# VENEZUELA

# Cybercrime legislation

## Domestic equivalent to the provisions of the Budapest Convention

## Table of contents

[reference to the provisions of the Budapest Convention]

*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.*

**www.coe.int/cybercrime**

**COUNCIL OF EUROPE**

**CONSEIL DE L'EUROPE**

| State: | |
|---|---|
| **Signature of the Budapest Convention:** | N/A |
| **Ratification/accession:** | N/A |

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| **Chapter I – Use of terms** | |

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| **Article 1 – "Computer system", "computer data", "service provider", "traffic data":** <br> For the purposes of this Convention: <br> 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; <br><br> 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*;* <br> c "service provider" means: <br><br> i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and <br> ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; <br> 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 | **Ley especial contra los delitos informáticos – 2001** <br><br> **Artículo 2. Definiciones** <br> A efectos de la presente Ley, y cumpliendo con lo previsto en el artículo 9 de la Constitución de la República Bolivariana de Venezuela, se entiende por: <br> b) **Sistema**: cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia para cumplir una serie de funciones específicas, así como la combinación de dos o más componentes interrelacionados, organizados en un paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas. <br> c) **Data (datos)**: hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por seres humanos o por medios automáticos y a los cuales se les asigna o se les puede asignar un significado. <br> f) **Computador**: dispositivo o unidad funcional que acepta data, la procesa de acuerdo con un programa guardado y genera resultados, incluidas operaciones aritméticas o lógicas. <br> g) **Hardware**: equipos o dispositivos físicos considerados en forma independiente de su capacidad o función, que conforman un computador o sus componentes periféricos, de manera que pueden incluir herramientas, implementos, instrumentos, conexiones, ensamblajes, componentes y partes. <br> h) **Firmware**: programa o segmento de programa incorporado de manera permanente en algún componente del hardware. <br> i) **Procesamiento de datos o de información**: realización sistemática de operaciones sobre data o sobre información, tales como manejo, fusión, organización o cómputo. |

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| **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** | |
| **Article 2 – Illegal access**<br>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. | **Ley especial contra los delitos informáticos – 2001**<br><br>**Artículo 6. Acceso indebido**<br>Toda persona que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias. |
| **Article 3 – Illegal interception**<br>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. | **Ley especial contra los delitos informáticos – 2001**<br><br>**Artículo 11. Espionaje informático**<br>Toda persona que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualesquiera de sus componentes […]. La pena se aumentará […] si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro. El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas, como consecuencia de la revelación de las informaciones de carácter reservado.<br><br>**Artículo 21. Violación de la privacidad de las comunicaciones**<br>Toda persona que mediante el uso de tecnologías de información acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. |

| | |
|---|---|
| **Article 4 – Data interference**<br>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.<br>2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm. | **Ley especial contra los delitos informáticos – 2001**<br><br>**Artículo 20. Violación de la privacidad de la data o información de carácter personal**<br>Toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.<br><br>**Artículo 22. Revelación indebida de data o información de carácter personal**<br>Quien revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos 6 por alguno de los medios indicados en los artículos 20 y 21, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro, o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad. |
| **Article 5 – System interference**<br>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 | **Ley especial contra los delitos informáticos – 2001**<br><br>**Artículo 7. Sabotaje o daño a sistemas**<br>Todo aquel que con intención destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualesquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.<br>Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualesquiera de sus componentes.<br>La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión intencional, por cualquier medio, de un virus o programa análogo.<br><br>**Artículo 9. Acceso indebido o sabotaje a sistemas protegidos** |

