

### Table of contents

Version 21 June 2022

[reference to the provisions of the Budapest Convention]

#### Chapter I – Use of terms

Article 1 – “Computer system”, “computer data”, “service provider”, “traffic data”

#### Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Article 2 – Illegal access

Article 3 – Illegal interception

Article 4 – Data interference

Article 5 – System interference

Article 6 – Misuse of devices

Article 7 – Computer-related forgery

Article 8 – Computer-related fraud

Article 9 – Offences related to child pornography

Article 10 – Offences related to infringements of copyright and related rights

Article 11 – Attempt and aiding or abetting

Article 12 – Corporate liability

Article 13 – Sanctions and measures

Section 2 – Procedural law

Article 14 – Scope of procedural provisions

Article 15 – Conditions and safeguards

Article 16 – Expedited preservation of stored computer data

Article 17 – Expedited preservation and partial disclosure of traffic data

Article 18 – Production order

Article 19 – Search and seizure of stored computer data

Article 20 – Real-time collection of traffic data

Article 21 – Interception of content data

Section 3 – Jurisdiction

Article 22 – Jurisdiction

#### 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

*This profile has been prepared by the Cybercrime Programme Office (C-PROC) of the Council of Europe in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Budapest Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the State covered or of the Council of Europe.*

<b>State:</b>	
<b>Signature of the Budapest Convention:</b>	N/A
<b>Ratification/accession:</b>	N/A

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<b>Chapter I – Use of terms</b>	
<p><b>Article 1 – “Computer system”, “computer data”, “service provider”, “traffic data”:</b>                      For the purposes of this Convention:                      a “computer system” means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;                      b “computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;                      c “service provider” means:                      i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and                      ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;                      d “traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service</p>	<p><b><u>CÓDIGO ORGÁNICO INTEGRAL PENAL</u></b>  <b>TÍTULO IV INFRACCIONES EN PARTICULAR</b>  <b>CAPÍTULO TERCERO DELITOS CONTRA LOS DERECHOS DEL BUEN VIVIR</b>  <b>SECCIÓN TERCERA Delitos contra la seguridad de los activos de los sistemas de información y comunicación</b></p> <p><b>Art. 234.4.- Definiciones.-</b>                      Para los efectos del presente Código, se considera:                      a. <b>Contenido digital-</b> El contenido digital es todo dato informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico o canal de comunicación que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí.                      b. <b>Datos de tráfico.-</b> Contenido digital relativo a una comunicación efectuada por medio de un sistema informático o canal de comunicación, generados por este sistema como elemento de una cadena de comunicación, indicando su origen, su destino, su trayecto, la hora, la fecha, el tamaño, la duración o el tipo de servicio subyacente.                      c. <b>Proveedor de servicios.-</b> Cualquier entidad, pública o privada, nacional o internacional, que proporciona a los usuarios de sus servicios la capacidad de comunicarse a través de un sistema informático, o de cualquiera de las tecnologías de la información y comunicación, así como cualquier otra entidad que procese o almacene contenido digital en nombre y por cuenta de aquella entidad proveedora o de sus usuarios.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>d. <b>Sistema informático.</b>- Cualquier dispositivo o conjunto de dispositivos interconectados o asociados, en que uno o varios de ellos desarrolla, ejecutando un programa, el tratamiento automatizado de contenido digital.</p>
<p><b>Chapter II – Measures to be taken at the national level</b></p>	
<p><b>Section 1 – Substantive criminal law</b></p>	
<p><b>Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems</b></p>	
<p><b>Article 2 – Illegal access</b>                      Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.</p>	<p><b><u>CÓDIGO ORGÁNICO INTEGRAL PENAL</u></b>  <b>TÍTULO IV INFRACCIONES EN PARTICULAR</b>  <b>CAPÍTULO TERCERO DELITOS CONTRA LOS DERECHOS DEL BUEN VIVIR</b>  <b>SECCIÓN TERCERA Delitos contra la seguridad de los activos de los sistemas de información y comunicación</b></p> <p><b>Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.</b></p> <p>1. La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho sobre dicho sistema, será sancionada con la pena privativa de la libertad de tres a cinco años.</p> <p>2. Si la persona que accede al sistema lo hace para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar el tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a las o los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.</p>
<p><b>Article 3 – Illegal interception</b>                      Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.</p>	<p><b><u>CÓDIGO ORGÁNICO INTEGRAL PENAL</u></b>  <b>TÍTULO IV INFRACCIONES EN PARTICULAR</b>  <b>CAPÍTULO TERCERO DELITOS CONTRA LOS DERECHOS DEL BUEN VIVIR</b>  <b>SECCIÓN TERCERA Delitos contra la seguridad de los activos de los sistemas de información y comunicación</b></p> <p><b>Artículo 230.- Interceptación ilegal de datos.-</b> Será sancionada con pena privativa de libertad de tres a cinco años:</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma, contenido digital en su origen, destino o en el interior de un sistema informático o dispositivo electrónico, una señal o una transmisión de datos o señales. 2. La persona que ilegítimamente diseñe, desarrolle, ejecute, produzca, programe o envíe contenido digital, códigos de accesos o contraseñas, certificados de seguridad o páginas electrónicas, enlaces o ventanaemergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente al que quiere acceder.</p> <p>3. La persona que posea, venda, distribuya o, de cualquier otra forma, disemine o introduzca en uno o más sistemas informáticos, dispositivos electrónicos, programas u otros contenidos digitales destinados a causar lo descrito en el número anterior.</p> <p>4. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.</p> <p>5. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos, o programas o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior</p>
<p><b>Article 4 – Data interference</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.</p> <p>2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.</p>	<p><b><u>CÓDIGO ORGÁNICO INTEGRAL PENAL</u></b>  <b>TÍTULO IV INFRACCIONES EN PARTICULAR</b>  <b>CAPÍTULO TERCERO DELITOS CONTRA LOS DERECHOS DEL BUEN VIVIR</b>  <b>SECCIÓN TERCERA Delitos contra la seguridad de los activos de los sistemas de información y comunicación</b></p> <p><b>Artículo 232.- Ataque a la integridad de sistemas informáticos.-</b> La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento o comportamiento no deseado, o suprima total o parcialmente contenido digital, sistemas informáticos, sistemas de tecnologías de la</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>información y comunicación, dispositivos electrónicos o infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general, con el propósito de obstaculizar de forma grave deliberada e ilegítima el funcionamiento de un sistema informático, será sancionada con pena privativa de libertad de tres a cinco años.</p> <p>Con igual pena será sancionada la persona que diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos, programas o sistemas informáticos maliciosos o destinados a causar los efectos señalados en el primer inciso de este artículo.</p> <p>Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.</p>
<p><b>Article 5 – System interference</b>                      Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data</p>	<p><b><u>CÓDIGO ORGÁNICO INTEGRAL PENAL</u></b>  <b>TÍTULO IV INFRACCIONES EN PARTICULAR</b>  <b>CAPÍTULO TERCERO DELITOS CONTRA LOS DERECHOS DEL BUEN VIVIR</b>  <b>SECCIÓN TERCERA Delitos contra la seguridad de los activos de los sistemas de información y comunicación</b></p> <p><b>Artículo 232.- Ataque a la integridad de sistemas informáticos.-</b> La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento o comportamiento no deseado, o suprima total o parcialmente contenido digital, sistemas informáticos, sistemas de tecnologías de la información y comunicación, dispositivos electrónicos o infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general, con el propósito de obstaculizar de forma grave deliberada e ilegítima el funcionamiento de un sistema informático, será sancionada con pena privativa de libertad de tres a cinco años.</p> <p>Con igual pena será sancionada la persona que diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos, programas o sistemas informáticos maliciosos o destinados a causar los efectos señalados en el primer inciso de este artículo.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.</p>
<p><b>Article 6 – Misuse of devices</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:</p> <p>a the production, sale, procurement for use, import, distribution or otherwise making available of:</p> <p>i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;</p> <p>ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and</p> <p>b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.</p> <p>2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.</p> <p>3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.</p>	<p><b><u>CÓDIGO ORGÁNICO INTEGRAL PENAL</u></b></p> <p><b>TÍTULO IV INFRACCIONES EN PARTICULAR</b></p> <p><b>CAPÍTULO TERCERO DELITOS CONTRA LOS DERECHOS DEL BUEN VIVIR</b></p> <p><b>SECCIÓN TERCERA Delitos contra la seguridad de los activos de los sistemas de información y comunicación</b></p> <p><b>Artículo 230.- Interceptación ilegal de datos.-</b> Será sancionada con pena privativa de libertad de tres a cinco años:</p> <ol style="list-style-type: none"> <li>1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma, contenido digital en su origen, destino o en el interior de un sistema informático o dispositivo electrónico, una señal o una transmisión de datos o señales.</li> <li>2. La persona que ilegítimamente diseñe, desarrolle, ejecute, produzca, programe o envíe contenido digital, códigos de accesos o contraseñas, certificados de seguridad o páginas electrónicas, enlaces o ventanaemergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente al que quiere acceder.</li> <li>3. La persona que posea, venda, distribuya o, de cualquier otra forma, disemine o introduzca en uno o más sistemas informáticos, dispositivos electrónicos, programas u otros contenidos digitales destinados a causar lo descrito en el número anterior.</li> <li>4. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.</li> </ol>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>5. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos, o programas o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior</p>
<b>Title 2 – Computer-related offences</b>	
<p><b>Article 7 – Computer-related forgery</b>                      Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.</p>	<p><b><u>CÓDIGO ORGÁNICO INTEGRAL PENAL</u></b>  <b>TÍTULO IV INFRACCIONES EN PARTICULAR</b>  <b>CAPÍTULO TERCERO DELITOS CONTRA LOS DERECHOS DEL BUEN VIVIR</b>  <b>SECCIÓN TERCERA Delitos contra la seguridad de los activos de los sistemas de información y comunicación</b></p> <p><b>Artículo 234.1.- Falsificación informática:</b> 1. La persona que, con intención de provocar un engaño en las relaciones jurídicas, introducir, modificar, eliminar o suprimir contenido digital, o interferir de cualquier otra forma en el tratamiento informático de datos, produzca datos o documentos no genuinos, será sancionada con pena privativa de libertad de tres a cinco años.</p> <p>2. Quien, actuando con intención de causar un perjuicio a otro o de obtener un beneficio ilegítimo para sí o para un tercero, use un documento producido a partir de contenido digital que sea objeto de los actos referidos en el número 1, será sancionado con la misma pena.</p>
<p><b>Article 8 – Computer-related fraud</b>                      Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:</p> <ul style="list-style-type: none"> <li>a any input, alteration, deletion or suppression of computer data;</li> <li>b any interference with the functioning of a computer system,</li> </ul> <p>with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.</p>	<p><b><u>CÓDIGO ORGÁNICO INTEGRAL PENAL</u></b>  <b>TÍTULO IV INFRACCIONES EN PARTICULAR</b>  <b>CAPÍTULO TERCERO DELITOS CONTRA LOS DERECHOS DEL BUEN VIVIR</b>  <b>SECCIÓN TERCERA Delitos contra la seguridad de los activos de los sistemas de información y comunicación</b></p> <p><b>Art. 231.- Transferencia electrónica de activo patrimonial.-</b> La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.</p>
<p><b>Title 3 – Content-related offences</b></p>	
<p><b>Article 9 – Offences related to child pornography</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:</p> <ul style="list-style-type: none"> <li>a producing child pornography for the purpose of its distribution through a computer system;</li> <li>b offering or making available child pornography through a computer system;</li> <li>c distributing or transmitting child pornography through a computer system;</li> <li>d procuring child pornography through a computer system for oneself or for another person;</li> <li>e possessing child pornography in a computer system or on a computer-data storage medium.</li> </ul> <p>2 For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:</p> <ul style="list-style-type: none"> <li>a a minor engaged in sexually explicit conduct;</li> <li>b a person appearing to be a minor engaged in sexually explicit conduct;</li> <li>c realistic images representing a minor engaged in sexually explicit conduct</li> </ul>	<p><b><u>CÓDIGO ORGÁNICO INTEGRAL PENAL</u></b>  <b>TÍTULO IV INFRACCIONES EN PARTICULAR</b>  <b>CAPÍTULO PRIMERO GRAVES VIOLACIONES A LOS DERECHOS HUMANOS Y DELITOS CONTRA EL DERECHO INTERNACIONAL HUMANITARIO</b>  <b>SECCIÓN TERCERA Diversas formas de explotación</b></p> <p><b>Artículo 103.- Pornografía con utilización de niñas, niños o adolescentes.-</b>          La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual, aunque el material tenga su origen en el extranjero o sea desconocido, será sancionada con pena privativa de libertad de trece a dieciséis años.</p> <p>Si la víctima, además, sufre algún tipo de discapacidad o enfermedad grave o incurable, se sancionará con pena privativa de libertad de dieciséis a diecinueve años.</p> <p>Cuando la persona infractora sea el padre, la madre, pariente hasta el cuarto grado de consanguinidad o segundo de afinidad, tutor, representante legal, curador o pertenezca al entorno íntimo de la familia; ministro de culto, profesor,</p>



BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>3 For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.</p> <p>4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.</p>	<p>maestro, o persona que por su profesión o actividad haya abusado de la víctima, será sancionada con pena privativa de libertad de veintidós a veintiséis años.</p> <p><b>Artículo 104.- Comercialización de pornografía con utilización de niñas, niños o adolescentes.-</b> La persona que publicite, compre, posea, porte, transmita, descargue, almacene, importe, exporte o venda, por cualquier medio, para uso personal o para intercambio pornografía de niños, niñas y adolescentes, será sancionada con pena privativa de libertad de diez a trece años.</p> <p><b>CAPÍTULO SEGUNDO DELITOS CONTRA LOS DERECHOS DE LIBERTAD SECCIÓN CUARTA Delitos contra la integridad sexual y reproductiva</b></p> <p><b>Artículo 173.- Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos.-</b> La persona que a través de un medio electrónico o telemático proponga concertar un encuentro con una persona menor de dieciocho años, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o erótica, será sancionada con pena privativa de libertad de uno a tres años.</p> <p>Cuando el acercamiento se obtenga mediante coacción o intimidación, será sancionada con pena privativa de libertad de tres a cinco años.</p> <p>La persona que suplantando la identidad de un tercero o mediante el uso de una identidad falsa por medios electrónicos o telemáticos, establezca comunicaciones de contenido sexual o erótico con una persona menor de dieciocho años o con discapacidad, será sancionada con pena privativa de libertad de tres a cinco años.</p> <p><b>Artículo 174.- Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos.-</b> La persona, que utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, fotoblogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años de edad, será sancionada con pena privativa de libertad de siete a diez años.</p>
<b>Title 4 – Offences related to infringements of copyright and related rights</b>	
<b>Article 10 – Offences related to infringements of copyright and related rights</b>	<b><u><a href="#">LEY DE PROPIEDAD INTELECTUAL (1998)</a></u> <b>LIBRO I</b></b>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.</p> <p>3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party’s international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.</p>	<p><b>TITULO I DE LOS DERECHOS DE AUTOR Y DERECHOS CONEXOS</b>  <b>SECCION II OBJETO DEL DERECHO DE AUTOR</b>  <b>Art. 8.-</b> La protección del derecho de autor recae sobre todas las obras del ingenio, en el ámbito literario o artístico, cualquiera que sea su género, forma de expresión, mérito o finalidad. Los derechos reconocidos por el presente Título son independientes de la propiedad del objeto material en el cual está incorporada la obra y su goce o ejercicio no están supeditados al requisito del registro o al cumplimiento de cualquier otra formalidad.</p> <p>Las obras protegidas comprenden, entre otras, las siguientes:</p> <ul style="list-style-type: none"> <li>a) Libros, folletos, impresos, epistolarios, artículos, novelas, cuentos, poemas, crónicas, críticas, ensayos, misivas, guiones para teatro, cinematografía, televisión, conferencias, discursos, lecciones, sermones, alegatos en derecho, memorias y otras obras de similar naturaleza, expresadas en cualquier forma;</li> <li>b) Colecciones de obras, tales como antologías o compilaciones y bases de datos de toda clase, que por la selección o disposición de las materias constituyan creaciones intelectuales, sin perjuicio de los derechos de autor que subsistan sobre los materiales o datos;</li> <li>c) Obras dramáticas y dramático musicales, las coreografías, las pantomimas y, en general las obras teatrales;</li> <li>d) Composiciones musicales con o sin letra;</li> <li>e) Obras cinematográficas y cualesquiera otras obras audiovisuales;</li> <li>f) Las esculturas y las obras de pintura, dibujo, grabado, litografía y las historietas gráficas, tebeos, comics, así como sus ensayos o bocetos y las demás obras plásticas;</li> <li>g) Proyectos, planos, maquetas y diseños de obras arquitectónicas y de ingeniería;</li> <li>h) Ilustraciones, gráficos, mapas y diseños relativos a la geografía, la topografía, y en general a la ciencia;</li> <li>i) Obras fotográficas y las expresadas por procedimientos análogos a la fotografía;</li> <li>j) Obras de arte aplicada, aunque su valor artístico no pueda ser disociado del carácter industrial de los objetos a los cuales estén incorporadas;</li> <li>k) Programas de ordenador; y,</li> <li>l) Adaptaciones, traducciones, arreglos, revisiones, actualizaciones y anotaciones; compendios, resúmenes y extractos; y, otras</li> </ul>

