First draft (30 May 2007)

Cybercrime legislation – country profile

Dominican Republic

This profile has been prepared within the framework of the Council of Europe's Project on Cybercrime in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the country covered or of the Council of Europe.

Comments may be sent to:

Alexander Seger
Department of Technical Cooperation
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

Country:	**Dominican Republic**
Signature of Convention:	No
Ratification/accession:	No What measures are being undertaken in your country to become a Party? *We have taken account of the provisions of the Convention in our recent Law 53-07 against cybercrime.* What specific obstacles (legislative or other) prevent ratification/accession? *It is necessary to obtain congressional approval*.
Provisions of the Convention	***Corresponding provisions/solutions in national legislation*** *(pls quote or summarise briefly; pls attach relevant extracts as an appendix)*
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data"	**Computer system:** Any electronic device, regardless of its form, size, capacity or technology used, capable of processing data and/or signals and performing logical, arithmetical and memory functions by manipulating electronic, optical, magnetic, electro-chemical or any other type of impulses, including all input, output, processing, storage, programme, communication or other facilities connected or linked to or integrated with the system. **Computer data:** Any information transmitted, saved, recorded, processed, copied or stored in any type of information system or in any of its component parts, such as those geared to the transmission, emission, storage, processing and reception of electro-

	magnetic signals, signs, signals, writing, still or moving images, videos, voice, sounds, data transmitted by optical, cellular or radio-electrical means, electro-magnetic systems or through any other channel suited to the purpose.
Chapter II – Measures to be taken at the national level *Section 1 – Substantive criminal law*	
Article 2 – Illegal access	**Article 6.- Illegal access.** The fact of acceding to an electronic, computing, telematics or telecommunications system, or its component parts, whether or not by usurping an identity or exceeding authorisation, shall be punished with a prison sentence of between three months and one year and a fine of up to two hundred times the minimum wage.
Article 3 – Illegal interception	**Article 9.- Interception and tapping of data or signals.** The fact of intercepting, tapping, interfering with, blocking, spying and listening in on, diverting, recording and observing, in any way, an item or set of data, a signal or transmission of data or signals belonging to another person on one's own or someone else's behalf, without prior authorisation from a competent judge, from, through or towards an electronic, computing, telematics or telecommunications system, or information transmitted by the latter, deliberately and intentionally violating the secrecy, confidentiality and privacy of natural or legal persons, shall be punished with a prison sentence of between one and three years and a fine of between twenty and one hundred times the minimum wage, without prejudice to any administrative sanctions imposed under separate laws and regulations.
Article 4 – Data interference	**Article 10.- Damaging and altering computer data.** The fact of deleting, damaging, introducing, copying, deforming, editing, altering or eliminating data and component parts of electronic, computing, telematics or telecommunications systems, or transmitted through one of the latter, for fraudulent purposes, shall be punished with a prison sentence of between three months and one year and a fine of between three and five hundred times the minimum wage.
Article 5 – System interference	**Article 11.- Sabotage.** The fact of altering, deforming, impeding, disabling, causing to malfunction, damaging or destroying an electronic, computing, telematics or telecommunications system or the programmes and logical operations run by such system shall be punished with a prison sentence of between three months and two years and a fine of between three and five hundred times the minimum wage.
Article 6 – Misuse of devices	**Article 8.- Fraudulent devices.** The fact of producing, using, possessing, trafficking in or distributing, without authorisation or legitimate cause, computer programmes, hardware, equipment or devices whose sole or primary use is to commit high-technology crimes and offences, shall be punished with a prison sentence of between one and three years and a fine of between twenty and one hundred times the minimum wage.
Article 7 – Computer-related forgery	**Article 18.- Forged documents and signatures.** Anyone forging, decoding or in any way deciphering, disclosing or trafficking in

