no pueda adoptar las medidas enunciadas en el apartado 1.a) por respeto a los principios establecidos en su ordenamiento jurídico interno, podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio con medios técnicos existentes en ese territorio. 3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto. 4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.	Investigaciones; peritos; instituciones públicas o privadas, u otra autoridad competente, tendrá la facultad de: d) Ordenar a un proveedor de servicios, incluyendo los proveedores de servicios de Internet, a suministrar información de los datos relativos a un usuario que pueda tener en su posesión o control;
Sección 3 – Jurisdicción	
Artículo 22 – Jurisdicción 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto de conformidad con los artículos 2 a 11 del presente Convenio, cuando el delito se haya cometido: a. en su territorio; o b. a bordo de un buque que enarbole su pabellón; o c. a bordo de una aeronave matriculada según sus leyes; o d. por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo. 2. Las Partes podrán reservarse el derecho a no aplicar, o a aplicar sólo en determinados casos o condiciones, las normas sobre jurisdicción establecidas en los apartados 1.b) a 1.d) del presente artículo o en cualquier parte de	**Artículo 65.- Tribunal Competente.** Los casos sobre crímenes y delitos de alta tecnología serán conocidos por los tribunales ordinarios correspondientes o por el Tribunal de Niños, Niñas y Adolescentes, dependiendo del caso. Los jueces podrán valerse de la presentación de un peritaje para el conocimiento del fondo del caso.

dichos apartados. 3. Cada Parte adoptará las medidas que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito mencionado en el párrafo 1 del artículo 24 del presente Convenio cuando el presunto autor del mismo se halle en su territorio y no pueda ser extraditado a otra Parte por razón únicamente de su nacionalidad, previa demanda de extradición. 4. El presente Convenio no excluye ninguna jurisdicción penal ejercida por una Parte de conformidad con su derecho interno. 5. En el caso de que varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, cuando ello sea oportuno, con el fin de decidir qué jurisdicción es más adecuada para entablar la acción penal.	
Capítulo III – Cooperación internacional	
Artículo 24 – Extradición 1. a. El presente artículo se aplicará a la extradición entre las Partes por los delitos definidos de conformidad con los artículos 2 a 11 del presente Convenio, siempre que sean castigados por la legislación de las dos Partes implicadas con una pena privativa de libertad de una duración de al menos un año, o con una pena más grave. b. Cuando se aplique una pena mínima diferente en virtud de un tratado de extradición aplicable entre dos o más Partes, incluido el Convenio Europeo de Extradición (STE nº 24), o de un acuerdo basado en legislación uniforme o recíproca, se aplicará la pena mínima prevista en dicho tratado o acuerdo. 2. Se considerará que los delitos descritos en el párrafo 1 del presente artículo están incluidos entre los delitos que pueden dar lugar a extradición en todos los tratados de extradición concluidos entre o por las Partes. Las Partes se comprometerán a incluir dichos delitos entre los que pueden dar lugar a extradición en todos los tratados de extradición que puedan concluir. 3. Cuando una parte que condicione la extradición a la existencia de un	Ley No. 489 sobre Extradición en la República Dominicana Art. 5.- (Modificada por la Ley 278-98 del 29 de julio de 1998). La extradición de un extranjero no podrá concederse, en los siguientes casos: a) Por delitos políticos conforme lo define la Ley 5007, del 1911, que modifica el Código Penal Dominicano; b) Por hechos que no estén calificados como infracciones sancionadas por la ley penal dominicana