<b>BUDAPEST CONVENTION</b>	<b>DOMESTIC LEGISLATION</b>
	<p>transformaciones de una obra, realizadas con expresa autorización de los autores de las obras originales, y sin perjuicio de sus derechos.</p> <p><b>SECCION IV CONTENIDO DEL DERECHO DE AUTOR</b></p> <p><b>Art. 24.-</b> El derecho de importación confiere al titular de los derechos de autor la facultad de prohibir la introducción en el territorio ecuatoriano, incluyendo la transmisión analógica y digital, del original o copias de obras protegidas, sin perjuicio de obtener igual prohibición respecto de las copias ilícitas. Este derecho podrá ejercerse tanto para suspender el ingreso del original y copias en fronteras, como para obtener el retiro o suspender la circulación de los ejemplares que ya hubieren ingresado. Este derecho no afectará los ejemplares que formen parte del equipaje personal.</p> <p><b>SECCION V DISPOSICIONES ESPECIALES SOBRE CIERTAS OBRAS</b></p> <p><b>Art. 28.-</b> Los programas de ordenador se consideran obras literarias y se protegen como tales. Dicha protección se otorga independientemente de que hayan sido incorporados en un ordenador y cualquiera sea la forma en que estén expresados, ya sea en forma legible por el hombre (código fuente) o en forma legible por máquina (código objeto), ya sean programas operativos y programas aplicativos, incluyendo diagramas de flujo, planos, manuales de uso, y en general, aquellos elementos que conformen la estructura, secuencia y organización del programa.</p> <p><b>LIBRO IV DE LA COMPETENCIA DESLEAL</b></p> <p><b>TITULO I DE LA PROTECCION Y OBSERVANCIA DE LOS DERECHOS DE PROPIEDAD INTELECTUAL</b></p> <p><b>CAPITULO I PRINCIPIOS GENERALES</b></p> <p><b>Art. 292.-</b> Si la violación de los derechos se realiza a través de redes de comunicación digital, tendrá responsabilidad solidaria el operador o cualquier otra persona natural o jurídica que tenga el control de un sistema informático interconectado a dicha red, a través del cual se permita, induzca o facilite la comunicación, reproducción, transmisión o cualquier otro acto violatorio de los derechos previstos en ésta Ley, siempre que tenga conocimiento o haya sido advertido de la posible infracción, o no haya podido ignorarla sin negligencia grave de su parte.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>Se entenderá que ha sido advertido de la posibilidad de la infracción cuando se le ha dado noticia debidamente fundamentada sobre ella.</p> <p>Los operadores u otras personas naturales o jurídicas referidas en esta norma, estarán exentos de responsabilidad por los actos y medidas técnicas que adopten a fin de evitar que la infracción se produzca o continúe.</p> <p><b>CAPITULO II DE LOS PROCESOS DE PROPIEDAD INTELECTUAL SECCION I DE LOS PROCESOS DE CONOCIMIENTO</b></p> <p><b>Art. 296.-</b> La competencia en materia de propiedad intelectual se fija de conformidad con las reglas establecidas en los artículos 27, 28, 29 y 30 del Código de Procedimiento Civil y en el presente artículo.</p> <p>Serán también competentes para conocer éstas causas los jueces del lugar en el que se hubiere cometido la infracción.</p> <p>Tratándose de transmisiones a través de un satélite, la infracción se entenderá cometida bien en el lugar en que se iniciare dicha transmisión, bien en el lugar en que la señal se hiciere accesible al público de forma predominante.</p> <p>En caso de infracciones cometidas a través de redes de comunicación digital, se entenderán cometidas las mismas, bien en el lugar en que se encuentren los sistemas informáticos referidos en el artículo 292, bien en el lugar en que la transmisión se hiciere accesible al público de forma predominante.</p>
<b>Title 5 – Ancillary liability and sanctions</b>	
<p><b>Article 11 – Attempt and aiding or abetting</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established</p>	<p><b><u>CÓDIGO ORGÁNICO INTEGRAL PENAL</u></b></p> <p><b>LIBRO PRIMERO LA INFRACCIÓN PENAL</b></p> <p><b>TÍTULO I LA INFRACCIÓN PENAL EN GENERAL</b></p> <p><b>CAPÍTULO SEGUNDO EJECUCIÓN DE LA INFRACCIÓN</b></p> <p><b>Artículo 39.- Tentativa.-</b> Tentativa es la ejecución que no logra consumarse o cuyo resultado no llega a verificarse por circunstancias ajenas a la voluntad del autor, a pesar de que de manera dolosa inicie la ejecución del tipo penal mediante actos idóneos conducentes de modo inequívoco a la realización de un delito.</p>