	digital or electronic documents, signatures, certificates, shall be punished with a prison sentence of between one and three years and a fine of between fifty and two hundred times the minimum wage.
Article 8 – Computer-related fraud	**Article 13.- High-technology theft.** Where theft is committed by using electronic, computing, telematics or telecommunications systems or devices to disable or inhibit alarm, protection or other similar mechanisms; or in cases where, in order to gain access to houses or other premises or to movables, recourse is had to the same means or means different from those intended by their owner for such purposes; or by using magnetic or perforated cards, controls or instruments for remote opening or any other high-technology mechanism or device, shall be punished with a prison sentence of between two and five years and a fine of between twenty and five hundred times the minimum salary. **Article 14.- Illegal obtainment of funds.** The fact of obtaining funds, appropriations or assets by coercing the legitimate user of a computing, electronic, telematics or telecommunications financial service shall be punished with a prison sentence of between three and ten years and a fine of between one hundred and five hundred times the minimum wage. **Paragraph.- Electronic transfers of funds.** The fact of effecting electronic transfers of funds through the illegal use of access codes or of any other similar mechanism, shall be punished with a prison sentence of between one and five years and a fine of between two and two hundred times the minimum wage. **Article 15.- Fraud.** Fraud committed through the use of electronic, computing, telematics or telecommunications facilities shall be punished with a prison sentence of between three months and seven years and a fine of between ten and five hundred times the minimum wage. **Article 16.- Blackmail**. Blackmail committed by means of electronic, computing, telematics or telecommunications systems or their component parts, and/or for the purpose of obtaining funds, assets, or the signature or handover of a document, whether digital or not, or an access code or any other component of a computer system, shall be punished with a prison sentence of between one and five years and a fine of between ten and two hundred times the minimum wage.
Article 9 – Offences related to child pornography	**Article 24.- Child pornography.** The production, circulation, sale and any form of marketing of images or representations of a child or adolescent of a pornographic nature as defined in this law shall be punished with a prison sentence of between two and four years and a fine of between ten and five hundred times the minimum wage. **Paragraph**.- **Purchase and possession of child pornography**. The purchase of child pornography via an information system for oneself or another person, and the deliberate possession of child pornography in an information system or any of its component parts shall be punished with a prison sentence of between three months and one year and a fine of between two and two hundred times the minimum wage.
Title 4 – Offences related to infringements of	

copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights	**Article 25.- Offences related to intellectual property and related subjects.** Where the offences set out in Law No.20-00 of 8 May 2000 on Industrial Property and Law No.65-00 of 21 August 2000 on Copyright are committed via electronic, computing, telematics or telecommunications systems or via any of their component parts, the culprit shall be liable to the penalties laid down in the relevant legislation on these illegal acts.
Article 11 – Attempt and aiding or abetting	- Law 53-07 does not cover this aspect.-
Article 12 – Corporate liability	**Article 60.- Civil and criminal responsibility of legal persons.** In addition to the sanctions set out below, legal persons bear civil responsibility for offences committed by their subordinate bodies or representatives. Criminal responsibility for the acts and offences set out in this law extends to the individuals ordering or arranging their commission and the legal representatives of the legal persons who, being apprised of the illegality of the act and empowered to prevent it, have permitted, taken part in, facilitated or concealed it. Criminal responsibility on the part of legal persons does not preclude that of any natural person who has perpetrated or aided the acts in question. Where the legal persons are used as a means or as cover for the commission of a crime or offence, or if they are used to commit an act of culpable negligence, they will be liable to one or more or all of the following penalties: a) A fine equal to or up to twice that imposed on the natural person for the illegal act as set out in this law; b) Liquidation, in cases of a crime or offence penalised, in the case of natural persons, with a prison sentence of more than five years; c) Prohibition, on a permanent basis or for a period of not more than five years, of direct or indirect exercise of specific professional or social activities; d) Subjection to court supervision for a period of not more than five years; e) Closing, on a permanent basis or for a period of not more than five years, of one or more of the company's branches which were used to commit the offences in question; f) Prohibition from taking part in public competitive bidding on a permanent basis or for a period of not more than five years; g) Prohibition, on a permanent basis or for a period of not more than five years, from participating in activities geared to obtaining assets from public savings; h) Confiscation of the item having served or been intended to commit the offence, or of the item constituting the proceeds of the offence; i) Publishing or disseminating the sentence pronounced, either in the press or via any other medium. **Paragraph.- Negligence on the part of the legal person.**