tratado reciba una demanda de extradición de otra Parte con la que no ha concluido ningún tratado de extradición, podrá tomar el presente Convenio como fundamento jurídico de la extradición en relación con cualquiera de los delitos previstos en el párrafo 1 del presente artículo. 4. Las Partes que no condicionen la extradición a la existencia de un tratado reconocerán los delitos mencionados en el párrafo 1 del presente artículo como delitos que pueden dar lugar a extradición entre ellas. 5. La extradición estará sujeta a las condiciones previstas en el derecho interno de la Parte requerida o en los tratados de extradición vigentes, incluidos los motivos por los que la Parte requerida puede denegar la extradición. 6. Si se deniega la extradición por un delito mencionado en el párrafo 1 del presente artículo únicamente por razón de la nacionalidad de la persona reclamada o porque la Parte requerida se considera competente respecto de dicho delito, la Parte requerida deberá someter el asunto, a petición de la Parte requirente, a sus autoridades competentes a efectos de la acción penal pertinente, e informará, a su debido tiempo, de la conclusión del asunto a la Parte requirente. Dichas autoridades tomarán su decisión y realizarán sus investigaciones y procedimientos del mismo modo que para cualquier otro delito de naturaleza comparable, de conformidad con la legislación de dicha Parte. 7. a. Cada Parte comunicará al Secretario General del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, el nombre y la dirección de cada autoridad responsable del envío o de la recepción de las demandas de extradición o de detención provisional, en ausencia de tratado. b. El Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades designadas por las Partes. Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro.	
Artículo 25 – Principios generales relativos a la asistencia mutua	**Código procesal penal de la República Dominicana penal capítulo 4,**

1. Las Partes se prestarán toda la ayuda mutua posible a efectos de las investigaciones o de los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o con el fin de obtener pruebas en formato electrónico de un delito. 2. Cada Parte adoptará asimismo las medidas legislativas y de otro tipo que resulten necesarias para cumplir con las obligaciones establecidas en los artículos 27 a 35. 3. Cada Parte podrá, en caso de urgencia, formular una solicitud de asistencia mutua, o realizar las comunicaciones relativas a la misma a través de medios de comunicación rápidos, como el fax o el correo electrónico, siempre que esos medios ofrezcan niveles suficientes de seguridad y de autenticación (incluido el criptado, en caso necesario), con confirmación oficial posterior si el Estado requerido así lo exige. El Estado requerido aceptará la solicitud y responderá a la misma por cualquiera de esos medios rápidos de comunicación. 4. Salvo en caso de que se disponga expresamente otra cosa en los artículos del presente Capítulo, la asistencia mutua estará sujeta a las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de asistencia mutua aplicables, incluidos los motivos sobre la base de los cuales la Parte requerida puede rechazar la cooperación. La Parte requerida no deberá ejercer su derecho a rehusar la asistencia mutua en relación con los delitos previstos en los artículos 2 a 11 únicamente porque la solicitud se refiera a un delito que dicha Parte considere de carácter fiscal. 5. Cuando, de conformidad con lo dispuesto en el presente Capítulo, la Parte requerida esté autorizada a condicionar la asistencia mutua a la existencia de doble tipificación penal, se considerará que dicha condición se satisface si el acto que constituye delito, y para el que se solicita la asistencia mutua, está tipificado como tal en su derecho interno, independientemente de que dicho derecho interno incluya o no el delito en la misma categoría o lo denomine o no con la misma terminología que la Parte requirente.	**cooperación judicial internacional** **Art. 155. Cooperación.** Los jueces y el ministerio público deben brindar la máxima cooperación a las solicitudes de las autoridades extranjeras siempre que sean formuladas conforme a lo previsto en los tratados internacionales y este código. En los casos de urgencia, el juez o el ministerio público, según corresponda, pueden dirigir, por cualquier medio, requerimientos de cooperación a cualquier autoridad judicial o administrativa, en cuyo caso informa posteriormente a la Secretaría de Estado de Relaciones Exteriores.
Artículo 26 – Información espontánea 1. Dentro de los límites de su derecho interno y sin que exista demanda previa, una Parte podrá comunicar a otra Parte información obtenida de sus	**A través de la Red I 24/7 de Interpol, de la cual somos país miembro.**