<b>BUDAPEST CONVENTION</b>	<b>DOMESTIC LEGISLATION</b>
<p>in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.</p> <p>3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.</p>	<p>En este caso, la persona responderá por tentativa y la pena aplicable será de uno a dos tercios de la que le correspondería si el delito se habría consumado.</p> <p>Las contravenciones solamente son punibles cuando se consuman.</p> <p><b>CAPÍTULO TERCERO PARTICIPACIÓN</b></p> <p><b>Artículo 41.- Participación.-</b> Las personas participan en la infracción como autores o cómplices.</p> <p>Las circunstancias o condiciones que limitan o agravan la responsabilidad penal de una autora, de un autor o cómplice no influyen en la situación jurídica de los demás partícipes en la infracción penal.</p> <p><b>Artículo 42.- Autores.-</b> Responderán como autoras las personas que incurran en alguna de las siguientes modalidades:</p> <p><b>1. Autoría directa:</b></p> <ul style="list-style-type: none"><li>a) Quienes cometan la infracción de una manera directa e inmediata.</li><li>b) Quienes no impidan o procuren impedir que se evite su ejecución teniendo el deber jurídico de hacerlo.</li></ul> <p><b>2. Autoría mediata:</b></p> <ul style="list-style-type: none"><li>a) Quienes instiguen o aconsejen a otra persona para que cometa una infracción, cuando se demuestre que tal acción ha determinado su comisión.</li><li>b) Quienes ordenen la comisión de la infracción valiéndose de otra u otras personas, imputables o no, mediante precio, dádiva, promesa, ofrecimiento, orden o cualquier otro medio fraudulento, directo o indirecto.</li><li>c) Quienes, por violencia física, abuso de autoridad, amenaza u otro medio coercitivo, obliguen a un tercero a cometer la infracción, aunque no pueda calificarse como irresistible la fuerza empleada con dicho fin.</li><li>d) Quienes ejerzan un poder de mando en la organización delictiva.</li></ul> <p><b>3. Coautoría:</b> Quienes coadyuven a la ejecución, de un modo principal, practicando deliberada e intencionalmente algún acto sin el cual no habría podido perpetrarse la infracción.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p><b>Artículo 43.- Cómplices.-</b> Responderán como cómplices las personas que, en forma dolosa, faciliten o cooperen con actos secundarios, anteriores o simultáneos a la ejecución de una infracción penal, de tal forma que aun sin esos actos, la infracción se habría cometido.</p> <p>No cabe complicidad en las infracciones culposas.</p> <p>Si de las circunstancias de la infracción resulta que la persona acusada de complicidad, coopera en un acto menos grave que el cometido por la autora o el autor, la pena se aplicará solamente en razón del acto que pretendió ejecutar.</p> <p>El cómplice será sancionado con una pena equivalente de un tercio a la mitad de aquella prevista para la o el autor.</p>
<p><b>Article 12 – Corporate liability</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:</p> <ul style="list-style-type: none"> <li>a a power of representation of the legal person;</li> <li>b an authority to take decisions on behalf of the legal person;</li> <li>c an authority to exercise control within the legal person.</li> </ul> <p>2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.</p> <p>3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.</p> <p>4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.</p>	<p><b><u>CÓDIGO ORGÁNICO INTEGRAL PENAL</u></b></p> <p><b>TÍTULO IV INFRACCIONES EN PARTICULAR</b></p> <p><b>CAPÍTULO TERCERO DELITOS CONTRA LOS DERECHOS DEL BUEN VIVIR</b></p> <p><b>SECCIÓN TERCERA Delitos contra la seguridad de los activos de los sistemas de información y comunicación</b></p> <p><b>Art. 234.3.- Responsabilidad de personas jurídicas.-</b> A los delitos de esta Sección es aplicable la responsabilidad prevista en los artículos 49 y 71 de este Código.</p> <p><b>LIBRO PRIMERO LA INFRACCIÓN PENAL TÍTULO I LA INFRACCIÓN PENAL EN GENERAL</b></p> <p><b>CAPÍTULO QUINTO RESPONSABILIDAD PENAL DE LA PERSONA JURÍDICA</b></p> <p><b>Art. 49.- Responsabilidad de las personas jurídicas.-</b> En los supuestos previstos en este Código, las personas jurídicas nacionales o extranjeras de derecho privado son penalmente responsables por los delitos cometidos para beneficio propio o de sus asociados, por la acción u omisión de quienes ejercen su propiedad o control, sus órganos de gobierno o administración, apoderadas o apoderados, mandatarias o mandatarios, representantes legales o convencionales, agentes, operadoras u operadores, factores, delegadas o delegados, terceros que contractualmente o no, se inmiscuyen en una actividad de gestión, ejecutivos principales o quienes cumplan actividades de</p>

<b>BUDAPEST CONVENTION</b>	<b>DOMESTIC LEGISLATION</b>
	<p>administración, dirección y supervisión y, en general, por quienes actúen bajo órdenes o instrucciones de las personas naturales citadas.</p> <p>La responsabilidad penal de la persona jurídica es independiente de la responsabilidad penal de las personas naturales que intervengan con sus acciones u omisiones en la comisión del delito. La responsabilidad penal de la persona jurídica subsistirá aun cuando no haya sido posible identificar a la persona natural infractora.</p> <p>No hay lugar a la determinación de la responsabilidad penal de la persona jurídica, cuando el delito se comete por cualquiera de las personas naturales indicadas en el inciso primero, en beneficio de un tercero ajeno a la persona jurídica.</p> <p>La responsabilidad penal de la persona jurídica se atenuará de conformidad con el número 7 del artículo 45 del presente Código. Los sistemas de integridad, normas, programas y/o políticas de cumplimiento, prevención, dirección y/o supervisión, deberán incorporar los siguientes requisitos mínimos, sin perjuicio de las disposiciones del Reglamento que se dicte para el efecto, y de otras normas específicas:</p> <ol style="list-style-type: none"><li>1. Identificación, detección y administración de actividades en las que se presente riesgo;</li><li>2. Controles internos con responsables para procesos que representen riesgo;</li><li>3. Supervisión y monitoreo continuo, tanto interna, como evaluaciones independientes de los sistemas, programas y políticas, protocolos o procedimientos para la adopción y ejecución de 15estion15s sociales;</li><li>4. Modelos de 15estion financiera;</li><li>5. Canal de denuncias;</li><li>6. Código de Ética;</li><li>7. Programas de capacitación del personal;</li><li>8. Mecanismos de investigación interna;</li><li>9. Obligación de informar al encargado de cumplimiento sobre posibles riesgos o incumplimientos;</li><li>10. Normas para sancionar disciplinariamente las vulneraciones del sistema;</li><li>y, 11. Programas conozca a su cliente o debida diligencia.</li></ol>
<b>Article 13 – Sanctions and measures</b>	<b><u><a href="#">CÓDIGO ORGÁNICO INTEGRAL PENAL</a></u></b>

<p style="text-align: center;"><b>BUDAPEST CONVENTION</b></p>	<p style="text-align: center;"><b>DOMESTIC LEGISLATION</b></p>
<p>1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.</p> <p>2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.</p>	<p><b>LIBRO PRIMERO LA INFRACCIÓN PENAL</b>  <b>TÍTULO II PENAS Y MEDIDAS DE SEGURIDAD</b>  <b>CAPÍTULO PRIMERO LA PENA EN GENERAL</b></p> <p><b>Art. 51.- Pena.-</b> La pena es una restricción a la libertad y a los derechos de las personas, como consecuencia jurídica de sus acciones u omisiones punibles. Se basa en una disposición legal e impuesta por una sentencia condenatoria ejecutoriada.</p> <p><b>Artículo 52.- Finalidad de la pena.-</b> Los fines de la pena son la prevención general para la comisión de delitos y el desarrollo progresivo de los derechos y capacidades de la persona con condena así como la reparación del derecho de la víctima.</p> <p>En ningún caso la pena tiene como fin el aislamiento y la neutralización de las personas como seres sociales.</p> <p><b>Artículo 53.- Legalidad de la pena.-</b> No se impondrán penas más severas que las determinadas en los tipos penales de este Código. El tiempo de duración de la pena debe ser determinado. Quedan proscritas las penas indefinidas.</p>
<p><b>Section 2 – Procedural law</b></p>	
<p><b>Article 14 – Scope of procedural provisions</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.</p> <p>2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:</p> <ul style="list-style-type: none"> <li>a the criminal offences established in accordance with Articles 2 through 11 of this Convention;</li> <li>b other criminal offences committed by means of a computer system; and</li> <li>c the collection of evidence in electronic form of a criminal offence.</li> </ul> <p>3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences</p>	



BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.</p> <p>b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:</p> <ul style="list-style-type: none"> <li>i is being operated for the benefit of a closed group of users, and</li> <li>ii does not employ public communications networks and is not connected with another computer system, whether public or private,</li> </ul> <p>that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21</p>	
<p><b>Article 15 – Conditions and safeguards</b></p> <p>1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.</p> <p>2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, <i>inter alia</i>, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.</p> <p>3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.</p>	<p><b><u>CÓDIGO ORGÁNICO INTEGRAL PENAL</u></b>  <b>LIBRO PRELIMINAR NORMAS RECTORAS</b>  <b>TÍTULO II GARANTÍAS Y PRINCIPIOS GENERALES</b>  <b>CAPÍTULO PRIMERO PRINCIPIOS GENERALES</b>  <b>Artículo 2.- Principios generales.-</b> En materia penal se aplican todos los principios que emanan de la Constitución de la República, de los instrumentos internacionales de derechos humanos y los desarrollados en este Código.</p> <p><b>CAPÍTULO SEGUNDO GARANTÍAS Y PRINCIPIOS RECTORES DEL PROCESO PENAL</b>  <b>Artículo 4.- Dignidad humana y titularidad de derechos.-</b> Las y los intervinientes en el proceso penal son titulares de los derechos humanos reconocidos por la Constitución de la República y los instrumentos internacionales.</p> <p>Las personas privadas de libertad conservan la titularidad de sus derechos humanos con las limitaciones propias de la privación de libertad y serán tratadas con respeto a su dignidad como seres humanos. Se prohíbe el hacinamiento.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p><b>LIBRO SEGUNDO PROCEDIMIENTO</b> <b>TÍTULO I JURISDICCIÓN Y COMPETENCIA</b> <b>TÍTULO IV PRUEBA</b> <b>CAPÍTULO PRIMERO DISPOSICIONES GENERALES</b> <b>Artículo 454.- Principios.-</b> El anuncio y práctica de la prueba se registrará por los siguientes principios:</p> <ol style="list-style-type: none"><li><b>1. Oportunidad.</b> Es anunciada en la etapa de evaluación y preparatoria de juicio y se practica únicamente en la audiencia de juicio.</li></ol> <p>Los elementos de convicción deben ser presentados en la etapa de evaluación y preparatoria de juicio. Las investigaciones y pericias practicadas durante la investigación alcanzarán el valor de prueba, una vez que sean presentadas, incorporadas y valoradas en la audiencia oral de juicio.</p> <p>Sin embargo, en los casos excepcionales previstos en este Código, podrá ser prueba el testimonio producido de forma anticipada.</p> <ol style="list-style-type: none"><li><b>2. Inmediación.-</b> Las o los juzgadores y las partes procesales deberán estar presentes en la práctica de la prueba.</li><li><b>3. Contradicción.-</b> Las partes tienen derecho a conocer oportunamente y controvertir las pruebas, tanto las que son producidas en la audiencia de juicio como las testimoniales que se practiquen en forma anticipada.</li><li><b>4. Libertad probatoria.-</b> Todos los hechos y circunstancias pertinentes al caso, se podrán probar por cualquier medio que no sea contrario a la Constitución, los instrumentos internacionales de derechos humanos, los instrumentos internacionales ratificados por el Estado y demás normas jurídicas.</li><li><b>5. Pertinencia.-</b> Las pruebas deberán referirse, directa o indirectamente a los hechos o circunstancias relativos a la comisión de la infracción y sus consecuencias, así como a la responsabilidad penal de la persona procesada.</li><li><b>6. Exclusión.-</b> Toda prueba o elemento de convicción obtenidos con violación a los derechos establecidos en la Constitución, en los instrumentos internacionales de derechos humanos o en la Ley, carecerán de eficacia probatoria, por lo que deberán excluirse de la actuación procesal.</li></ol>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>Se inadmitirán aquellos medios de prueba que se refieran a las conversaciones que haya tenido la o el fiscal con la persona procesada o su defensa en desarrollo de manifestaciones preacordadas.</p> <p>Los partes informativos, noticias del delito, versiones de los testigos, informes periciales y cualquier otra declaración previa, se podrán utilizar en el juicio con la única finalidad de recordar y destacar contradicciones, siempre bajo la prevención de que no sustituyan al testimonio. En ningún caso serán admitidos como prueba.</p> <p><b>7. Principio de igualdad de oportunidades para la prueba.-</b> Se deberá garantizar la efectiva igualdad material y formal de los intervinientes en el desarrollo de la actuación procesal.</p>
<p><b>Article 16 – Expedited preservation of stored computer data</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.</p> <p>2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person’s possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.</p>	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	
<p><b>Article 17 – Expedited preservation and partial disclosure of traffic data</b></p> <p>1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:</p> <ul style="list-style-type: none"> <li>a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and</li> <li>b ensure the expeditious disclosure to the Party’s competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.</li> </ul> <p>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>N/A</p>
<p><b>Article 18 – Production order</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:</p> <ul style="list-style-type: none"> <li>a a person in its territory to submit specified computer data in that person’s possession or control, which is stored in a computer system or a computer-data storage medium; and</li> <li>b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider’s possession or control.</li> </ul> <p>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p> <p>3 For the purpose of this article, the term “subscriber information” means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:</p> <ul style="list-style-type: none"> <li>a the type of communication service used, the technical provisions taken thereto and the period of service;</li> </ul>	<p>N/A</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<ul style="list-style-type: none"> <li>b the subscriber’s identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;</li> <li>c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.</li> </ul>	
<p><b>Article 19 – Search and seizure of stored computer data</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:</p> <ul style="list-style-type: none"> <li>a a computer system or part of it and computer data stored therein;</li> </ul> <p>and</p> <ul style="list-style-type: none"> <li>b a computer-data storage medium in which computer data may be stored</li> </ul> <p style="padding-left: 40px;">in its territory.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:</p> <ul style="list-style-type: none"> <li>a seize or similarly secure a computer system or part of it or a computer-data storage medium;</li> <li>b make and retain a copy of those computer data;</li> <li>c maintain the integrity of the relevant stored computer data;</li> <li>d render inaccessible or remove those computer data in the accessed computer system.</li> </ul> <p>4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the</p>	<p><b><u>CÓDIGO ORGÁNICO INTEGRAL PENAL</u></b></p> <p><b>TÍTULO IV PRUEBA</b></p> <p><b>CAPÍTULO SEGUNDO ACTUACIONES Y TÉCNICAS ESPECIALES DE INVESTIGACIÓN</b></p> <p><b>SECCIÓN SEGUNDA Registros y allanamiento</b></p> <p><b>Artículo 480.- Allanamiento.-</b> El domicilio o el lugar donde la persona desarrolle su actividad familiar, comercial o laboral, podrá ser allanado en los siguientes casos:</p> <ol style="list-style-type: none"> <li>1. Cuando se trate de detener a una persona contra la que se ha dictado orden de detención con fines de investigación, prisión preventiva o se ha pronunciado sentencia condenatoria ejecutoriada con pena privativa de libertad.</li> <li>2. Cuando la Policía Nacional esté en persecución ininterrumpida de una persona que ha cometido un delito flagrante.</li> <li>3. Cuando se trate de impedir la consumación de una infracción que se está realizando o de socorrer a sus víctimas.</li> <li>4. Cuando se trate de socorrer a las víctimas de un accidente del que pueda correr peligro la vida de las personas.</li> <li>5. Cuando se trate de recaudar la cosa sustraída o reclamada o los objetos que constituyan elementos probatorios o estén vinculados al hecho que se investiga. En estos casos se procederá a la aprehensión de los bienes.</li> <li>6. En los casos de violencia contra la mujer o miembros del núcleo familiar, cuando deba recuperarse a la agredida, agredido, o a sus familiares; cuando la agresora o el agresor se encuentre armado o bajo los efectos del alcohol, de</li> </ol>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.</p> <p>5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>sustancias catalogadas sujetas a fiscalización o esté agrediendo a su pareja o poniendo en riesgo la integridad física, psicológica o sexual de cualquier miembro de la familia de la víctima.</p> <p>7. Cuando se trate de situaciones de emergencia, tales como: incendio, explosión, inundación u otra clase de estragos que pongan en peligro la vida o la propiedad.</p> <p>En los casos de los numerales 1 y 5 se requerirá orden motivada de la o el juzgador y en los demás casos no requerirá formalidad alguna.</p> <p>Para evitar la fuga de personas o la extracción de armas, instrumentos, objetos o documentos probatorios y mientras se ordena el allanamiento, la o el fiscal podrá disponer la vigilancia del lugar, la retención de las cosas y solicitar a la o al juzgador la orden de detención con fines investigativos para las personas que se encuentren en él.</p> <p><b>Artículo 481.- Orden de allanamiento.-</b> La orden de allanamiento deberá constar por escrito y señalar los motivos que determinan el registro, las diligencias por practicar, la dirección o ubicación concreta del lugar o lugares donde se ejecute el allanamiento y su fecha de expedición. En casos de urgencia, la o el fiscal podrá solicitar la orden verbalmente o por cualquier medio conveniente, dejando constancia de los motivos que determinen el allanamiento.</p> <p>De no ser posible la descripción exacta del lugar o lugares por registrar, la o el fiscal indicará los argumentos para que, a pesar de ello, se deberá proceder al operativo. En ninguna circunstancia podrá emitirse órdenes de registro y allanamiento arbitrarios.</p> <p>La o el juzgador podrá autorizar el allanamiento por cualquier medio, dejando constancia de dicho acto.</p> <p><b>Artículo 482.- Procedimiento del allanamiento.-</b> El allanamiento deberá realizarse de conformidad con las siguientes reglas:</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>1. Con la presencia de la o el fiscal acompañado de la Policía Nacional, sin que puedan ingresar personas no autorizadas por la o el fiscal al lugar que deba allanarse.</p> <p>2. Si presentada la orden de allanamiento, la o el propietario o habitante de la vivienda, lugar de trabajo o local, se resiste a la entrega de la persona o de las cosas o al ingreso o exhibición de lugares u objetos que se encuentren al interior de dichos lugares, el o la fiscal ordenará el quebrantamiento de las puertas o cerraduras.</p> <p>3. Practicado el allanamiento, la o el fiscal reconocerá en presencia de los concurrentes las dependencias del local allanado, las armas, documentos u objetos concernientes a la infracción. El personal del Sistema especializado integral de investigación, medicina legal y ciencias forenses, recogerá los elementos de convicción pertinentes, previo inventario, descripción detallada y embalaje para cadena de custodia.</p> <p>(...)</p>
<p><b>Article 20 – Real-time collection of traffic data</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:</p> <ul style="list-style-type: none"> <li>a collect or record through the application of technical means on the territory of that Party, and</li> <li>b compel a service provider, within its existing technical capability: <ul style="list-style-type: none"> <li>i to collect or record through the application of technical means on the territory of that Party; or</li> <li>ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.</li> </ul> </li> </ul> <p>2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified</p>	<p><b><u>CÓDIGO ORGÁNICO INTEGRAL PENAL</u></b></p> <p><b>TÍTULO IV PRUEBA</b></p> <p><b>CAPÍTULO SEGUNDO ACTUACIONES Y TÉCNICAS ESPECIALES DE INVESTIGACIÓN</b></p> <p><b>SECCIÓN PRIMERA Actuaciones especiales de investigación</b></p> <p><b>Art. 500.- Contenido digital.-</b> El contenido digital es todo acto informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí.</p> <p>En la investigación se seguirán las siguientes reglas:</p> <p>1. El análisis, valoración, recuperación y presentación del contenido digital almacenado en dispositivos o sistemas informáticos se realizará a través de técnicas digitales forenses.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>communications transmitted in its territory, through the application of technical means on that territory.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>2. Cuando el contenido digital se encuentre almacenado en sistemas y memorias volátiles o equipos tecnológicos que formen parte de la infraestructura critica del sector público o privado, se realizará su recolección, en el lugar y en tiempo real, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.</p> <p>3. Cuando el contenido digital se encuentre almacenado en medios no volátiles, se realizará su recolección, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.</p> <p>4. Cuando se recolecte cualquier medio físico que almacene, procese o transmita contenido digital durante una investigación, registro o allanamiento, se deberá identificar e inventariar cada objeto individualmente, fijará su ubicación física con fotografías y un plano del lugar, se protegerá a través de técnicas digitales forenses y se trasladará mediante cadena de custodia a un centro de acopio especializado para este efecto.</p>
<p><b>Article 21 – Interception of content data</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:</p> <p>a collect or record through the application of technical means on the territory of that Party, and</p> <p>b compel a service provider, within its existing technical capability:</p> <p>    i to collect or record through the application of technical means on the territory of that Party, or</p> <p>    ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.</p> <p>2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the</p>	<p><b><u>CÓDIGO ORGÁNICO INTEGRAL PENAL</u></b></p> <p><b>TÍTULO IV PRUEBA</b></p> <p><b>CAPÍTULO SEGUNDO ACTUACIONES Y TÉCNICAS ESPECIALES DE INVESTIGACIÓN</b></p> <p><b>SECCIÓN PRIMERA Actuaciones especiales de investigación</b></p> <p><b>Artículo 476.- Interceptación de las comunicaciones o datos informáticos.-</b> La o el juzgador ordenará la interceptación de las comunicaciones o datos informáticos previa solicitud fundamentada de la o el fiscal, cuando existan indicios que resulten relevantes a los fines de la investigación y la medida sea idónea, necesaria y proporcional, de conformidad con las siguientes reglas:</p> <p>1. La o el juzgador determinará la comunicación interceptada y el tiempo de interceptación, que no podrá ser mayor a un plazo de noventa días. Transcurrido el tiempo autorizado se podrá solicitar motivadamente por una sola vez una prórroga hasta por un plazo de noventa días.</p> <p>Cuando sean investigaciones de delincuencia organizada y sus delitos relacionados, la interceptación podrá realizarse hasta por un plazo de seis meses.</p>



