

Table of contents*Version 20 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.

State:	
Signature of the Budapest Convention:	N/A
Ratification/accession:	20/04/2017

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
<p>Article 1 – “Computer system”, “computer data”, “service provider”, “traffic data”: For the purposes of this Convention:</p> <p>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;</p> <p>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;</p> <p>c “service provider” means:</p> <p>i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and</p> <p>ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;</p> <p>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>LEY N° 21.459 DE 2022 QUE ESTABLECE NORMAS SOBRE DELITOS INFORMÁTICOS</p> <p>TÍTULO III - DISPOSICIONES FINALES</p> <p>Artículo 15.- Para efectos de esta ley, se entenderá por:</p> <p>a) Datos informáticos: Toda representación de hechos, información o conceptos expresados en cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.</p> <p>b) Sistema informático: Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.</p> <p>c) Prestadores de servicios: Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático y cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo.</p>
Chapter II – Measures to be taken at the national level	
Section 1 – Substantive criminal law	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>Article 2 – Illegal access</p> <p>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><u>LEY N° 21.459 DE 2022 QUE ESTABLECE NORMAS SOBRE DELITOS INFORMÁTICOS</u></p> <p>TÍTULO I - DE LOS DELITOS INFORMÁTICOS Y SUS SANCIONES</p> <p>Artículo 2°.- Acceso ilícito. El que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.</p> <p>Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático, se aplicará la pena de presidio menor en su grado mínimo a medio. Igual pena se aplicará a quien divulgue la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste.</p> <p>En caso de ser una misma persona la que hubiere obtenido y divulgado la información, se aplicará la pena de presidio menor en sus grados medio a máximo.</p>
<p>Article 3 – Illegal interception</p> <p>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><u>LEY N° 21.459 DE 2022 QUE ESTABLECE NORMAS SOBRE DELITOS INFORMÁTICOS</u></p> <p>TÍTULO I - DE LOS DELITOS INFORMÁTICOS Y SUS SANCIONES</p> <p>Artículo 3°.- Interceptación ilícita. El que indebidamente intercepte, interrumpa o interfiera, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos, será castigado con la pena de presidio menor en su grado medio.</p> <p>El que, sin contar con la debida autorización, capte, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos, será castigado con la pena de presidio menor en su grado medio a máximo.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>Article 4 – Data interference</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><u>LEY N° 21.459 DE 2022 QUE ESTABLECE NORMAS SOBRE DELITOS INFORMÁTICOS</u></p> <p>TÍTULO I - DE LOS DELITOS INFORMÁTICOS Y SUS SANCIONES</p> <p>Artículo 4°.- Ataque a la integridad de los datos informáticos. El que indebidamente altere, dañe o suprima datos informáticos, será castigado con presidio menor en su grado medio, siempre que con ello se cause un daño grave al titular de estos mismos.</p>
<p>Article 5 – System interference</p> <p>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><u>LEY N° 21.459 DE 2022 QUE ESTABLECE NORMAS SOBRE DELITOS INFORMÁTICOS</u></p> <p>TÍTULO I - DE LOS DELITOS INFORMÁTICOS Y SUS SANCIONES</p> <p>Artículo 1°.- Ataque a la integridad de un sistema informático. El que obstaculice o impida el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos, será castigado con la pena de presidio menor en su grado medio a máximo.</p>
<p>Article 6 – Misuse of devices</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><u>LEY N° 21.459 DE 2022 QUE ESTABLECE NORMAS SOBRE DELITOS INFORMÁTICOS</u></p> <p>TÍTULO I - DE LOS DELITOS INFORMÁTICOS Y SUS SANCIONES</p> <p>Artículo 8°.- Abuso de los dispositivos. El que para la perpetración de los delitos previstos en los artículos 1° a 4° de esta ley o de las conductas señaladas en el artículo 7° de la ley N° 20.009, entregare u obtuviere para su utilización, importare, difundiera o realizare otra forma de puesta a disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados principalmente para la perpetración de dichos delitos, será sancionado con la pena de presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<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>	
Title 2 – Computer-related offences	