propias investigaciones si considera que ello puede ayudar a la Parte destinataria a iniciar o a concluir investigaciones o procedimientos en relación con delitos previstos de conformidad con el presente Convenio, o cuando dicha información pueda conducir a una petición de cooperación de dicha Parte en virtud del presente Capítulo. 2. Antes de comunicar dicha información, la Parte que la proporciona podrá pedir que sea tratada de forma confidencial o que sólo se utilice bajo ciertas condiciones. Si la Parte destinataria no puede atender a dicha petición, deberá informar de ello a la otra Parte, que decidirá a continuación si, no obstante, debe proporcionar la información. Si la Parte destinataria acepta la información bajo las condiciones establecidas, estará obligada a respetarlas.	
Artículo 27 – Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables 1. En ausencia de tratado de asistencia mutua o de acuerdo basado en legislación uniforme o recíproca en vigor entre la Parte requirente y la Parte requerida, se aplicarán las disposiciones de los párrafos 2 a 9 del presente artículo. Dichas disposiciones no se aplicarán cuando exista un tratado, acuerdo o legislación de este tipo, a menos que las Partes implicadas decidan aplicar en su lugar la totalidad o una parte del resto del presente artículo. 2. a. Cada Parte designará una o varias autoridades centrales encargadas de enviar las solicitudes de asistencia mutua o de responder a las mismas, de ejecutarlas o de remitirlas a las autoridades competentes para su ejecución; b. las autoridades centrales comunicarán directamente entre sí; c. en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte comunicará al Secretario General del Consejo de Europa los nombres y direcciones de las autoridades designadas en aplicación del presente párrafo. d. el Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades centrales designadas por las Partes. Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro. 3. Las solicitudes de asistencia mutua en virtud del presente artículo se ejecutarán de conformidad con el procedimiento especificado por la Parte requirente, salvo cuando dicho procedimiento sea incompatible con la	**A través de la Red I 24/7 de Interpol, de la cual somos país miembro.**

legislación de la Parte requerida. 4. Además de las condiciones o los motivos de denegación previstos en el párrafo 4 del artículo 25, la asistencia mutua puede ser denegada por la Parte requerida: a. si la solicitud tiene que ver con un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político; o b. si la Parte requerida estima que acceder a la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales. 5. La Parte requerida podrá aplazar su actuación en respuesta a una solicitud si dicha actuación puede perjudicar a investigaciones o procedimientos llevados a cabo por sus autoridades. 6. Antes de denegar o aplazar su cooperación, la Parte requerida estudiará, previa consulta con la Parte requirente cuando proceda, si puede atenderse la solicitud parcialmente o bajo las condiciones que considere necesarias. 7. La Parte requerida informará rápidamente a la Parte requirente del curso que prevé dar a la solicitud de asistencia. Deberá motivar toda denegación o aplazamiento de la misma. La Parte requerida informará asimismo a la Parte requirente de cualquier motivo que imposibilite la ejecución de la asistencia o que pueda retrasarla sustancialmente. 8. La Parte requirente podrá solicitar que la Parte requerida mantenga confidenciales la presentación y el objeto de cualquier solicitud formulada en virtud del presente Capítulo, salvo en la medida en que sea necesario para la ejecución de la misma. Si la Parte requerida no puede acceder a la petición de confidencialidad, deberá informar de ello sin demora a la Parte requirente, quien decidirá a continuación si, no obstante, la solicitud debe ser ejecutada. 9. a. En caso de urgencia, las autoridades judiciales de la Parte requirente podrán dirigir directamente a las autoridades homólogas de la Parte requerida las solicitudes de asistencia y las comunicaciones relativas a las mismas. En tales casos, se remitirá simultáneamente una copia a la autoridad central de la Parte requerida a través de la autoridad central de la Parte requirente. b. Toda solicitud o comunicación en virtud del presente párrafo podrá formularse a través de la Organización Internacional de Policía Criminal (Interpol). c. Cuando se formule una solicitud en aplicación del apartado a) del	