	Similarly, the legal person shall be considered civilly liable where a lack of supervision of the legal representative or employee has led to the commission of an illegal act as provided for in this law.
Article 13 – Sanctions and measures	- Each offence includes the corresponding sanction. -
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions	**Article 52.- Application of the Code of Criminal Procedure.** The rules on immediate verification and auxiliary resources set out in the Code of Criminal Procedure, Law No.76-02, apply to the obtaining and safeguarding of the data contained in an information system or its component parts, traffic, connection or access data or any other relevant information for investigating the offences covered by this law and for all the procedures set out in this chapter.
Article 15 – Conditions and safeguards	**Article 57.- Perverting the course of justice.** Attempts to hamper the investigations conducted by the competent authorities shall be punished with immediate dismissal, a prison sentence of between six months and five years and a fine of not less than ten times the minimum wage. Such attempts to pervert the course of justice include: a) Implementing or requesting measures for reasons other than that of the actual prosecution of one of the crimes or offences set out in this law; b) Trafficking in and marketing data obtained during the investigations; c) Disclosure of personal and commercial data on the defendant which are irrelevant to the investigations, as well as trafficking in or marketing such data.
Article 16 – Expedited preservation of stored computer data	**Article 53.- Safeguarding the data.** The competent authorities must take prompt action to safeguard the data contained in an information system or its component parts, or the system traffic data, especially where the latter are exposed to loss or modification.
Article 17 – Expedited preservation and partial disclosure of traffic data	**Article 56.- Service providers.** Without prejudice to the provisions of Article 47 b) of this law, service providers must store traffic, connection and access data and any other information which might be useful for investigations, for a minimum period of ninety (90) days. The Dominican Institute of Telecommunications (INDOTEL) will set out the regulations on procedure for obtaining and storing data and information on the part of service providers for a period of 6 months from publication of this law. These regulations should take account of the importance of preserving evidence, regardless of the number of service providers involved in the data transmission or communication.
Article 18 – Production order	**Article 54.- Powers of the Public Prosecutor's Office**. Subject to compliance with the formalities laid down in the Code of Criminal Procedure, the Public Prosecutor's Office, which may co-opt the services of one or more of the following: State investigating agencies such as the Investigation Department for High-Technology Crimes and Offences (DICAT) of the National Police Force, the

	Computer Crime Investigation Division (DIDI) of the National CID, experts, public or private institutions or other competent authorities, is empowered to: a) Order a natural or legal person to supply information stored in an information or system in any of its component parts;
Article 19 – Search and seizure of stored computer data	**Article 54.- Powers of the Public Prosecutor's Office**. b) Accede to or order access to such information system or to any of its component parts; e) Seize or distrain an information system or any of its component parts, in toto or in parte; j) Retrieve or record data from an information system or from any of its component parts by technological means;
Article 20 – Real-time collection of traffic data	**Article 54.- Powers of the Public Prosecutor's Office**. k) Invite the service provider to retrieve, extract or record data on a given user, as well as real-time traffic data, by technological means; l) Intercept telecommunications in real time, in accordance with the procedure set out in Article 192 of the Code of Criminal Procedure for the investigation of all the offences punishable under this law;
Article 21 – Interception of content data	**Article 54.- Powers of the Public Prosecutor's Office**. d) Order service providers, including Internet service providers, to supply information on any user data they may have in their possession or control;
Section 3 – Jurisdiction	
Article 22 – Jurisdiction	**Article 65.- Competent court.** Cases of high-technology crimes and offences are brought before the relevant ordinary courts or the Youth Court, depending on the type of case. Judges may order the presentation of an expert report on the merits of the case.
Chapter III – International co-operation	
Article 24 – Extradition	
Article 25 – General principles relating to mutual assistance	
Article 26 – Spontaneous information	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements	
Article 28 – Confidentiality and limitation on use	
Article 29 – Expedited	

preservation of stored computer data	
Article 30 – Expedited disclosure of preserved traffic data	
Article 31 – Mutual assistance regarding accessing of stored computer data	
Article 32 – Trans-border access to stored computer data with consent or where publicly available	
Article 33 – Mutual assistance in the real-time collection of traffic data	
Article 34 – Mutual assistance regarding the interception of content data	
Article 35 – 24/7 Network	
Article 42 – Reservations	

Appendix: Law 53-07

EL CONGRESO NACIONAL

En Nombre de la República

Ley No. 53-07, del 23 de abril de 2007, contra Crímenes y Delitos de Alta Tecnología.

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 no están previstos en la legislación penal dominicana, por lo que los autores de tales acciones no pueden ser sancionados sin la creación de una legislación previa, y en consecuencia, resulta necesaria su tipificación, y la adopción de mecanismos suficientes para su lucha efectiva, facilitando la cooperación entre el Estado y el sector privado para la detección, investigación y sanción a nivel nacional de estos nuevos tipos de delitos, y estableciendo disposiciones que permitan una cooperación internacional fiable y rápida;

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 han originado grandes retos de seguridad; y que en la actualidad, la Comisión Interamericana de Telecomunicaciones (CITEL), el Comité Interamericano contra el Terrorismo (CICTE) y la Reunión de Ministro, de Justicia o Procuradores Generales de las Américas (REMJA) están trabajando en la adopción de una estrategia hemisférica para la seguridad cibernética en la región, conforme a lo dispuesto por la Resolución AG/RES. 2004 (XXXIV-0/04) de la Asamblea General de la Organización de Estados Americanos (OEA) de fecha 8 de junio de 2004, para la Adopción de una Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética;

CONSIDERANDO: Que en la actual era del conocimiento, la información y los instrumentos electrónicos de canalización de la misma se han vuelto cada vez más importantes y trascendentes en los procesos de desarrollo, competitividad y cambios estructurales registrados en las vertientes económicas, políticas, sociales, culturales y empresariales del país.