<p>Article 7 – Computer-related forgery 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><u>LEY N° 21.459 DE 2022 QUE ESTABLECE NORMAS SOBRE DELITOS INFORMÁTICOS</u></p> <p>TÍTULO I - DE LOS DELITOS INFORMÁTICOS Y SUS SANCIONES Artículo 5°.- Falsificación informática. El que indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos, será sancionado con la pena de presidio menor en sus grados medio a máximo.</p> <p>Cuando la conducta descrita en el inciso anterior sea cometida por empleado público, abusando de su oficio, será castigado con la pena de presidio menor en su grado máximo a presidio mayor en su grado mínimo.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>Article 8 – Computer-related fraud</p> <p>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"> a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, <p>with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.</p>	<p><u>LEY N° 21.459 DE 2022 QUE ESTABLECE NORMAS SOBRE DELITOS INFORMÁTICOS</u></p> <p>TÍTULO I - DE LOS DELITOS INFORMÁTICOS Y SUS SANCIONES</p> <p>Artículo 7°.- Fraude informático. El que, causando perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero, manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático, será penado:</p> <ul style="list-style-type: none"> 1) Con presidio menor en sus grados medio a máximo y multa de once a quince unidades tributarias mensuales, si el valor del perjuicio excediera de cuarenta unidades tributarias mensuales. 2) Con presidio menor en su grado medio y multa de seis a diez unidades tributarias mensuales, si el valor del perjuicio excediere de cuatro unidades tributarias mensuales y no pasare de cuarenta unidades tributarias mensuales. 3) Con presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales, si el valor del perjuicio no excediere de cuatro unidades tributarias mensuales. <p>Si el valor del perjuicio excediere de cuatrocientas unidades tributarias mensuales, se aplicará la pena de presidio menor en su grado máximo y multa de veintiuna a treinta unidades tributarias mensuales.</p> <p>Para los efectos de este artículo se considerará también autor al que, conociendo o no pudiendo menos que conocer la ilicitud de la conducta descrita en el inciso primero, facilita los medios con que se comete el delito.</p>
Title 3 – Content-related offences	
<p>Article 9 – Offences related to child pornography</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"> a producing child pornography for the purpose of its distribution through a computer system; 	<p><u>CÓDIGO PENAL, 1874</u></p> <p>TÍTULO SÉPTIMO - CRÍMENES Y DELITOS CONTRA EL ORDEN DE LAS FAMILIAS, CONTRA LA MORALIDAD PÚBLICA Y CONTRA LA INTEGRIDAD SEXUAL.</p> <p>§VI. Del estupro y otros delitos sexuales.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>b offering or making available child pornography through a computer system;</p> <p>c distributing or transmitting child pornography through a computer system;</p> <p>d procuring child pornography through a computer system for oneself or for another person;</p> <p>e possessing child pornography in a computer system or on a computer-data storage medium.</p> <p>2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:</p> <p>a a minor engaged in sexually explicit conduct;</p> <p>b a person appearing to be a minor engaged in sexually explicit conduct;</p> <p>c realistic images representing a minor engaged in sexually explicit conduct</p> <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>Art. 366 quinquies. El que participare en la producción de material pornográfico, cualquiera sea su soporte, en cuya elaboración hubieren sido utilizados menores de dieciocho años, será sancionado con presidio menor en su grado máximo.</p> <p>Para los efectos de este artículo y del artículo 374 bis, se entenderá por material pornográfico en cuya elaboración hubieren sido utilizados menores de dieciocho años, toda representación de éstos dedicados a actividades sexuales explícitas, reales o simuladas, o toda representación de sus partes genitales con fines primordialmente sexuales, o toda representación de dichos menores en que se emplee su voz o imagen, con los mismos fines.</p> <p>Art. 367. El que promoviere o facilitare la prostitución de menores de edad para satisfacer los deseos de otro, sufrirá la pena de presidio menor en su grado máximo.</p> <p>Si concurriere habitualidad, abuso de autoridad o de confianza o engaño, se impondrán las penas de presidio mayor en cualquiera de sus grados y multa de treinta y una a treinta y cinco unidades tributarias mensuales.</p> <p>Art. 374 bis. El que comercialice, importe, exporte, distribuya, difunda o exhiba material pornográfico, cualquiera sea su soporte, en cuya elaboración hayan sido utilizados menores de dieciocho años, será sancionado con la pena de presidio menor en su grado máximo.</p> <p>El que maliciosamente adquiera o almacene material pornográfico, cualquiera sea su soporte, en cuya elaboración hayan sido utilizados menores de dieciocho años, será castigado con presidio menor en su grado medio.</p> <p>Art. 374 ter. Las conductas de comercialización, distribución y exhibición señaladas en el artículo anterior, se entenderán cometidas en Chile cuando se realicen a través de un sistema de telecomunicaciones al que se tenga acceso desde territorio nacional.</p> <p><u>LEY N° 21.459 DE 2022 QUE ESTABLECE NORMAS SOBRE DELITOS INFORMÁTICOS</u></p> <p>TÍTULO I - DE LOS DELITOS INFORMÁTICOS Y SUS SANCIONES</p> <p>Artículo 10.- Circunstancias agravantes. Constituyen circunstancias agravantes de los delitos de que trata esta ley:</p> <p>(...)</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	2) Cometer el delito abusando de la vulnerabilidad, confianza o desconocimiento de niños, niñas, adolescentes o adultos mayores.