presente artículo y la autoridad no tenga competencia para tratarla, la remitirá a la autoridad nacional competente e informará directamente de ello a la Parte requirente. d. Las solicitudes o comunicaciones realizadas en aplicación del presente párrafo que no impliquen medidas coercitivas podrán ser transmitidas directamente por las autoridades competentes de la Parte requirente a las autoridades competentes de la Parte requerida. e. En el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, las Partes podrán informar al Secretario General del Consejo de Europa de que, en aras de la eficacia, las solicitudes formuladas en virtud del presente párrafo deberán dirigirse a su autoridad central.	
Artículo 28 – Confidencialidad y restricciones de uso 1. En ausencia de tratado de asistencia mutua o de acuerdo basado en legislación uniforme o recíproca en vigor entre la Parte requirente y la Parte requerida, se aplicarán las disposiciones del presente artículo. Dichas disposiciones no se aplicarán cuando exista un tratado, acuerdo o legislación de este tipo, a menos que las Partes interesadas decidan aplicar en su lugar la totalidad o una parte del presente artículo. 2. La Parte requerida podrá supeditar la transmisión de información o de material en respuesta a una solicitud al cumplimiento de las siguientes condiciones: a. que se preserve su confidencialidad cuando la solicitud de asistencia no pueda ser atendida en ausencia de dicha condición; o b. que no se utilicen para investigaciones o procedimientos distintos a los indicados en la solicitud. 3. Si la Parte requirente no pudiera satisfacer alguna de las condiciones mencionadas en el párrafo 2, informará de ello sin demora a la Parte requerida, quien determinará a continuación si, no obstante, la información ha de ser proporcionada. Si la Parte requirente acepta esta condición, estará obligada a cumplirla. 4. Toda Parte que proporcione información o material supeditado a alguna de las condiciones mencionadas en el párrafo 2 podrá exigir a la otra Parte precisiones sobre el uso que haya hecho de dicha información o material en relación con dicha condición.	**Ley General de Libre Acceso a la Información Pública, No. 200-04.**

Sección 2 – Disposiciones específicas	
Artículo 29 – Conservación rápida de datos informáticos almacenados 1. Una Parte podrá solicitar a otra Parte que ordene o imponga de otro modo la conservación rápida de datos almacenados por medio de sistemas informáticos que se encuentren en el territorio de esa otra Parte, y en relación con los cuales la Parte requirente tenga intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, la confiscación o la obtención por un medio similar, o a la revelación de dichos datos. 2. En toda solicitud de conservación formulada en virtud del párrafo 1 deberá precisarse: a. la autoridad que solicita la conservación; b. el delito objeto de la investigación o de procedimientos penales y una breve exposición de los hechos relacionados con el mismo; c. los datos informáticos almacenados que deben conservarse y su relación con el delito; d. toda información disponible que permita identificar al responsable de la custodia de los datos informáticos almacenados o el emplazamiento del sistema informático; e. la necesidad de la medida de conservación; y f. que la Parte tiene intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, a la confiscación o a la obtención por un medio similar, o a la revelación de los datos informáticos almacenados. 3. Tras recibir la solicitud de otra Parte, la Parte requerida deberá adoptar todas las medidas adecuadas para proceder sin demora a la conservación de los datos solicitados, de conformidad con su derecho interno. A los efectos de responder a solicitudes de este tipo no se requiere la doble tipificación penal como condición para proceder a la conservación. 4. Cuando una Parte exige la doble tipificación penal como condición para atender a una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, a la confiscación o a la obtención por un medio similar o a la revelación de los datos almacenados en relación con delitos diferentes de los previstos de conformidad con los artículos 2 a 11 del presente	**Ley Contra Crimenes y Delitos de Alta Tecnologia 53-07.** **Artículo 54.- Facultades del Ministerio Público**. Previo cumplimiento de las formalidades dispuestas en el Código Procesal Penal, el Ministerio Público, quien podrá auxiliarse de una o más de las siguientes personas: organismos de investigación del Estado, tales como el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional; la División de Investigación de Delitos Informáticos (DIDI) del Departamento Nacional de investigaciones; peritos; instituciones públicas o privadas, u otra autoridad competente, tendrá la facultad de: a) Ordenar a una persona física o moral preservar y mantener la integridad de un sistema de información o de cualquiera de sus componentes, por un período de hasta noventa (90) días, pudiendo esta orden ser renovada por períodos sucesivos; j) Solicitar al 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;