| | |
|---|---|
| | Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad, cuando los hechos allí previstos o sus efectos recaigan sobre cualesquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas. |
| **Article 6 – Misuse of devices**<br>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:<br>a the production, sale, procurement for use, import, distribution or otherwise making available of:<br>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;<br>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,<br>with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and<br><br>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.<br><br>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.<br><br>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. | **Ley especial contra los delitos informáticos – 2001**<br><br>**Artículo 10. Posesión de equipos o prestación de servicios de sabotaje**<br>Quien importe, fabrique, distribuya, venda o utilice equipos, dispositivos o programas, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.<br><br>**Artículo 19. Posesión de equipo para falsificaciones**<br>Todo aquel que sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de tarjetas inteligentes o de instrumentos destinados a los mismos fines, o cualquier equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o instrumentos, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.<br><br>**Artículo 27. Agravantes**<br>La pena correspondiente a los delitos previstos en la presente Ley se incrementará entre un tercio y la mitad: 1. Si para la realización del hecho se hubiere hecho uso de alguna contraseña ajena indebidamente obtenida, quitada, retenida o que se hubiere perdido. 2. Si el hecho hubiere sido cometido mediante el abuso de la posición de acceso a data o información reservada, o al conocimiento privilegiado de contraseñas, en razón del ejercicio de un cargo o función. |

| Title 2 – Computer-related offences | |
|---|---|
| **Article 7 – Computer-related forgery**<br>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. | **Ley especial contra los delitos informáticos – 2001**<br><br>**Artículo 12. Falsificación de documentos**<br>Quien, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias. Cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio, la pena se aumentará entre un tercio y la mitad. El aumento será de la mitad a dos tercios si del hecho resultare un perjuicio para otro.<br><br>**Artículo 18. Provisión indebida de bienes o servicios**<br>Todo aquel que, a sabiendas de que una tarjeta inteligente o instrumento destinado a los mismos fines, se encuentra vencido, revocado; se haya indebidamente obtenido, retenido, falsificado, alterado; provea a quien los presente de dinero, efectos, bienes o servicios, o cualquier otra cosa de valor económico será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. |
| **Article 8 – Computer-related fraud**<br>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:<br><br>    a      any input, alteration, deletion or suppression of computer data;<br><br>    b      any interference with the functioning of a computer system,<br><br>with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person. | **Ley especial contra los delitos informáticos – 2001**<br><br>**Artículo 13. Hurto**<br>Quien a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.<br><br>**Artículo 14. Fraude**<br>Todo aquel que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes, o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas, que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias. |

**Artículo 15. Obtención indebida de bienes o servicios.**
Quien, sin autorización para portarlos, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice indebidamente tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio; o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida, será castigado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

**Artículo 16. Manejo fraudulento de tarjetas inteligentes o instrumentos análogos.**
Toda persona que por cualquier medio cree, capture, grabe, copie, altere, duplique o elimine la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; o la persona que, mediante cualquier uso indebido de tecnologías de información, cree, capture, duplique o altere la data o información en un sistema, con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos, será penada con prisión de cinco a diez años y multa de quinientas a mil unidades tributarias. 5 En la misma pena incurrirá quien, sin haber tomado parte en los hechos anteriores, adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de tarjetas inteligentes o instrumentos destinados al mismo fin, o de la data o información contenidas en ellos o en un sistema.

| | |
|---|---|
| **Title 3 – Content-related offences** | |

**Article 9 – Offences related to child pornography**
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:
    a    producing child pornography for the purpose of its distribution through a computer system;
    b    offering or making available child pornography through a computer system;
    c    distributing or transmitting child pornography through a computer system;

**Ley especial contra los delitos informáticos – 2001**

**Artículo 23. Difusión o exhibición de material pornográfico**
Todo aquel que, por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

|  |  |
|---|---|
| d  procuring child pornography through a computer system for oneself or for another person;<br>e  possessing child pornography in a computer system or on a computer-data storage medium.<br><br>2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:<br>  a  a minor engaged in sexually explicit conduct;<br>  b  a person appearing to be a minor engaged in sexually explicit conduct;<br>  c  realistic images representing a minor engaged in sexually explicit conduct<br><br>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.<br><br>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. | **Artículo 24. Exhibición pornográfica de niños o adolescentes**<br>Toda persona que por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos, será penada con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.<br><br>**CÓDIGO PENAL**<br><br>**TITULO VIII.** De los delitos contra las buenas costumbres y buen orden de las familias<br>**CAPITULO I.** De la violación, de la seducción, de la prostitución o corrupción de menores y de los ultrajes al pudor<br>**Artículos 375-383.** |

| Title 4 – Offences related to infringements of copyright and related rights | |
|---|---|