<b>BUDAPEST CONVENTION</b>	<b>DOMESTIC LEGISLATION</b>
<p>execution of any power provided for in this article and any information relating to it.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>Transcurrido el tiempo autorizado se podrá solicitar motivadamente por una sola vez una prórroga hasta por un plazo de seis meses.</p> <p>2. La información relacionada con la infracción que se obtenga de las comunicaciones que se intercepten durante la investigación serán utilizadas en el proceso para el cual se las autoriza y con la obligación de guardar secreto de los asuntos ajenos al hecho que motive su examen.</p> <p>3. Cuando, en el transcurso de una interceptación se conozca del cometimiento de otra infracción, se comunicará inmediatamente a la o al fiscal para el inicio de la investigación correspondiente. En el caso de delitos flagrantes, se procederá conforme con lo establecido en este Código.</p> <p>4. Previa autorización de la o el juzgador, la o el fiscal, realizará la interceptación y registro de los datos informáticos en transmisión a través de los servicios de telecomunicaciones como: telefonía fija, satelital, móvil e inalámbrica, con sus servicios de llamadas de voz, mensajes SMS, mensajes MMS, transmisión de datos y voz sobre IP, correo electrónico, redes sociales, videoconferencias, multimedia, entre otros, cuando la o el fiscal lo considere indispensable para comprobar la existencia de una infracción o la responsabilidad de los partícipes.</p> <p>5. Está prohibida la interceptación de cualquier comunicación protegida por el derecho a 25rofessio el secreto 25rofessional y religioso. Las actuaciones procesales que violenten esta garantía carecen de eficacia probatoria, sin perjuicio de las respectivas sanciones.</p> <p>6. Al proceso solo se introducirá de manera textual la transcripción de aquellas conversaciones o parte de ellas que se estimen útiles o relevantes para los fines de la investigación. No obstante, la persona procesada podrá 25upervisi la audición de todas sus grabaciones, cuando lo considere apropiado para su defensa.</p> <p>Toda información que no resulte útil o relevante a los fines de la investigación será eliminada de oficio por parte del fiscal y se remitirá el acta que deje constancia de este hecho a fin registrarlo en el expediente 25upervisi. La destrucción de la información se realizará bajo la 25upervision del juez competente, el cual podrá ordenar la eliminación de la información que no haya</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>sido considerada relevante o útil para probar la materialidad o responsabilidad de una infracción.</p> <p>7. El personal de las prestadoras de servicios de telecomunicaciones, así como las personas encargadas de interceptar, grabar y transcribir las comunicaciones o datos informáticos tendrán la obligación de guardar reserva sobre su contenido, salvo cuando se las llame a declarar en juicio.</p> <p>8. El medio de almacenamiento de la información obtenida durante la interceptación deberá ser conservado por la o el fiscal en un centro de acopio especializado para el efecto, hasta que sea presentado en juicio.</p> <p>9. Quedan prohibidas la interceptación, grabación y transcripción de comunicaciones que vulneren los derechos de los niños, niñas y adolescentes, especialmente en aquellos casos que generen la revictimización en infracciones.</p> <p><b>Art. 477.- Reconocimiento de grabaciones.-</b> La o el juzgador autorizará a la o al fiscal el reconocimiento de las grabaciones mencionadas en el artículo anterior, así como de vídeos, datos informáticos, fotografías, discos u otros medios análogos o digitales. Para este efecto, con la intervención de dos peritos que juren guardar reserva, la o el fiscal, en audiencia privada, procederá a la exhibición de la película o a escuchar el disco o la grabación y a examinar el contenido de los registros informáticos. Las partes podrán asistir con el mismo juramento.</p> <p>La o el fiscal podrá ordenar la identificación de voces grabadas, por parte de personas que afirmen poder reconocerlas, sin perjuicio de ordenar el reconocimiento por medios técnicos.</p>
<b>Section 3 – Jurisdiction</b>	
<p><b>Article 22 – Jurisdiction</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:</p> <ul style="list-style-type: none"> <li>a in its territory; or</li> <li>b on board a ship flying the flag of that Party; or</li> </ul>	<p><b><u>CODIGO DE PROCEDIMIENTO PENAL</u></b></p> <p><b>LIBRO PRIMERO PRINCIPIOS FUNDAMENTALES</b></p> <p><b>TITULO I LA JURISDICCION Y LA COMPETENCIA</b></p> <p><b>CAPITULO I LA JURISDICCION</b></p> <p><b>Art. 18. - Ambito de la jurisdicción penal.-</b> Están sujetos a la jurisdicción penal del Ecuador:</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>c on board an aircraft registered under the laws of that Party; or</p> <p>d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.</p> <p>2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.</p> <p>3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.</p> <p>4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.</p> <p>When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.</p>	<p>1) Los ecuatorianos y extranjeros que cometan una infracción en el territorio de la República. Se exceptúan, con arreglo a las convenciones internacionales ratificadas por el Ecuador, los Jefes de otros Estados que se encuentren en el país; los representantes diplomáticos acreditados ante el Gobierno del Ecuador y residentes en territorio ecuatoriano; y, los representantes diplomáticos transeúntes de otro Estado que pasen ocasionalmente por el Ecuador. Esta excepción se extiende al cónyuge e hijos, empleados extranjeros y demás comitiva del Jefe de Estado o de cada representante diplomático, siempre que oficialmente, pongan en conocimiento del Ministerio de Relaciones Exteriores la nómina de tal comitiva o del personal de la Misión.</p> <p>Se exceptúa también a los que cometieren una infracción dentro del perímetro de las operaciones militares de un ejército extranjero, cuando el Estado ecuatoriano haya autorizado el paso por su territorio, salvo que el presunto infractor no tenga relación legal con dicho ejército;</p> <p>2) El Jefe del Estado y los representantes diplomáticos del Ecuador, su familia y comitiva, que cometan un delito en territorio extranjero, y los Cónsules ecuatorianos que, en igual caso, lo hagan en el ejercicio de sus funciones consulares;</p> <p>3) Los ecuatorianos o extranjeros que delincan a bordo de naves o de aeronaves nacionales, en alta mar o en el espacio aéreo libre;</p> <p>4) Los ecuatorianos o extranjeros que, en las aguas o en el espacio aéreo de otro Estado, delincan a bordo de naves o aeronaves de guerra ecuatorianas;</p> <p>5) Los ecuatorianos o extranjeros que cometieren un delito a bordo de naves o aeronaves extranjeras que no sean de guerra, en las aguas o en el espacio aéreo del Ecuador;</p> <p>6) Los ecuatorianos o extranjeros que cometan delitos contra el Decreto Internacional o previstos en Convenios o Tratados Internacionales vigentes, siempre que no hayan sido juzgados en otro Estado; y,</p> <p>7) Los nacionales o extranjeros que se hallen comprendidos en algunos de los demás casos señalados en el Código Penal.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<b>Chapter III – International co-operation</b>	
<p><b>Article 24 – Extradition</b></p> <p>1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.</p> <p>b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.</p> <p>2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.</p> <p>3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.</p> <p>4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.</p> <p>5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.</p> <p>6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those</p>	<p><b><u>REGLEAMENTO A LA LEY DE EXTRANJERIA</u></b>  <b>CAPITULO I Procedimientos Fundamentales</b>  <b>TITULO I LA EXTRADICION PASIVA</b></p> <p><b>Art. 1.-</b> La extradición será solicitada por vía diplomática o en caso de falta de representante diplomático del Estado requirente, de Gobierno a Gobierno, acompañando al pedido una copia auténtica de la sentencia condenatoria o del mandamiento de prisión preventiva, emitido por juez o tribunal competente, con indicación precisa sobre el lugar, fecha, naturaleza y circunstancias del hecho delictivo, identidad del sindicado y un ejemplar de la Ley penal sobre el delito, pena y prescripción aplicables al caso.</p> <p>Cuando el trámite se realice por vía diplomática no será necesaria la autenticación de los documentos presentados.</p> <p><b>Art. 2.-</b> En caso de urgencia, el Ministro de Gobierno, dispondrá la prisión preventiva del sindicado, mediante requerimiento idóneo efectuado por cualquier medio de comunicación, por juez o tribunal competente, funcionario diplomático o consular del Estado requirente.</p> <p>Para la procedencia de esta medida, deberá indicarse el delito cometido y fundamentarse en sentencia condenatoria o mandamiento de prisión.</p> <p>Dentro de los sesenta días siguientes a la fecha de la prisión preventiva, el Estado requirente deberá presentar el pedido formal de extradición acompañando los documentos determinados en el artículo primero.</p> <p><b>Art. 3.-</b> Serán condiciones para conceder la extradición: I. Que el delito haya sido cometido en el territorio del Estado requirente o sean aplicables al sindicado las leyes penales de ese Estado. II. Que exista sentencia ejecutoriada de privación de libertad del sindicado, emitida por juez o tribunal competente del Estado requirente.</p> <p><b>Art. 4.-</b> No se concederá la extradición en los casos siguientes:</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.</p> <p>7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.</p> <p>b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure</p>	<p>I. De ecuatorianos, exceptuándose los que hubieran adquirido esta nacionalidad con posterioridad al hecho delictivo que motiva el pedido.</p> <p>II. Cuando el hecho que motiva la solicitud no sea considerado delito por la Ley Ecuatoriana ni por la del Estado requirente.</p> <p>III. Cuando los jueces nacionales resulten competentes de acuerdo con la Ley interna, para juzgar el delito imputado al sindicado.</p> <p>IV. Cuando la Ley Ecuatoriana impusiere al delito imputado una pena igual o inferior a un año de prisión.</p> <p>V. Cuando el sindicado hubiere sido procesado o hubiere sido condenado o absuelto en el Ecuador por el mismo hecho en que se fundamente el pedido.</p> <p>VI. Cuando se hubiere verificado la prescripción según la Ley ecuatoriana o la del Estado requirente.</p> <p>VII. Cuando se trate de un delito político, exceptuándose los casos en que el hecho punible constituya principalmente infracción de la Ley penal común o cuando el delito común conexo al delito político constituya el hecho principal.</p> <p>La calificación del carácter de la infracción punible competirá exclusivamente al Presidente de la Corte Suprema de Justicia de conformidad con las leyes y tratados internacionales vigentes.</p> <p>VIII. Cuando el sindicado tuviere que responder en el Estado requirente ante juez o tribunal de excepción.</p> <p><b>Art. 5.-</b> Cuando más de un estado solicite la extradición de una misma persona por el mismo hecho, tendrá preferencia el pedido del Estado en cuyo territorio se haya cometido el delito.</p> <p>Tratándose de diversos delitos, tendrán preferencia sucesivamente:</p> <p>I. El Estado requirente en cuyo territorio haya sido cometido el delito más grave según las leyes ecuatorianas.</p> <p>II. El Estado que en primer lugar hubiera solicitado la entrega, siendo de igual gravedad el delito.</p> <p>III. El Estado de origen o en su falta, el del último domicilio del sindicado, si los pedidos son simultáneos.</p> <p>IV. En caso de duda la preferencia queda a discreción del Gobierno del Ecuador.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>Habiendo tratado con algunos de los Estados requirentes prevalecerán sus estipulaciones respecto a la preferencia que trata este artículo.</p> <p><b>Art. 6.-</b> Presentada la solicitud de extradición al Ministro de Relaciones Exteriores, éste examinará si se han acompañado a la misma los documentos que establezca el respectivo Tratado o, en su falta, los del artículo primero de este Reglamento. Si el Ministro estimare que falta alguno de los requisitos de forma, devolverá la solicitud para que sean presentados, sin perjuicio de que el Ministerio de Relaciones Exteriores pueda considerar dicha solicitud incompleta como simple pedido de detención preventiva hasta por sesenta días, vencidos los cuales, sin que la hubiere completado, el sindicado será puesto en libertad. (...)</p> <p><b>TITULO II LA EXTRADICION ACTIVA</b></p> <p><b>Art. 12.-</b> Para que el Juez de la causa eleve los antecedentes al Presidente de la Corte Suprema de Justicia, será necesario que se haya dictado previamente auto firme de prisión o recaído sentencia ejecutoriada contra el acusado cuya extradición se pretende. D</p> <p>berán también constar en el proceso el país y lugar en que el reo se encuentre en la actualidad.</p> <p><b>Art. 13.-</b> Recibido el proceso pasará a conocimiento del Presidente de la Corte Suprema de Justicia para que dictamine si es o no procedente la petición de extradición de conformidad a los tratados celebrados en la nación en que el reo se encuentre refugiado o en defecto de tratado, con arreglo a los principios de Derecho Internacional.</p>
<p><b>Article 25 – General principles relating to mutual assistance</b> 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.</p>	<p><b><u>CÓDIGO ORGÁNICO INTEGRAL PENAL</u></b> <b>TÍTULO IV PRUEBA</b> <b>CAPÍTULO SEGUNDO ACTUACIONES Y TÉCNICAS ESPECIALES DE INVESTIGACIÓN</b></p> <p><b>Art. 488.- Remisión de elementos probatorios.-</b> Sin perjuicio del desarrollo de investigaciones conjuntas y de la asistencia judicial recíproca, la o el fiscal solicitará directamente a las autoridades policiales y judiciales extranjeras, la</p>