Convenio, podrá reservarse el derecho a denegar la solicitud de conservación en virtud del presente artículo en caso de que tenga motivos para creer que, en el momento de la revelación de los datos, no se cumplirá la condición de la doble tipificación penal. 5. Asimismo, las solicitudes de conservación sólo podrán ser denegadas si: a. la solicitud se refiere a un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político; o b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales. 6. Cuando la Parte requerida considere que la conservación por sí sola de los datos no bastará para garantizar su disponibilidad futura, o que pondrá en peligro la confidencialidad de la investigación de la Parte requirente, o causará cualquier otro perjuicio a la misma, informará de ello rápidamente a la Parte requirente, quien determinará a continuación la conveniencia, no obstante, de dar curso a la solicitud. 7. Las medidas de conservación adoptadas en respuesta a solicitudes como la prevista en el párrafo 1 serán válidas por un periodo mínimo de 60 días, con el fin de que la Parte requirente pueda presentar una solicitud con vistas al registro o el acceso por un medio similar, la confiscación o la obtención por un medio similar, o la revelación de los datos. Una vez recibida la solicitud, los datos deberán conservarse hasta que se tome una decisión sobre la misma.	
Artículo 30 – Revelación rápida de datos conservados 1. Si, al ejecutar una solicitud formulada de conformidad con el artículo 29 para la conservación de datos relativos al tráfico de una determinada comunicación la Parte requerida descubriera que un proveedor de servicios de otro Estado ha participado en la transmisión de dicha comunicación, dicha Parte revelará rápidamente a la Parte requirente un volumen suficiente de datos relativos al tráfico para que pueda identificarse al proveedor de servicios, así como la vía por la que la comunicación ha sido transmitida. 2. La revelación de datos relativos al tráfico en aplicación del párrafo 1 sólo podrá ser denegada si: a. la solicitud se refiere a un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político; o b. la Parte requerida considera que la ejecución de la solicitud podría atentar	**Ley Contra Crimenes y Delitos de Alta Tecnologia 53-07.** **Artículo 54.- Facultades del Ministerio Público**. Previo cumplimiento de las formalidades dispuestas en el Código Procesal Penal, el Ministerio Público, quien podrá auxiliarse de una o más de las siguientes personas: organismos de investigación del Estado, tales como el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional; la División de Investigación de Delitos Informáticos (DIDI) del Departamento Nacional de investigaciones; peritos; instituciones públicas o privadas, u otra autoridad competente, tendrá la facultad de: Ordenar a una persona física o moral preservar y mantener la integridad de un