VISTA: La Constitución de la República Dominicana;

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

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, del 20 de agosto de 1884, y sus modificaciones;

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

VISTO: El Código Procesal Penal de la República 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 Declaración Universal de Derechos Humanos de 1948 y la Convención Americana sobre Derechos Humanos, suscrita en San José de Costa Rica, el 22 de noviembre de 1969;

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

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

TÍTULO I

DISPOSICIONES GENERALES Y CONCEPTUALES

SECCIÓN I

OBJETO, ÁMBITO Y PRINCIPIOS

Artículo l.- Objeto de la Ley. La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información y comunicación y su contenido, así como la prevención 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 física o morales, en los términos previstos en esta ley. La integridad de los sistemas de información y sus componentes, la información o los datos, que se almacenan o transmiten a través de éstos, las transacciones y acuerdos comerciales o de cualquiera otra índole que se llevan a cabo por su medio y la confidencialidad de éstos, son todos bienes jurídicos protegidos.

Artículo 2.- Ámbito de Aplicación. Esta ley se aplicará en todo el territorio de la República Dominicana, a toda persona física o moral, nacional o extranjera, que cometa un hecho sancionado por sus disposiciones, en cualquiera de las siguientes circunstancias:

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

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

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

d) Cuando se caracterice cualquier tipo de complicidad desde el territorio dominicano.

Párrafo.- Aplicación General. La presente ley es de aplicación general a todas las personas físicas o morales, públicas o privadas, nacionales o internacionales.

Artículo 3.- Principios Generales. La presente ley tendrá como principios:

a) Principio de Territorialidad. Esta ley penal se aplicará a las infracciones cometidas en el territorio de la República Dominicana. Sinembargo, la infracción se reputará cometida en el territorio nacional desde que alguno de los crímenes o delitos previstos en la presente ley, se cometa fuera del territorio de la República en las condiciones expresadas en los literales b) y c) del Artículo 2, quedando el sujeto activo, en caso de que no haya sido juzgado mediante sentencia definitiva por el mismo hecho o evadido la persecución penal en tribunales extranjeros, a la disposición de la jurisdicción nacional;

b) 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. Al aplicar las penalidades impuestas por la presente ley, el juez competente deberá considerar la gravedad del hecho cometido y tomar en cuenta que las penas deben tener un efecto social y regenerador, no sólo para el individuo al que se le aplica sino también para la sociedad en su conjunto.

SECCIÓN II

DEFINICIONES

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 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.

TÍTULO II

NORMATIVA EFECTIVA A NIVEL NACIONAL

SECCIÓN I

DERECHO PENAL SUSTANTIVO

CAPÍTULO I

CRÍMENES Y DELITO CONTRA LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE DATOS Y SISTEMAS DE INFORMACIÓN

Artículo 5.- **Códigos de Acceso.** El hecho de divulgar, generar, copiar, grabar, capturar, utilizar, 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 ilícito a un sistema electrónico, informático, telemático o de telecomunicaciones, o a sus componentes, o falsificar cualquier tipo de dispositivo de acceso al mismo, se sancionará con la pena de uno a tres años de prisión y multa de veinte a cien veces el salario mínimo.

Párrafo.- 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 informático, electrónico o de telecomunicaciones, 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 uno a diez años de prisión y multa de dos a quinientas veces el salario mínimo.

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 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 7.- Acceso Ilícito para Servicios a Terceros. El hecho de utilizar un programa, equipo, material o dispositivo para obtener acceso a un sistema electrónico, informático, telemático o de telecomunicaciones, o a cualquiera de sus componentes, para ofrecer

servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, se sancionará con la pena de tres meses a un año de prisión y multa desde tres a quinientas veces el salario mínimo.

Párrafo.- Beneficio de Actividades de un Tercero. El hecho de aprovechar las actividades fraudulentas de un tercero descritas en este artículo, para recibir ilícitamente 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 la pena de tres a seis meses de prisión y multa desde dos a doscientas veces el salario mínimo.

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.