Title 4 – Offences related to infringements of copyright and related rights	
<p>Article 10 – Offences related to infringements of copyright and related rights</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 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><u>Ley N° 17.336 sobre Propiedad Intelectual</u></p> <p>TITULO I DERECHO DE AUTOR</p> <p>CAPITULO V Derecho patrimonial, su ejercicio y limitaciones</p> <p>Artículo 19.- Nadie podrá utilizar públicamente una obra del dominio privado sin haber obtenido la autorización expresa del titular del derecho de autor.</p> <p>La infracción de lo dispuesto en este artículo hará incurrir al o los responsables en las sanciones civiles y penales correspondientes.</p> <p>TITULO III DISPOSICIONES GENERALES</p> <p>CAPITULO II Contravenciones y sanciones</p> <p>Artículo 79.- Los delitos de violación de los derechos de autor o los derechos conexos serán penados con multas de dos a diez sueldos vitales anuales, escala A), del departamento de Santiago.</p> <p>Sin perjuicio de esa sanción, si la rendición de cuentas a que se refiere el artículo 50 falseare el número de ejemplares que se hubiere vendido efectivamente, el gerente o representante legal de la editorial será responsable del delito que sanciona el artículo 467 del Código Penal.</p>
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting	<u>CÓDIGO PENAL, 1874</u>

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, 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 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>TITULOS PRIMERO - DE LOS DELITOS Y DE LAS CIRCUNSTANCIAS QUE EXIMEN DE RESPONSABILIDAD CRIMINAL, LA ATENÚAN O LA AGRAVAN.</p> <p>§1 De los delitos</p> <p>Artículo 7º- Son punibles, no sólo el crimen o simple delito consumado, sino el frustrado y la tentativa.</p> <p>Hay crimen o simple delito frustrado cuando el delincuente pone de su parte todo lo necesario para que el crimen o simple delito se consuma y esto no se verifica por causas independientes de su voluntad.</p> <p>Hay tentativa cuando el culpable da principio a la ejecución del crimen o simple delito por hechos directos, pero faltan uno o más para su complemento.</p> <p>Artículo 8º.- La conspiración y proposición para cometer un crimen o un simple delito, sólo son punibles en los casos en que la ley las pena especialmente.</p> <p>La conspiración existe cuando dos o más personas se conciertan para la ejecución del crimen o simple delito.</p> <p>La proposición se verifica cuando el que ha resuelto cometer un crimen o un simple delito, propone su ejecución a otra u otras personas.</p> <p>Exime de toda pena por la conspiración o proposición para cometer un crimen o un simple delito, el desistimiento de la ejecución de éstos antes de principiar a ponerlos por obra y de iniciarse procedimiento judicial contra el culpable, con tal que denuncie a la autoridad pública el plan y sus circunstancias.</p> <p><u>LEY Nº 21.459 DE 2022 QUE ESTABLECE NORMAS SOBRE DELITOS INFORMÁTICOS</u></p> <p>TÍTULO I - DE LOS DELITOS INFORMÁTICOS Y SUS SANCIONES</p> <p>Artículo 7º.- Fraude informático.</p> <p>(...)</p> <p>Para los efectos de este artículo se considerará también autor al que, conociendo o no pudiendo menos que conocer la ilicitud de la conducta descrita en el inciso primero, facilita los medios con que se comete el delito.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>Article 12 – Corporate liability</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"> a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. <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><u>CÓDIGO PROCESAL PENAL, 2000</u> Libro Primero Disposiciones generales Título III Acción penal Artículo 58.- Responsabilidad penal. La acción penal, fuere pública o privada, no puede entablarse sino contra las personas responsables del delito.</p> <p>La responsabilidad penal sólo puede hacerse efectiva en las personas naturales. Por las personas jurídicas responden los que hubieren intervenido en el acto punible, sin perjuicio de la responsabilidad civil que las afectare.</p> <p><u>LEY 20.393 QUE ESTABLECE LA RESPONSABILIDAD PENAL DE LAS PERSONAS JURIDICAS EN LOS DELITOS QUE INDICA</u></p> <p><u>LEY N° 21.459 DE 2022 QUE ESTABLECE NORMAS SOBRE DELITOS INFORMÁTICOS</u></p> <p>TÍTULO III - DISPOSICIONES FINALES Artículo 21.- Modifícase la ley N° 20.393, que establece la responsabilidad penal de las personas jurídicas en los delitos de lavado de activos, financiamiento del terrorismo y delitos de cohecho que indica, en el siguiente sentido:</p> <ul style="list-style-type: none"> 1) Intercálase, en el inciso primero del artículo 1, a continuación de la expresión "N° 18.314", la expresión ", en el Título I de la ley que sanciona delitos informáticos". 2) Intercálase, en el inciso primero del artículo 15, entre "Código Penal," y "y en el artículo 8°", la expresión "en el Título I de la ley que sanciona delitos informáticos".
