

Project on Cybercrime

www.coe.int/cybercrime



COUNCIL OF EUROPE CONSEIL DE L'EUROPE

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? <i>We have taken into account provisions of the Convention in our recent Law 53-07, against cybercrimes.</i> What specific obstacles (legislative or other) prevent ratification/accession? <i>It is necessary to obtain congressional approval.</i>
Provisions of the Convention	Corresponding provisions/solutions in national legislation <i>(pls quote or summarise briefly; pls attach relevant extracts as an appendix)</i>
<i>Chapter I – Use of terms</i>	
Article 1 – “Computer system”, “computer data”, “service provider”, “traffic data”	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. 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.
<i>Chapter II – Measures to be taken at the national level</i> <i>Section 1 – Substantive criminal law</i>	
Article 2 – Illegal access	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.
Article 3 – Illegal interception	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.
Article 4 – Data interference	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.
Article 5 – System interference	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.
Article 6 – Misuse of devices	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.
Article 7 – Computer-related forgery	Artículo 18.- De la Falsedad de Documentos y Firmas. Todo aquel que falsifique, descripte, 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.
Article 8 – Computer-related fraud	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

	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
Article 9 – Offences related to child pornography	<p>Artículo 24.- Pornografía Infantil. La producción, difusión, venta y cualquier tipo de comercialización de imágenes o 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.</p> <p>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.</p>
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights	<p>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.</p>
Article 11 – Attempt and aiding or abetting	- It is not contemplated in Law 53-07.-

<p>Article 12 – Corporate liability</p>	<p>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:</p> <ul style="list-style-type: none"> 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 inculcados; 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. <p>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.</p>
<p>Article 13 – Sanctions and measures</p>	<p>- Each offence includes the corresponding sanction. -</p>
<p><i>Section 2 – Procedural law</i></p>	
<p>Article 14 – Scope of procedural provisions</p>	<p>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</p>

	información de utilidad, en la investigación de los delitos penalizados en la presente ley y para todos los procedimientos establecidos en este capítulo.
Article 15 – Conditions and safeguards	<p>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:</p> <ul style="list-style-type: none"> 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.
Article 16 – Expedited preservation of stored computer data	<p>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.</p>
Article 17 – Expedited preservation and partial disclosure of traffic data	<p>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.</p>
Article 18 – Production order	<p>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:</p> <ul style="list-style-type: none"> 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;
Article 19 – Search and seizure of stored computer data	<p>Artículo 54.- Facultades del Ministerio Público.</p> <ul style="list-style-type: none"> b) Acceder u ordenar el acceso a dicho sistema de información o a cualquiera de sus componentes; 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;

Article 20 – Real-time collection of traffic data	Artículo 54.- Facultades del Ministerio Público. 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;
Article 21 – Interception of content data	Artículo 54.- Facultades del Ministerio Público. 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;
<i>Section 3 – Jurisdiction</i>	
Article 22 – Jurisdiction	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.
<i>Chapter III – International co-operation</i>	
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	