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 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 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 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.

CAPÍTULO II

DELITOS DE CONTENIDO

Artículo 12.- Atentado contra la Vida de la Persona. Se sancionará con las mismas penas del homicidio intencional o inintencional, el atentado contra la vida, o la provocación de la muerte de una persona cometido utilizando sistemas de carácter electrónico, informático, telemático o de telecomunicaciones, o sus componentes.

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.

Artículo 17.- Robo de Identidad. El hecho de una persona valerse de una identidad ajena a la suya, a través de medios electrónicos, informáticos, telemáticos o de telecomunicaciones, se sancionará con penas de tres meses a siete años de prisión y multa de dos a doscientas veces el salario mínimo.

Artículo 18.- De la Falsedad de Documentos y Firmas. Todo aquel que falsifique, desencripte, 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 tres años de prisión y multa de cincuenta a doscientas veces el salario mínimo.

Artículo 19.- Uso de Equipos para Invasión de Privacidad. El uso, sin causa legítima o autorización de la entidad legalmente competente, de sistemas electrónicos, informáticos, telemáticos, de telecomunicaciones, o dispositivos 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 dos años de prisión y multa de cinco a quinientas veces el salario mínimo.

Artículo 20.- Comercio Ilícito de Bienes y Servicios. La comercialización no autorizada o ilícita de bienes y servicios, a través del Internet o de cualquiera de los componentes de un sistema de información, se castigará con la pena de tres meses a cinco años de prisión y multa de cinco a quinientas veces el salario mínimo.

Párrafo.- El hecho de traficar ilícitamente humanos o migrantes, de cometer el delito tipificado como trata de personas o la venta de drogas o sustancias controladas, utilizando como soporte sistema electrónicos, informáticos, telemáticos o de telecomunicaciones, se castigará con las penas establecidas en las legislaciones especiales sobre estas materias.

Artículo 21.- Difamación. La difamación cometida a través de medios electrónicos, informáticos, telemáticos, de telecomunicaciones o audiovisuales, se sancionará con la pena de tres meses a un año de prisión y multa de cinco a quinientas veces el salario mínimo.

Artículo 22.- Injuria Pública. La injuria pública cometida a través de medios electrónicos, informáticos, telemáticos, de telecomunicaciones, o audiovisuales, se sancionará con la pena de tres meses a un año de prisión y multa de cinco a quinientas veces el salario mínino.

Artículo 23.- Atentado Sexual. El hecho de ejercer un atentado sexual contra un niño, niña, adolescente, incapacitado o enajenado mental, 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 desde cinco a doscientas veces el salario mínimo.

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.

CAPÍTULO III

DELITOS DE PROPIEDAD INTELECTUAL Y AFINES

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.

CAPÍTULO IV

DELITOS CONTRA LAS TELECOMUNICACIONES

Artículo 26.- Delitos de Telecomunicaciones. Incurren en penas de prisión de tres meses a diez años y multa desde cinco a doscientas veces el salario mínimo, los que cometan uno o varios de los siguientes hechos:

a) **Llamada de Retorno de Tipo Fraudulento:** La generación de tráfico internacional en sentido inverso al normal, con fines comerciales, mediante mecanismos y sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones. 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 Información Líneas Tipo 1-976:** 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, ya sea un desvío de servicios, desvío de facilidades contratadas, o cualquier otro tipo de desvío ilícito;

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.

CAPÍTULO V

CRÍMENES, DELITOS CONTRA LA NACIÓN

Y ACTOS DE TERRORISMO

Artículo 27.- Crímenes y Delitos contra la Nación. Los actos que se realicen a través de un sistema informático, electrónico, telemático o de telecomunicaciones, que atenten contra los intereses fundamentales y seguridad de la Nación, tales como el sabotaje, el espionaje o el suministro de informaciones, serán castigados con penas de quince a treinta años de reclusión y multa de trescientas a dos mil veces el salario mínimo.

Artículo 28.- Actos de Terrorismo. Todo aquel que con el uso de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones, ejerza actos de terrorismo, será castigado con pena de veinte a treinta años de reclusión y multa de trescientos a mil salarios mínimos, del sector público. Asimismo, se podrá ordenar la confiscación y destrucción del sistema de información o sus componentes, propiedad del sujeto pasivo utilizado para cometer el crimen.