<p>Article 13 – Sanctions and measures</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>Section 2 – Procedural law</p>	
<p>Article 14 – Scope of procedural provisions</p>	<p><u>CÓDIGO PROCESAL PENAL, 2000</u></p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<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"> a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. <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 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> <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, <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>Libro Primero Disposiciones generales</p> <p>Título II Actividad procesal</p> <p>Párrafo 2º Comunicaciones entre autoridades</p> <p>Art. 19.- Requerimientos de información, contenido y formalidades. Todas las autoridades y órganos del Estado deberán realizar las diligencias y proporcionar, sin demora, la información que les requirieren el ministerio público y los tribunales con competencia penal. El requerimiento contendrá la fecha y lugar de expedición, los antecedentes necesarios para su cumplimiento, el plazo que se otorgare para que se llevare a efecto y la determinación del fiscal o tribunal requirente.</p> <p>Con todo, tratándose de informaciones o documentos que en virtud de la ley tuvieren carácter secreto, el requerimiento se atenderá observando las prescripciones de la ley respectiva, si las hubiere, y, en caso contrario, adoptándose las precauciones que aseguraren que la información no será divulgada.</p> <p>Si la autoridad requerida retardare el envío de los antecedentes solicitados o se negare a enviarlos, a pretexto de su carácter secreto o reservado y el fiscal estimare indispensable la realización de la actuación, remitirá los antecedentes al fiscal regional quien, si compartiere esa apreciación, solicitará a la Corte de Apelaciones respectiva que, previo informe de la autoridad de que se tratare, recabado por la vía que considerare más rápida, resuelva la controversia. La Corte adoptará esta decisión en cuenta. Si fuere el tribunal el que requiriere la información, formulará dicha solicitud directamente ante la Corte de Apelaciones.</p> <p>Si la razón invocada por la autoridad requerida para no enviar los antecedentes solicitados fuere que su publicidad pudiere afectar la seguridad nacional, la cuestión deberá ser resuelta por la Corte Suprema.</p> <p>Aun cuando la Corte llamada a resolver la controversia rechazare el requerimiento del fiscal, por compartir el juicio de la autoridad a la que se hubieren requerido los antecedentes, podrá ordenar que se suministren al ministerio público o al tribunal los datos que le parecieren necesarios para la adopción de decisiones relativas a la investigación o para el pronunciamiento de resoluciones judiciales. Las resoluciones que los ministros de Corte pronunciaren para resolver estas materias no los inhabilitarán para conocer, en su caso, los recursos que se dedujeren en la causa de que se tratare.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>Art. 20.- Solicitudes entre tribunales. Cuando un tribunal debiere requerir de otro la realización de una diligencia dentro del territorio jurisdiccional de éste, le dirigirá directamente la solicitud, sin más menciones que la indicación de los antecedentes necesarios para la cabal comprensión de la solicitud y las demás expresadas en el inciso primero del artículo anterior.</p> <p>Si el tribunal requerido rechazare el cumplimiento del trámite o diligencia indicado en la solicitud, o si transcurriere el plazo fijado para su cumplimiento sin que éste se produjere, el tribunal requirente podrá dirigirse directamente al superior jerárquico del primero para que ordene, agilice o gestione directamente la petición.</p>
<p>Article 15 – Conditions and safeguards</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>Proceso legal (Arts. 42 and 43 Código de Procedimiento Penal; Arts. 1º and 2º. Código Procesal Penal, 2000 ; Art. 21. Constitución Política de Chile)</p> <p>Derecho a no ser citado, arrestado, detenido, puesto en prisión preventiva, separado del hogar o arraigado (Art. 42 bis Código de Procedimiento Penal)</p> <p>El derecho a la libertad personal y a la seguridad individual (Art. 19 Constitución Política de Chile)</p> <p>Derechos del acusado (Art. 67 Código de Procedimiento Penal; Arts. 4, 7, 8, 9 y 10 Código Procesal Penal, 2000)</p> <p>Derechos de las víctimas en los procesos penales (Art. 6º. Código procesal penal, 2000)</p> <p>El respeto a la vida privada y pública y al honor del individuo y su familia (Art. 19 numeral 4 Constitución Política de Chile)</p> <p>La inviolabilidad del domicilio y todas las formas de comunicación privada (Art. 19 numeral 5º. Constitución Política de Chile).</p>