contra su soberanía, seguridad, orden público u otros intereses esenciales.	sistema de información o de cualquiera de sus componentes, por un período de hasta noventa (90) días, pudiendo esta orden ser renovada por períodos sucesivos;
Artículo 31 – Asistencia mutua en relación con el acceso a datos almacenados 1. Una Parte podrá solicitar a otra Parte el registro o el acceso de un modo similar, la confiscación o la obtención de un modo similar o la revelación de datos almacenados por medio de un sistema informático que se encuentre en el territorio de esa otra Parte, incluidos los datos conservados de conformidad con el artículo 29. 2. La Parte requerida responderá a la solicitud aplicando los instrumentos internacionales, acuerdos y legislación mencionados en el artículo 23, así como de conformidad con las disposiciones pertinentes del presente Capítulo. 3. La solicitud deberá responderse lo más rápidamente posible en los siguientes casos: a. cuando existan motivos para creer que los datos pertinentes están particularmente expuestos al riesgo de pérdida o de modificación; o b. cuando los instrumentos, acuerdos o legislación mencionados en el párrafo 2 prevean una cooperación rápida.	**Código Procesal Penal de la República Dominicana Penal Capítulo 4, Cooperación Judicial Internacional** **Art. 155. Cooperación.** Los jueces y el ministerio público deben brindar la máxima cooperación a las solicitudes de las autoridades extranjeras siempre que sean formuladas conforme a lo previsto en los tratados internacionales y este código. En los casos de urgencia, el juez o el ministerio público, según corresponda, pueden dirigir, por cualquier medio, requerimientos de cooperación a cualquier autoridad judicial o administrativa, en cuyo caso informa posteriormente a la Secretaría de Estado de Relaciones Exteriores. **Ley Contra Crimenes y Delitos de Alta Tecnologia 53-07.** **Artículo 54.- Facultades del Ministerio Público**. Previo cumplimiento de las formalidades dispuestas en el Código Procesal Penal, el Ministerio Público, quien podrá auxiliarse de una o más de las siguientes personas: organismos de investigación del Estado, tales como el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional; la División de Investigación de Delitos Informáticos (DIDI) del Departamento Nacional de investigaciones; peritos; instituciones públicas o privadas, u otra autoridad competente, tendrá la facultad de: Ordenar a una persona física o moral preservar y mantener la integridad de un sistema de información o de cualquiera de sus componentes, por un período de hasta noventa (90) días, pudiendo esta orden ser renovada por períodos sucesivos;
Artículo 32 – Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público	**Ley Contra Crimenes y Delitos de Alta Tecnologia 53-07.** **Artículo 54.- Facultades del Ministerio Público**. Previo cumplimiento de las

Una Parte podrá, sin autorización de otra: a. tener acceso a datos informáticos almacenados accesibles al público (fuente abierta), independientemente de la ubicación geográfica de los mismos; o b. tener acceso a datos informáticos almacenados en otro Estado, o recibirlos, a través de un sistema informático situado en su territorio, si dicha Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada a revelárselos por medio de ese sistema informático.	formalidades dispuestas en el Código Procesal Penal, el Ministerio Público, quien podrá auxiliarse de una o más de las siguientes personas: organismos de investigación del Estado, tales como el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional; la División de Investigación de Delitos Informáticos (DIDI) del Departamento Nacional de investigaciones; peritos; instituciones públicas o privadas, u otra autoridad competente, tendrá la facultad de: a) Ordenar a una persona física o moral preservar y mantener la integridad de un sistema de información o de cualquiera de sus componentes, por un período de hasta noventa (90) días, pudiendo esta orden ser renovada por períodos sucesivos; b) b Acceder u ordenar el acceso a dicho sistema de información o a cualquiera de sus componentes; c) Ordenar a un proveedor de servicios, incluyendo los proveedores de servicios de Internet, a suministrar información de los datos relativos a un usuario que pueda tener en su posesión o control; d) Tomar en secuestro o asegurar un sistema de información o cualquiera de sus componentes, en todo o en parte; e) Realizar y retener copia del contenido del sistema de información o de cualquiera de sus componentes; f) Ordenar el mantenimiento de la integridad del contenido de un sistema de información o de cualquiera de sus componentes; g) Hacer inaccesible o remover el contenido de un sistema de información o de cualquiera de sus componentes, que haya sido accesado para la investigación; h) 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;

	i) Recolectar o grabar los datos de un sistema de información o de cualquiera de sus componentes, a través de la aplicación de medidas tecnológicas; j) Solicitar al 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; k) 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, l) Ordenar cualquier otra medida aplicable a un sistema de información o sus componentes para obtener los datos necesarios y asegurar la preservación de los mismos.
Artículo 33 – Asistencia mutua para la obtención en tiempo real de datos relativos al tráfico 1. Las Partes se prestarán asistencia mutua para la obtención en tiempo real de datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático. A reserva de las disposiciones del párrafo 2, dicha asistencia mutua estará sujeta a las condiciones y procedimientos previstos en el derecho interno. 2. Cada Parte prestará dicha asistencia al menos en relación con los delitos para los cuales sería posible la obtención en tiempo real de datos relativos al tráfico en situaciones análogas a nivel interno.	**Ley Contra Crimenes y Delitos de Alta Tecnologia 53-07.** **Artículo 54.- Facultades del Ministerio Público**. Previo cumplimiento de las formalidades dispuestas en el Código Procesal Penal, el Ministerio Público, quien podrá auxiliarse de una o más de las siguientes personas: organismos de investigación del Estado, tales como el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional; la División de Investigación de Delitos Informáticos (DIDI) del Departamento Nacional de investigaciones; peritos; instituciones públicas o privadas, u otra autoridad competente, tendrá la facultad de: a) Ordenar a una persona física o moral preservar y mantener la integridad