SECCIÓN II

ORGANISMOS COMPETENTES Y REGLAS DE DERECHO PROCESAL

CAPÍTULO I

ORGANISMOS COMPETENTES

Artículo 29.- Dependencia del Ministerio Público. El Ministerio Público contará con una dependencia especializada en la investigación y persecución de los delitos y crímenes contenidos en la presente ley. El Departamento de Telecomunicaciones, Propiedad Intelectual y Comercio Electrónico de la Procuraduría General de la República o cualquier departamento creado a tales fines dentro del organigrama de la Procuraduría General de la República, coordinará el funcionamiento de dicha dependencia.

Artículo 30.- **Creación y Composición de la Comisión Interinstitucional contra Crímenes y Delitos de Alta Tecnología (CICDAT).** Se crea la Comisión Interinstitucional

contra Crímenes y Delitos de Alta Tecnología, la cual estará compuesta por un representante de las siguientes entidades:

a) La Procuraduría General de la República;

b) La Secretaría de Estado de las Fuerzas Armadas;

c) La Secretaría de Estado de Interior y Policía;

d) La Policía Nacional;

e) La Dirección Nacional de Control de Drogas (DNCD);

f) El Departamento Nacional de Investigaciones (DNI);

g) El Instituto Dominicano de las Telecomunicaciones (INDOTEL);

h) La Superintendencia de Bancos de la República Dominicana;

i) El Consejo Nacional para la Niñez y la Adolescencia (CONANI); y,

j) El Instituto Tecnológico de las Américas (ITLA).

Artículo 31.- Presidencia de la Comisión. 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 32.- Funciones de la Comisión. La Comisión tendrá como funciones principales:

a) La coordinación y cooperación 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) La coordinación y cooperación con gobiernos e instituciones nacionales y extranjeras para prevenir y reducir la comisión de actos ilícitos de alta tecnología en la República Dominicana y el resto del mundo, en coordinación con la entidad nacional competente;

c) Definir las políticas, establecer las directrices y elaborar propuestas de estrategias 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; y,

e) Coordinar la representación dominicana a través de la entidad nacional competente ante los diferentes organismos internacionales en el área de crímenes y delitos de alta tecnología.

Artículo 33.- 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 más de la mitad de sus miembros.

Artículo 34.- Secretaría General. Actuará como Secretario General de la Comisión, el representante del Instituto Tecnológico de las Américas (ITLA), quien dentro de sus funciones convocará y fijará el orden del día de las reuniones de acuerdo con el presidente; redactará el acta 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 35.- Capacitación. La Comisión coordinará la capacitación de las autoridades competentes mediante un acuerdo con el Instituto Tecnológico de las Américas (ITLA) o cualquier otra entidad que se considere necesaria.

Artículo 36.- Creación del Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT). Se crea el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT), como entidad subordinada a la Dirección Central de Investigaciones Criminales de la Policía Nacional.

Artículo 37.- Investigación y Sometimiento. Las investigaciones de los casos y el sometimiento a la justicia de las personas involucradas serán apoyadas por el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT), el cual tendrá oficiales de enlace de la División de Investigación de Delitos Informáticos (DIDI) del Departamento Nacional de Investigaciones, de la Secretaría de Estado de las Fuerzas Armadas y de la Dirección Nacional de Control de Drogas.

Artículo 38.- Funciones del DICAT. El DICAT tendrá como principales funciones:

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

b) Investigar todas las denuncias de crímenes o delitos considerados de alta tecnología;

c) Responder con capacidad investigativa a todas las amenazas y ataques a la infraestructura crítica nacional;

d) Desarrollar análisis estratégicos de amenazas informáticas; y,

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

Artículo 39.- Personal del DICAT. El personal del DICAT, incluyendo a su comandante, deberá contar con certificaciones de la industria que avalen su pericia en áreas de la informática, la investigación y áreas afines.

Artículo 40.- **Requisitos del Comandante del DICAT.** El comandante de este departamento deberá:

a) Ser Oficial Superior de la Policía Nacional;

b) Ser ingeniero en sistemas o profesional de otra rama que posea certificaciones en áreas especializadas de la informática;

c) Tener mínimo 10 años de experiencia profesional;

d) Tener mínimo 12 años de carrera policial; y,

e) Tener especializaciones en las diferentes áreas del Delito Informático e Investigaciones Criminales.

Párrafo.- Inamovilidad del Comandante del DICAT. El comandante del DICAT deberá permanecer en el cargo un mínimo de 2 años, salvo casos de mal desempeño o incompetencia debidamente comprobada, en cuyo caso su destitución deberá ser aprobada por el Jefe de la Policía Nacional.