<p>Article 16 – Expedited preservation of stored computer data</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,</p>	<p>LEY N° 21.459 DE 2022 QUE ESTABLECE NORMAS SOBRE DELITOS INFORMÁTICOS</p> <p>TÍTULO III - DISPOSICIONES FINALES</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>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> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>Artículo 18.- Modifícase el Código Procesal Penal en el siguiente sentido:</p> <p>1) Agrégase el siguiente artículo 218 bis, nuevo:</p> <p>“Artículo 218 bis.- Preservación provisoria de datos informáticos. El Ministerio Público con ocasión de una investigación penal podrá requerir, a cualquier proveedor de servicio, la conservación o protección de datos informáticos o informaciones concretas incluidas en un sistema informático, que se encuentren a su disposición hasta que se obtenga la respectiva autorización judicial para su entrega. Los datos se conservarán durante un período de 90 días, prorrogable una sola vez, hasta que se autorice la entrega o se cumplan 180 días. La empresa requerida estará obligada a prestar su colaboración y guardar secreto del desarrollo de esta diligencia.”.</p>
<p>Article 17 – Expedited preservation and partial disclosure of traffic data</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> <p>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</p> <p>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.</p> <p>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>Article 18 – Production order</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:</p> <p>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</p> <p>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.</p> <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> <p>a the type of communication service used, the technical provisions taken thereto and the period of service;</p> <p>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;</p> <p>c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.</p>	<p><u>LEY N° 21.459 DE 2022 QUE ESTABLECE NORMAS SOBRE DELITOS INFORMÁTICOS</u></p> <p>TÍTULO II DEL PROCEDIMIENTO</p> <p>Artículo 11.- Sin perjuicio de las reglas contenidas en el Código Procesal Penal, las investigaciones a que dieren lugar los delitos previstos en esta ley también podrán iniciarse por querrela del Ministro del Interior y Seguridad Pública, de los delegados presidenciales regionales y de los delegados presidenciales provinciales, cuando las conductas señaladas en esta ley interrumpieren el normal funcionamiento de un servicio de utilidad pública.</p> <p>Artículo 12.- Cuando la investigación de los delitos contemplados en los artículos 1º, 2º, 3º, 4º, 5º y 7º de esta ley lo hiciere imprescindible y existieren fundadas sospechas basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión de algunos de los delitos contemplados en los preceptos precedentemente señalados, el juez de garantía, a petición del Ministerio Público, quien deberá presentar informe previo detallado respecto de los hechos y la posible participación, podrá ordenar la realización de las técnicas previstas y reguladas en los artículos 222 a 226 del Código Procesal Penal, conforme lo disponen dichas normas.</p> <p>La orden que disponga la realización de estas técnicas deberá indicar circunstanciadamente el nombre real o alias y dirección física o electrónica del afectado por la medida y señalar el tipo y la duración de la misma. El juez podrá prorrogar la duración de esta orden, para lo cual deberá examinar cada vez la concurrencia de los requisitos previstos en el inciso precedente.</p> <p>De igual forma, cumpliéndose los requisitos establecidos en el inciso anterior, el juez de garantía, a petición del Ministerio Público, podrá ordenar a funcionarios policiales actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación, con el fin de esclarecer los hechos tipificados como delitos en esta ley, establecer la identidad y participación de personas determinadas en la comisión de los mismos, impedirlos o comprobarlos. El referido agente encubierto en línea podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido, pudiendo obtener también imágenes y grabaciones de las referidas comunicaciones. No obstará a la consumación de los delitos que se pesquisen el hecho de que hayan participado en su investigación agentes encubiertos. El agente encubierto en sus actuaciones estará exento de responsabilidad criminal por aquellos delitos en que deba incurrir o que no haya</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>podido impedir, siempre que sean consecuencia necesaria del desarrollo de la investigación y guarden la debida proporcionalidad con la finalidad de la misma.</p> <p>Artículo 13.- Sin perjuicio de las reglas generales, caerán especialmente en comiso los instrumentos de los delitos penados en esta ley, los efectos que de ellos provengan y las utilidades que hubieren originado, cualquiera que sea su naturaleza jurídica.