<p style="text-align: center;"><b>BUDAPEST CONVENTION</b></p>	<p style="text-align: center;"><b>DOMESTIC LEGISLATION</b></p>
<p>2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.</p> <p>3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.</p> <p>4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.</p> <p>5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.</p>	<p>remisión de los elementos probatorios necesarios para acreditar el hecho constitutivo de la infracción y la presunta responsabilidad penal de las personas investigadas en el país, de conformidad con los instrumentos internacionales vigentes, así como otorgar a dichas autoridades extranjeras tales antecedentes, si lo solicitan.</p> <p><b>Art. 496.- Investigaciones conjuntas.-</b> La República del Ecuador en sujeción de las normas de asistencia penal internacional, podrá desarrollar investigaciones conjuntas con uno o más países u órganos mixtos de investigación para combatir la delincuencia organizada transnacional.</p> <p><b>Art. 497.- Asistencia judicial recíproca.-</b> Las o los fiscales podrán solicitar asistencia directa a sus similares u órganos policiales extranjeros para la práctica de diligencias procesales, pericias e investigación de los delitos previstos en este Código. Esta asistencia se refiere entre otros hechos, a la detención y remisión de procesados y acusados, recepción de testimonios, exhibición de documentos inclusive bancarios, recuperación de contenido digital, inspecciones del lugar, envío de elementos probatorios, identificación y análisis de sustancias catalogadas sujetas a fiscalización e incautación y comiso de bienes. Asimismo, la o el fiscal podrá efectuar actuaciones en el extranjero dirigidas a recoger antecedentes acerca de hechos constitutivos de alguna infracción, a través de la asistencia penal internacional. Las diligencias señaladas serán incorporadas al proceso, presentadas y valoradas en la etapa del juicio.</p> <p><b><u>CODIGO ORGANICO GENERAL DE PROCESOS</u></b></p> <p><b>Art. 70.- Comunicaciones internacionales.</b> Las comunicaciones dirigidas a autoridades en el extranjero se enviarán por medio de exhorto o carta rogatoria conforme con lo dispuesto en los tratados e instrumentos internacionales.</p>
<p><b>Article 26 – Spontaneous information</b></p> <p>1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.</p>	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.</p>	
<p><b>Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements</b></p> <p>1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.</p> <p>2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.</p> <p>b The central authorities shall communicate directly with each other;</p> <p>c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;</p> <p>d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.</p> <p>3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.</p> <p>4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:</p> <p>a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or</p> <p>b it considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests.</p>	