Artículo 41.- Relaciones Interinstitucionales del DICAT. El DICAT deberá:

a) Trabajar en coordinación con la Comisión Interinstitucional contra Crímenes y Delitos de Alta Tecnología creada por esta ley;

b) Ser el punto de contacto oficial de República Dominicana en la Red Internacional 24/7 de Asistencia en Crímenes que Involucran Alta Tecnología perteneciente al Subgrupo de Crímenes de Alta Tecnología del Grupo de Expertos en Crimen Organizado Transnacional G8; y,

c) Trabajar en coordinación con los demás organismos nacionales e internacionales de investigación de crímenes y delitos de alta tecnología.

Artículo 42.- Presupuesto. El presupuesto del DICAT estará conformado por:

a) La proporción de la asignación presupuestaria que cada año deberá otorgar la Policía Nacional a la Dirección Central de Investigaciones Criminales;

b) Las asignaciones presupuestarias que, en su caso, le asigne el Gobierno Central; y

c) Los fondos que pueda obtener por cualquier otro concepto legítimo.

Artículo 43.- Creación de la División de Investigaciones de Delitos Informáticos (DIDI). Se crea la División de Investigaciones de Delitos Informáticos (DIDI) como dependencia del Departamento Nacional de Investigaciones (DNI).

Artículo 44.- Investigación y Sometimiento. La División de Investigación de Delitos Informáticos (DIDI) trabajará los casos relacionados a: crímenes contra la humanidad; crímenes y delitos contra la Nación, el Estado y la paz pública; amenazas o ataques contra el Estado dominicano, la seguridad nacional o que involucren la figura del presidente de la República, secretarios de Estado o funcionarios electos. Tendrá oficiales de enlace del Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional, de la Secretaría de Estado de las Fuerzas Armadas y de la Dirección Nacional de Control de Drogas.

Artículo 45.- Funciones del DIDI. 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 de crímenes o delitos considerados de alta tecnología dentro del ámbito del Artículo 46;

c) Responder con capacidad investigativa a todas las amenazas y ataques a la infraestructura crítica nacional;

d) Desarrollar análisis estratégicos de amenazas informáticas; y,

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

Artículo 46.- Personal de la División de Investigación de Delitos Informáticos (DIDI). El personal de la División de Investigación de Delitos Informáticos (DIDI), incluyendo a su encargado, deberá contar con certificaciones de la industria que avalen su pericia en áreas de la informática, la investigación y áreas afines.

Artículo 47.- Requisitos del Encargado de la División de Investigación de Delitos Informáticos (DIDI). El encargado de esta división deberá:

a) Ser Oficial Superior de las Fuerzas Armadas o la Policía Nacional;

b) Ser ingeniero en sistemas o profesional de otra rama que posea certificaciones en áreas especializadas de la informática;

c) Tener mínimo cinco años de experiencia profesional;

d) Tener especializaciones en las diferentes áreas del delito informático e investigaciones criminales.

Artículo 48.- Presupuesto. El presupuesto de la División de Investigación de Delitos Informáticos (DIDI) estará conformado por:

a) La proporción de la asignación presupuestaria que cada año deberá otorgarle el Departamento Nacional de Investigaciones;

b) Las asignaciones presupuestarías que, en su caso, le asigne el Gobierno Central; y

c) Los fondos que pueda obtener por cualquier otro concepto legítimo.

Artículo 49.- Relaciones Interinstitucionales de la DIDI. La División de Investigación de Delitos Informáticos (DIDI) deberá:

a) Trabajar en coordinación con la Comisión Interinstitucional contra Crímenes y Delitos de Alta Tecnología creada por esta ley;

b) Trabajar en coordinación con los demás organismos nacionales e internacionales de investigación de crímenes y delitos de alta tecnología.

Artículo 50.- Documentación y Tramitación de Investigaciones. Tanto la DIDI como el DICAT contarán con representantes especializados del Ministerio Público, quienes documentarán y tramitarán las investigaciones de estos departamentos.

Artículo 51.- Reglamentación. La División de Investigación de Delitos Informáticos (DIDI) y el Departamento de Investigación contra Crímenes y Delitos de Alta Tecnología (DICAT), en coordinación con sus organismos superiores, crearán administrativamente la reglamentación correspondiente a su estructura organizacional, la cual podrá contemplar secciones de enlaces, de inteligencia, investigaciones, operaciones, recuperación de evidencia, personal, planificación y capacitación.

CAPÍTULO II

MEDIDAS CAUTELARES Y PROCESALES

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.

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.