|  |  |
|---|---|
| **Article 10 – Offences related to infringements of copyright and related rights**<br>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.<br>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 | **Ley especial contra los delitos informáticos – 2001**<br><br>**Artículo 25. Apropiación de propiedad intelectual**<br>Quien sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias.<br><br>**Artículo 26. Oferta engañosa**<br>Toda persona que ofrezca, comercialice o provea de bienes o servicios, mediante el uso de tecnologías de información, y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta, de modo que pueda resultar algún perjuicio para los consumidores, será sancionada con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias, sin perjuicio de la comisión de un delito más grave. |

| | |
|---|---|
| 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.<br>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. | |

| Title 5 – Ancillary liability and sanctions | |
|---|---|

| | |
|---|---|
| **Article 11 – Attempt and aiding or abetting**<br>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.<br>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.<br>3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article. | |
| **Article 12 – Corporate liability**<br>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:<br>    a    a power of representation of the legal person;<br>    b    an authority to take decisions on behalf of the legal person;<br>    c    an authority to exercise control within the legal person.<br>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 | **Ley especial contra los delitos informáticos – 2001**<br><br>**Artículo 5. Responsabilidad de las personas jurídicas**<br>Cuando los delitos previstos en esta Ley fuesen cometidos por los gerentes, administradores, directores o dependientes de una persona jurídica, actuando en su nombre o representación, éstos responderán de acuerdo con su participación culpable. La persona jurídica será sancionada en los términos previstos en esta Ley, en los casos en que el hecho punible haya sido cometido por decisión de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en su interés exclusivo o preferente. |

| | |
|---|---|
| offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.<br>3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.<br>4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence. | |
| **Article 13 – Sanctions and measures**<br>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.<br>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. | **Ley especial contra los delitos informáticos – 2001**<br><br>**Artículo 4. Sanciones**<br>Las sanciones por los delitos previstos en esta Ley serán principales y accesorias. Las sanciones principales concurrirán con las penas accesorias y ambas podrán también concurrir entre sí, de acuerdo con las circunstancias particulares del delito del cual se trate, en los términos indicados en la presente Ley. |

## Section 2 – Procedural law

**Article 14 – Scope of procedural provisions**
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.
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:
     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.
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.
  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:<br>    i     is being operated for the benefit of a closed group of users, and<br>    ii    does not employ public communications networks and is not connected with another computer system, whether public or private,<br>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 | |
| **Article 15 – Conditions and safeguards**<br>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.<br>2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.<br><br>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. | **CONSTITUCIÓN**<br><br>**Artículo 19.** El Estado garantizará a toda persona, conforme al principio de progresividad y sin discriminación alguna, el goce y ejercicio irrenunciable, indivisible e interdependiente de los derechos humanos. Su respeto y garantía son obligatorios para los órganos del Poder Público de conformidad con la Constitución, los tratados sobre derechos humanos suscritos y ratificados por la República y las leyes que los desarrollen.<br><br>**Artículo 21.** Todas las personas son iguales ante la ley […].<br><br>**Artículo 26.** Toda persona tiene derecho de acceso a los órganos de administración de justicia para hacer valer sus derechos e intereses, incluso los colectivos o difusos, a la tutela efectiva de los mismos y a obtener con prontitud la decisión correspondiente. El Estado garantizará una justicia gratuita, accesible, imparcial, idónea, transparente, autónoma, independiente, responsable, equitativa y expedita, sin dilaciones indebidas, sin formalismos o reposiciones inútiles.<br><br>**Artículo 27.** Toda persona tiene derecho a ser amparada por los tribunales en el goce y ejercicio de los derechos y garantías constitucionales, aun de aquellos inherentes a la persona que no figuren expresamente en esta Constitución o en los instrumentos internacionales sobre derechos humanos.<br><br>**Artículo 28.** Toda persona tiene derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga |

de los mismos y su finalidad, y a solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley.

**Artículo 29.** El Estado estará obligado a investigar y sancionar legalmente los delitos contra los derechos humanos cometidos por sus autoridades. Las acciones para sancionar los delitos de lesa humanidad, violaciones graves a los derechos humanos y los crímenes de guerra son imprescriptibles. Las violaciones de derechos humanos y los delitos de lesa humanidad serán investigados y juzgados por los tribunales ordinarios. Dichos delitos quedan excluidos de los beneficios que puedan conllevar su impunidad, incluidos el indulto y la amnistía.