	de un sistema de información o de cualquiera de sus componentes, por un período de hasta noventa (90) días, pudiendo esta orden ser renovada por períodos sucesivos; b) b Acceder u ordenar el acceso a dicho sistema de información o a cualquiera de sus componentes; c) Ordenar a un proveedor de servicios, incluyendo los proveedores de servicios de Internet, a suministrar información de los datos relativos a un usuario que pueda tener en su posesión o control; d) Tomar en secuestro o asegurar un sistema de información o cualquiera de sus componentes, en todo o en parte; e) Realizar y retener copia del contenido del sistema de información o de cualquiera de sus componentes; f) Ordenar el mantenimiento de la integridad del contenido de un sistema de información o de cualquiera de sus componentes; g) Hacer inaccesible o remover el contenido de un sistema de información o de cualquiera de sus componentes, que haya sido accesado para la investigación; h) 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; i) Recolectar o grabar los datos de un sistema de información o de cualquiera de sus componentes, a través de la aplicación de medidas tecnológicas; j) Solicitar al 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;

	k) 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, l) Ordenar cualquier otra medida aplicable a un sistema de información o sus componentes para obtener los datos necesarios y asegurar la preservación de los mismos.
Artículo 34 – Asistencia mutua en relación con la interceptación de datos relativos al contenido Las Partes se prestarán asistencia mutua, en la medida en que lo permitan sus tratados y leyes internas aplicables, para la obtención o el registro en tiempo real de datos relativos al contenido de comunicaciones específicas transmitidas por medio de un sistema informático.	**Ley Contra Crimenes y Delitos de Alta Tecnologia 53-07.** **Artículo 54.- Facultades del Ministerio Público**. Previo cumplimiento de las formalidades dispuestas en el Código Procesal Penal, el Ministerio Público, quien podrá auxiliarse de una o más de las siguientes personas: organismos de investigación del Estado, tales como el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional; la División de Investigación de Delitos Informáticos (DIDI) del Departamento Nacional de investigaciones; peritos; instituciones públicas o privadas, u otra autoridad competente, tendrá la facultad de: Realizar y retener copia del contenido del sistema de información o de cualquiera de sus componentes; Ordenar el mantenimiento de la integridad del contenido de un sistema de información o de cualquiera de sus componentes; 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,
Artículo 35 – Red 24/7 1. Cada Parte designará un punto de contacto localizable las 24 horas del día, siete días a la semana, con el fin de garantizar una asistencia inmediata para investigaciones relativas a delitos vinculados a sistemas y datos	

informáticos, o para obtener las pruebas en formato electrónico de un delito. Esta asistencia comprenderá toda acción que facilite las medidas que figuran a continuación, o su aplicación directa si lo permite el derecho y la práctica internos: a. asesoramiento técnico; b. conservación de datos, de conformidad con los artículos 29 y 30; y c. obtención de pruebas, suministro de información de carácter jurídico y localización de sospechosos. 2. a. El punto de contacto de una Parte dispondrá de los medios para comunicarse con el punto de contacto de otra Parte siguiendo un procedimiento acelerado. b. Si el punto de contacto designado por una Parte no depende de la autoridad o autoridades de dicha Parte responsables de la asistencia mutua internacional o de la extradición, dicho punto de contacto se asegurará de poder actuar coordinadamente con esta o estas autoridades por medio de un procedimiento acelerado. 3. Cada Parte garantizará la disponibilidad de personal formado y equipado con objeto de facilitar el funcionamiento de la red.	
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	