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;

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;

c) Acceder u ordenar el acceso a dicho sistema de información o a cualquiera de sus componentes;

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;

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 accesado 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 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,

m) 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 55.- Mejores Prácticas de Recopilación de Evidencia. El Ministerio Público, el Departamento de Investigación de Delitos y Crímenes de Alta Tecnología (DICAT) de la Policía Nacional, la División de Investigación de Delitos Informáticos (DIDI) 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 y conservación de evidencia.

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.

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 58.- Responsabilidad del Custodio. A quien se le haya confiado la preservación del sistema de información o de cualquiera de sus componentes, así como de su contenido, conservará la confidencialidad e integridad de los mismos, impidiendo que terceros extraños, fuera de las autoridades competentes, tengan acceso y conocimiento de ellos. Asimismo, la persona encargada de la custodia no podrá hacer uso del objeto en custodia para fines distintos a los concernientes al proceso investigativo.

Artículo 59.- Confidencialidad del Proceso Investigativo. Quien colabore con el proceso de investigación, en la recolección, interceptación e intervención de datos de un sistema de información o de sus componentes, o cualquiera 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.

Párrafo.- La violación a los Artículos 51 y 52 será castigada con las penas establecidas para la revelación de secretos en el Código Penal de la República Dominicana.

TÍTULO III

DISPOSICIONES FINALES

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;

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 61.- Acciones Administrativas. Nada de lo establecido en la presente ley, impide recurrir a las acciones administrativas que puedan resultar de leyes y reglamentos especiales aplicables.

Artículo 62.- Pago de Indemnizaciones. Sin perjuicio de las sanciones penales y de las sanciones administrativas que puedan resultar de leyes y reglamentos especiales, las personas

físicas o morales podrán ser condenadas al pago de indemnizaciones civiles a favor del sujeto pasivo.

Artículo 63.- Legislaciones Complementarias. Los términos no contemplados en esta ley se regirán por:

a) El Código Procesal Penal de la República Dominicana, Ley No. 76-02, del 19 de julio del 2002;

b) El Código Penal Dominicano;

c) La Ley No.126-02, del 4 de septiembre del 2002, de Comercio Electrónico, Documentos, y Firmas Digitales, y sus reglamentos;

d) La Ley General de Telecomunicaciones No.153-98, del 27 de mayo de 1998, y sus reglamentos;

e) Las leyes No.65-00 y No.20-00, del 21 de agosto del 2000 y del 8 de mayo del 2000, sobre Derecho de Autor y Propiedad Industrial, respectivamente, para cada una de sus materias;

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

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

h) Las disposiciones del derecho común y las disposiciones legales relacionadas que sean aplicables.

Artículo 64.- Acción Pública. Las infracciones previstas en el presente Capítulo se consideran de acción pública a instancia privada conforme a lo previsto en el Código Procesal Penal. Sinembargo, el Ministerio Público podrá ejercer de oficio la acción pública en los casos de pornografía infantil, que se atente contra el orden público, los intereses de la nación, los derechos de un incapaz que no tenga representación o cuando el crimen o delito haya sido cometido por uno de los padres, el tutor o el representante legal del sujeto pasivo.

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.

Artículo 66.- Entrada en Vigencia. La presente ley entrará en vigencia desde la fecha de su publicación.

Artículo 67.- Derogaciones. Con la promulgación de la presente ley, queda derogada cualquier norma o disposición que le sea contraria a la misma en esta materia.

DADA en la Sala de Sesiones de la Cámara de Diputados, Palacio del Congreso Nacional, en Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los diecisiete (17) días del mes de enero del año dos mil siete; años 163 de la Independencia y 144 de la Restauración.

Lucía Medina Sánchez,

Vicepresidenta en Funciones;

María Cleofia Sánchez Lora, Teodoro Ursino Reyes,

Secretaria Secretario

DADA en la Sala de Sesiones del Senado, Palacio del Congreso Nacional, en Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los diez (10) días del mes de abril del año dos mil siete (2007); años 164 de la Independencia y 144 de la Restauración.

Reinaldo Pared Pérez,

Presidente

Amarilis Santana Cedano, Diego Aquino Acosta Rojas,

Secretaria Secretario

LEONEL FERNANDEZ

Presidente de la República Dominicana

En ejercicio de las atribuciones que me confiere el Artículo 55 de la Constitución de la República.

PROMULGO la presente Ley y mando que sea publicada en la Gaceta Oficial, para su conocimiento y cumplimiento.

DADA en Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los veintitrés (23) días del mes de abril del año dos mil siete (2007); años 163 de la Independencia y 144 de la Restauración.

LEONEL FERNANDEZ