**Artículo 31.** Toda persona tiene derecho, en los términos establecidos por los tratados, pactos y convenciones sobre derechos humanos ratificados por la República, a dirigir peticiones o quejas ante los órganos internacionales creados para tales fines, con el objeto de solicitar el amparo a sus derechos humanos.

**Artículo 48.** Se garantiza el secreto e inviolabilidad de las comunicaciones privadas en todas sus formas. No podrán ser interferidas sino por orden de un tribunal competente, con el cumplimiento de las disposiciones legales y preservándose el secreto de lo privado que no guarde relación con el correspondiente proceso.

**Artículo 49.** El debido proceso se aplicará a todas las actuaciones judiciales y administrativas y, en consecuencia: 1. La defensa y la asistencia jurídica son derechos inviolables en todo estado y grado de la investigación y del proceso. Toda persona tiene derecho a ser notificada de los cargos por los cuales se le investiga, de acceder a las pruebas y de disponer del tiempo y de los medios adecuados para ejercer su defensa. Serán nulas las pruebas obtenidas mediante violación del debido proceso. Toda persona declarada culpable tiene derecho a recurrir del fallo, con las excepciones establecidas en esta Constitución y la ley. 2. Toda persona se presume inocente mientras no se pruebe lo contrario. 3. Toda persona tiene derecho a ser oída en cualquier clase de proceso, con las debidas garantías y dentro del plazo razonable determinado legalmente, por un tribunal competente, independiente e imparcial establecido con anterioridad. Quien no hable castellano o no pueda comunicarse de manera verbal, tiene derecho a un

intérprete. 4. Toda persona tiene derecho a ser juzgada por sus jueces naturales en las jurisdicciones ordinarias, o especiales, con las garantías establecidas en esta Constitución y en la ley. Ninguna persona podrá ser sometida a juicio sin conocer la identidad de quien la juzga, ni podrá ser procesada por tribunales de excepción o por comisiones creadas para tal efecto. 5. Ninguna persona podrá ser obligada a confesarse culpable o declarar contra sí misma, su cónyuge, concubino o concubina, o pariente dentro del cuarto grado de consanguinidad y segundo de afinidad. La confesión solamente será válida si fuere hecha sin coacción de ninguna naturaleza. 6. Ninguna persona podrá ser sancionada por actos u omisiones que no fueren previstos como delitos, faltas o infracciones en leyes preexistentes. 7. Ninguna persona podrá ser sometida a juicio por los mismos hechos en virtud de los cuales hubiese sido juzgada anteriormente. 8. Toda persona podrá solicitar del Estado el restablecimiento o reparación de la situación jurídica lesionada por error judicial, retardo u omisión injustificados. Queda a salvo el derecho del o de la particular de exigir la responsabilidad personal del magistrado o magistrada, juez o jueza y del Estado, y de actuar contra éstos o éstas.

**Artículo 51.** Toda persona tiene el derecho de representar o dirigir peticiones ante cualquier autoridad, funcionario público o funcionaria pública sobre los asuntos que sean de la competencia de éstos, y a obtener oportuna y adecuada respuesta. Quienes violen este derecho serán sancionados conforme a la ley, pudiendo ser destituidos del cargo respectivo.

**Artículo 60.** Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación.

**CÓDIGO ORGÁNICO PROCESAL PENAL**

**Artículo 220. Autorización**
En los casos señalados en el artículo anterior, el Ministerio Público, solicitará razonadamente al juez de control del lugar donde se realizará la intervención, la correspondiente autorización con expreso señalamiento del delito que se investiga, el tiempo de duración, que no excederá de treinta días, los medios técnicos a ser empleados y el sitio o lugar desde donde se efectuará. Podrán acordarse prórrogas sucesivas mediante el mismo procedimiento y por lapsos iguales, medios, lugares y demás extremos pertinentes. El órgano de policía de investigaciones penales, en casos de necesidad y urgencia, que deberán ser debidamente justificados, podrá solicitar directamente al juez de control la