</p> <p>Cuando por cualquier circunstancia no sea posible decomisar estas especies, se podrá aplicar el comiso a una suma de dinero equivalente a su valor, respecto de los responsables del delito. Si por la naturaleza de la información contenida en las especies, estas no pueden ser enajenadas a terceros, se podrá ordenar la destrucción total o parcial de los instrumentos del delito y los efectos que de ellos provengan.</p> <p>Artículo 14.- Sin perjuicio de las reglas generales, los antecedentes de investigación que se encuentren en formato electrónico y estén contenidos en documentos electrónicos o sistemas informáticos o que correspondan a datos informáticos, serán tratados en conformidad a los estándares definidos para su preservación o custodia en el procedimiento respectivo, de acuerdo a las instrucciones generales que al efecto dicte el Fiscal Nacional.</p>
<p>Article 19 – Search and seizure of stored computer data</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"> a a computer system or part of it and computer data stored therein; <p>and</p> <ul style="list-style-type: none"> b a computer-data storage medium in which computer data may be stored <p>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><u>CÓDIGO PROCESAL PENAL, 2000</u></p> <p>LIBRO SEGUNDO PROCEDIMIENTO ORDINARIO TÍTULO I ETAPA DE INVESTIGACIÓN</p> <p>PÁRRAFO 3º ACTUACIONES DE LA INVESTIGACIÓN</p> <p>Artículo 187.- Objetos, documentos e instrumentos.</p> <p>Los objetos, documentos e instrumentos de cualquier clase que parecieren haber servido o haber estado destinados a la comisión del hecho investigado, o los que de él provinieren, o los que pudieren servir como medios de prueba, así como los que se encontraren en el sitio del suceso a que se refiere la letra c) del artículo 83, serán recogidos, identificados y conservados bajo sello. En todo caso, se levantará un registro de la diligencia, de acuerdo con las normas generales.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<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"> a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. <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 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>Si los objetos, documentos e instrumentos se encontraran en poder del imputado o de otra persona, se procederá a su incautación, de conformidad a lo dispuesto en este Título. Con todo, tratándose de objetos, documentos e instrumentos que fueren hallados en poder del imputado respecto de quien se practicare detención en ejercicio de la facultad prevista en el artículo 83 letra b) o se encontraran en el sitio del suceso, se podrá proceder a su incautación en forma inmediata.</p> <p>Artículo 217.- Incautación de objetos y documentos. Los objetos y documentos relacionados con el hecho investigado, los que pudieren ser objeto de la pena de comiso y aquellos que pudieren servir como medios de prueba, serán incautados, previa orden judicial librada a petición del fiscal, cuando la persona en cuyo poder se encontraran no los entregare voluntariamente, o si el requerimiento de entrega voluntaria pudiere poner en peligro el éxito de la investigación.</p> <p>Si los objetos y documentos se encontraran en poder de una persona distinta del imputado, en lugar de ordenar la incautación, o bien con anterioridad a ello, el juez podrá apercibirla para que los entregue. Regirán, en tal caso, los medios de coerción previstos para los testigos. Con todo, dicho apercibimiento no podrá ordenarse respecto de las personas a quienes la ley reconoce la facultad de no prestar declaración.</p> <p>Cuando existieren antecedentes que permitieren presumir suficientemente que los objetos y documentos se encuentran en un lugar de aquellos a que alude el artículo 205 se procederá de conformidad a lo allí prescrito.</p>
<p>Article 20 – Real-time collection of traffic data</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"> a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: <ul style="list-style-type: none"> i to collect or record through the application of technical means on the territory of that Party; or 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. 	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<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 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>Article 21 – Interception of content data</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 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><u>CÓDIGO PENAL, 1874</u></p> <p>TÍTULO SÉPTIMO CRÍMENES Y DELITOS CONTRA EL ORDEN DE LAS FAMILIAS CONTRA LA MORALIDAD PÚBLICA Y CONTRA LA INTEGRIDAD SEXUAL</p> <p>§ VII.Disposiciones comunes a los dos párrafos anteriores</p> <p>Art. 369 ter. Cuando existieren sospechas fundadas de que una persona o una organización delictiva hubiere cometido o preparado la comisión de alguno de los delitos previstos en los artículos 366 quinquies, 367, 367 ter, 374 bis, inciso primero, y 374 ter, y la investigación lo hiciera imprescindible, el tribunal, a petición del Ministerio Público, podrá autorizar la interceptación o grabación de las telecomunicaciones de esa persona o de quienes integren dicha organización, la fotografía, filmación u otros medios de reproducción de imágenes conducentes al esclarecimiento de los hechos y la grabación de comunicaciones. En lo demás, se estará íntegramente a lo dispuesto en los artículos 222 a 225 del Código Procesal Penal.