<b>BUDAPEST CONVENTION</b>	<b>DOMESTIC LEGISLATION</b>
<p>5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.</p> <p>6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.</p> <p>7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.</p> <p>8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.</p> <p>9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.</p> <p>b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).</p> <p>c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.</p> <p>d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.</p> <p>e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency,</p>	

<b>BUDAPEST CONVENTION</b>	<b>DOMESTIC LEGISLATION</b>
requests made under this paragraph are to be addressed to its central authority.	
<p><b>Article 28 – Confidentiality and limitation on use</b></p> <p>1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.</p> <p>2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:</p> <ul style="list-style-type: none"><li>a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or</li><li>b not used for investigations or proceedings other than those stated in the request.</li></ul> <p>3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.</p> <p>4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.</p>	
<p><b>Article 29 – Expedited preservation of stored computer data</b></p> <p>1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.</p> <p>2 A request for preservation made under paragraph 1 shall specify:</p> <ul style="list-style-type: none"><li>a the authority seeking the preservation;</li><li>b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;</li><li>c the stored computer data to be preserved and its relationship to the offence;</li></ul>	

<b>BUDAPEST CONVENTION</b>	<b>DOMESTIC LEGISLATION</b>
----------------------------	-----------------------------

<p>d any available information identifying the custodian of the stored computer data or the location of the computer system;</p> <p>e the necessity of the preservation; and</p> <p>f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.</p> <p>3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.</p> <p>4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.</p> <p>5 In addition, a request for preservation may only be refused if:</p> <p>a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or</p> <p>b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests.</p> <p>6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.</p> <p>4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.</p>	
--	--

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p><b>Article 30 – Expedited disclosure of preserved traffic data</b></p> <p>1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.</p> <p>2 Disclosure of traffic data under paragraph 1 may only be withheld if:</p> <ul style="list-style-type: none"> <li>a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or</li> <li>b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests.</li> </ul>	
<p><b>Article 31 – Mutual assistance regarding accessing of stored computer data</b></p> <p>1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.</p> <p>2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.</p> <p>3 The request shall be responded to on an expedited basis where:</p> <ul style="list-style-type: none"> <li>a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or</li> <li>b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.</li> </ul>	
<p><b>Article 32 – Trans-border access to stored computer data with consent or where publicly available</b></p> <p>A Party may, without the authorisation of another Party:</p> <ul style="list-style-type: none"> <li>a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or</li> <li>b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and</li> </ul>	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.</p>	
<p><b>Article 33 – Mutual assistance in the real-time collection of traffic data</b>                      1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.                      2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.</p>	
<p><b>Article 34 – Mutual assistance regarding the interception of content data</b>                      The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.</p>	<p><b><u>CÓDIGO ORGÁNICO INTEGRAL PENAL</u></b>  <b>TÍTULO IV PRUEBA</b>  <b>CAPÍTULO SEGUNDO ACTUACIONES Y TÉCNICAS ESPECIALES DE INVESTIGACIÓN</b></p> <p><b>Art. 477.1.- Interceptación de las comunicaciones en cooperación internacional.-</b> En ejecución de una petición de una autoridad extranjera competente, el fiscal puede solicitar al juez de garantías penales competente que ordene la interceptación de transmisiones de contenido digital realizadas por medio de un sistema informático ubicado en el Ecuador, si así se prevé en algún acuerdo, tratado o convenio internacional vigente ratificado por el Ecuador y si se trata de situación en la que dicha interceptación está permitida en un caso nacional de características similares, respetándose el procedimiento y observándose los límites y garantías previstos en el derecho interno.</p>
<p><b>Article 35 – 24/7 Network</b>                      1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:                      a the provision of technical advice;</p>	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>b the preservation of data pursuant to Articles 29 and 30;</p> <p>c the collection of evidence, the provision of legal information, and locating of suspects.</p> <p>2 a A Party’s point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.</p> <p>b If the point of contact designated by a Party is not part of that Party’s authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.</p> <p>3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.</p>	
<p><b>Article 42 – Reservations</b></p> <p>By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.</p>	