| | respectiva orden, previa autorización, por cualquier medio, del Ministerio Público, que deberá constar en la solicitud, en la cual, además, se harán los señalamientos a que se contrae el aparte anterior. La decisión del juez que acuerde la intervención, deberá ser motivada y en la misma se harán constar todos los extremos de éste artículo.<br><br>**Artículo 221. Uso de la grabación**<br>Toda grabación autorizada conforme a lo previsto en este Código y en leyes especiales, será de uso exclusivo de las autoridades encargadas de la investigación y enjuiciamiento, quedando en consecuencia prohibido divulgar la información obtenida |
|---|---|
| **Article 16 – Expedited preservation of stored computer data**<br>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.<br><br>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.<br><br>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.<br><br>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. | |
| **Article 17 – Expedited preservation and partial disclosure of traffic data**<br>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: | |

| | |
|---|---|
| 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<br>  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.<br><br>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. | |
| **Article 18 – Production order**<br>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:<br>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<br>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.<br><br>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.<br>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:<br>    a    the type of communication service used, the technical provisions taken thereto and the period of service;<br>    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;<br>    c    any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement. | |
| **Article 19 – Search and seizure of stored computer data**<br>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: | **CÓDIGO ORGÁNICO PROCESAL PENAL**<br><br>**Artículo 218. Incautación** |

| | |
|---|---|
| a    a computer system or part of it and computer data stored therein; and<br>b    a computer-data storage medium in which computer data may be stored<br>        in its territory.<br>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.<br>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:<br>a    seize or similarly secure a computer system or part of it or a computer-data storage medium;<br>b    make and retain a copy of those computer data;<br>c    maintain the integrity of the relevant stored computer data;<br>d    render inaccessible or remove those computer data in the accessed computer system.<br>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.<br>5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. | En el curso de la investigación de un hecho delictivo, el Ministerio Público, con autorización del juez de control podrá incautar la correspondencia y otros documentos que se presuman emanados del autor del hecho punible o dirigidos por él, y que puedan guardar relación con los hechos investigados. De igual modo, podrá disponer la incautación de documentos, títulos, valores y cantidades de dinero disponibles en cuentas bancarias o en caja de seguridad de los bancos o en poder de terceros, cuando existan fundamentos razonables para deducir que ellos guardan relación con el hecho delictivo investigado. En los supuestos previstos en éste artículo, el órgano de policía de investigaciones penales, en casos de necesidad y urgencia, podrá solicitar directamente al juez de control la respectiva orden, previa autorización, por cualquier medio, del Ministerio Público, la cual deberá constar en la solicitud. |
| **Article 20 – Real-time collection of traffic data**<br>1    Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:<br>a    collect or record through the application of technical means on the territory of that Party, and<br>b    compel a service provider, within its existing technical capability:<br>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. | |
| 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. | |
| 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. | |
| 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. | |
| **Article 21 – Interception of content data** | **CÓDIGO ORGÁNICO PROCESAL PENAL** |
| 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: | |
| a collect or record through the application of technical means on the territory of that Party, and | **Artículo 219. Interceptación o grabación de comunicaciones privadas** |
| b compel a service provider, within its existing technical capability: | Podrá disponerse igualmente, conforme a la ley, la interceptación o grabación de comunicaciones privadas, sean éstas ambientales, telefónicas o realizadas por cualquier otro medio, cuyo contenido se transcribirá y agregará a las actuaciones. |
| i to collect or record through the application of technical means on the territory of that Party, or | Se conservarán las fuentes originales de grabación, asegurando su inalterabilidad y su posterior identificación. A los efectos del presente artículo, se entienden por comunicaciones ambientales aquellas que se realizan personalmente o en forma directa, sin ningún instrumento o dispositivo de que se valgan los interlocutores. |
| 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. | |
| 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. | |
| 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. | |

| | |
|---|---|
| 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. | |

## Section 3 – Jurisdiction

| | |
|---|---|
| **Article 22 – Jurisdiction**<br>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:<br>    a    in its territory; or<br>    b    on board a ship flying the flag of that Party; or<br>    c    on board an aircraft registered under the laws of that Party; or<br>    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.<br>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.<br>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.<br>4    This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.<br>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. | **Ley especial contra los delitos informáticos – 2001**<br><br>**Artículo 3. Extraterritorialidad**<br>Cuando alguno de los delitos previstos en la presente Ley se cometa fuera del territorio de la República, el sujeto activo quedará sometido a sus disposiciones si dentro del territorio de la República se hubieren producido efectos del hecho punible, y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros. |

## Chapter III – International co-operation

| | |
|---|---|
| **Article 24 – Extradition**<br>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 | **CONSTITUCIÓN** |

concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

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.