</p> <p>Igualmente, bajo los mismos supuestos previstos en el inciso precedente, podrá el tribunal, a petición del Ministerio Público, autorizar la intervención de agentes encubiertos. Mediando igual autorización y con el objeto exclusivo de facilitar la labor de estos agentes, los organismos policiales pertinentes podrán mantener un registro reservado de producciones del carácter investigado. Asimismo, podrán tener lugar entregas vigiladas de material respecto de la investigación de hechos que se instigaren o materializaren a través del intercambio de dichos elementos, en cualquier soporte.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>La actuación de los agentes encubiertos y las entregas vigiladas serán plenamente aplicables al caso en que la actuación de los agentes o el traslado o circulación de producciones se desarrolle a través de un sistema de telecomunicaciones.</p> <p>Los agentes encubiertos, el secreto de sus actuaciones, registros o documentos y las entregas vigiladas se regirán por las disposiciones de la ley N° 20.000.</p>
Section 3 – Jurisdiction	
<p>Article 22 – Jurisdiction</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> <ol style="list-style-type: none"> in its territory; or on board a ship flying the flag of that Party; or on board an aircraft registered under the laws of that Party; or 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>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><u>CÓDIGO PENAL, 1874.</u> LIBRO PRIMERO TÍTULO PRIMERO - DE LOS DELITOS Y DE LAS CIRCUNSTANCIAS QUE EXIMEN DE RESPONSABILIDAD CRIMINAL, LA ATENUAN O LA AGRAVAN § I. De los delitos.</p> <p>Art. 5. La ley penal chilena es obligatoria para todos los habitantes de la República, incluso los extranjeros. Los delitos cometidos dentro del mar territorial o adyacente quedan sometidos a las prescripciones de este Código.</p> <p>Art. 6. Los crímenes o simples delitos perpetrados fuera del territorio de la República por chilenos o por extranjeros, no serán castigados en Chile sino en los casos determinados por la ley.</p> <p>Es posible la aplicación extraterritorial de la ley penal de acuerdo a lo establecido en el Código Orgánico de Tribunales.</p>
Chapter III – International co-operation	
Article 24 – Extradition	<p><u>CÓDIGO PROCESAL PENAL, 2000</u> Libro Cuarto Procedimientos especiales y ejecución</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<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 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>Título VI - Extradición Párrafo 2º - Extradición pasiva Artículo 440.- Procedencia de la extradición pasiva. Cuando un país extranjero solicitare a Chile la extradición de individuos que se encontraren en el territorio nacional y que en el país requirente estuvieren imputados de un delito o condenados a una pena privativa de libertad de duración superior a un año, el Ministerio de Relaciones Exteriores remitirá la petición y sus antecedentes a la Corte Suprema.</p> <p>Artículo 443.- Representación del Estado requirente. El ministerio público representará el interés del Estado requirente en el procedimiento de extradición pasiva, lo que no obstará al cumplimiento de lo dispuesto en su ley orgánica constitucional.</p> <p>Artículo 449.- Fallo de la extradición pasiva. El tribunal concederá la extradición si estimare comprobada la existencia de las siguientes circunstancias: a) La identidad de la persona cuya extradición se solicitare; b) Que el delito que se le imputare o aquél por el cual se le hubiere condenado sea de aquellos que autorizan la extradición según los tratados vigentes o, a falta de éstos, en conformidad con los principios de derecho internacional, y c) Que de los antecedentes del procedimiento pudiere presumirse que en Chile se deduciría acusación en contra del imputado por los hechos que se le atribuyen.</p> <p>La sentencia correspondiente se dictará, por escrito, dentro de quinto día de finalizada la audiencia.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<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>Article 25 – General principles relating to mutual assistance</p> <p>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>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</p>	<p><u>CÓDIGO PROCESAL PENAL, 2000</u></p> <p>Libro Primero Disposiciones generales</p> <p>Título II Actividad procesal</p> <p>Párrafo 2º Comunicaciones entre autoridades</p> <p>Artículo 20 bis. Tramitación de solicitudes de asistencia internacional. Las solicitudes de autoridades competentes de país extranjero para que se practiquen diligencias en Chile serán remitidas directamente al Ministerio Público, el que solicitará la intervención del juez de garantía del lugar en que deban practicarse, cuando la naturaleza de las diligencias lo hagan necesario de acuerdo con las disposiciones de la ley chilena.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>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>Article 26 – Spontaneous information</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> <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>Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements</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</p>	

BUDAPEST CONVENTION**DOMESTIC LEGISLATION**

the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

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.

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.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

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.

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.

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.

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.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<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, requests made under this paragraph are to be addressed to its central authority.</p>	
<p>Article 28 – Confidentiality and limitation on use</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> <p>a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or</p> <p>b not used for investigations or proceedings other than those stated in the request.</p> <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>	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>Article 29 – Expedited preservation of stored computer data</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">a the authority seeking the preservation;b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;c the stored computer data to be preserved and its relationship to the offence;d any available information identifying the custodian of the stored computer data or the location of the computer system;e the necessity of the preservation; andf 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>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> <ul style="list-style-type: none">a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, orb the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests.	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<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>	
<p>Article 30 – Expedited disclosure of preserved traffic data</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> <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>Article 31 – Mutual assistance regarding accessing of stored computer data</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>	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or</p> <p>b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.</p>	
<p>Article 32 – Trans-border access to stored computer data with consent or where publicly available</p> <p>A Party may, without the authorisation of another Party:</p> <p>a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or</p> <p>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 voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.</p>	
<p>Article 33 – Mutual assistance in the real-time collection of traffic data</p> <p>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.</p> <p>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>Article 34 – Mutual assistance regarding the interception of content data</p> <p>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>Article 35 – 24/7 Network</p> <p>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</p>	<p>Para estos efectos el Ministerio Público a través de la Unidad de Cooperación Internacional y Extradiciones es el punto de contacto 24X7. Las solicitudes pueden dirigirse al correo electrónico uciex@minpublico.cl.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>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:</p> <p>a the provision of technical advice;</p> <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>El punto de contacto puede ejecutar todas las solicitudes establecidas en el artículo 35 del Convenio.</p> <p>Respecto del numeral 1 punto c, ello dependerá del tipo de solicitud, probablemente algunas solicitudes descritas deben ser solicitadas por solicitud de asistencia internacional.</p> <p>2. b. El Ministerio Público tiene la calidad de Autoridad Central, Autoridad Competente y punto de contacto 24x7.</p>
<p>Article 42 – Reservations</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>	