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.

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.

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.

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.

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.

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.

---

**Artículo 69.** La República Bolivariana de Venezuela reconoce y garantiza el derecho de asilo y refugio. Se prohíbe la extradición de venezolanos y venezolanas.

**Artículo 156.** Es de la competencia del Poder Público Nacional:
4. La naturalización, la admisión, la extradición y expulsión de extranjeros o extranjeras.

**Artículo 271.** En ningún caso podrá ser negada la extradición de los extranjeros o extranjeras responsables de los delitos de deslegitimación de capitales, drogas, delincuencia organizada internacional, hechos contra el patrimonio público de otros Estados y contra los derechos humanos. No prescribirán las acciones judiciales dirigidas a sancionar los delitos contra los derechos humanos, o contra el patrimonio público o el tráfico de estupefacientes. Asimismo, previa decisión judicial, serán confiscados los bienes provenientes de las actividades relacionadas con tales delitos.

## CÓDIGO PENAL

**Artículo 6.**- La extradición de un venezolano no podrá concederse por ningún motivo; pero deberá ser enjuiciado en Venezuela, a solicitud de parte agraviada o del Ministerio Público, si el delito que se le Imputa mereciere pena por la ley venezolana. La extradición de un extranjero no podrá tampoco concederse por delitos políticos ni por infracciones conexas con estos delitos, ni por ningún hecho que no esté calificado de delito por la ley venezolana.
La extradición de un extranjero por delitos comunes no podrá acordarse sino por la autoridad competente, de conformidad con los trámites y requisitos establecidos al efecto por los Tratados Internacionales suscritos por Venezuela y que estén en vigor y, a falta de estos, por las leyes venezolanas. No se acordara la extradición de un extranjero acusado de un delito que tenga asignada en la legislación del país requirente la pena de muerte o una pena perpetua.
En todo caso, hecha la solicitud de extradición, toca al Ejecutivo Nacional, según el mérito de los comprobantes que se acompañen, resolver sobre la detención preventiva del extranjero, antes de pasar el asunto al Tribunal Supremo de justicia.

## CÓDIGO ORGÁNICO PROCESAL PENAL

**TITULO VII.** Del Procedimiento de Extradición

| | |
|---|---|
| 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 | **Artículos 391-399**. |
| **Article 25 – General principles relating to mutual assistance**<br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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. | |
| **Article 26 – Spontaneous information** | |

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.

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.

**Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements**
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.
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.
 b    The central authorities shall communicate directly with each other;
 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;
 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.

b    Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

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.

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.

| | |
|---|---|
| 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. | |
| **Article 28 – Confidentiality and limitation on use**<br>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.<br>2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:<br>a    kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or<br>b    not used for investigations or proceedings other than those stated in the request.<br>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.<br>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. | |
| **Article 29 – Expedited preservation of stored computer data**<br>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.<br>2    A request for preservation made under paragraph 1 shall specify:<br>    a    the authority seeking the preservation;<br>    b    the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;<br>    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; and | |
| 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. | |
| 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. | |
| 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. | |
| 5    In addition, a request for preservation may only be refused 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    the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. | |
| 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. | |
| 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. | |
| **Article 30 – Expedited disclosure of preserved traffic data** | |

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.

2 Disclosure of traffic data under paragraph 1 may only be withheld 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 the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

**Article 31 – Mutual assistance regarding accessing of stored computer data**

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.

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.

3 The request shall be responded to on an expedited basis where:

a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

**Article 32 – Trans-border access to stored computer data with consent or where publicly available**

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

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.

**Article 33 – Mutual assistance in the real-time collection of traffic data**

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.

**Article 34 – Mutual assistance regarding the interception of content data**
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.

**Article 35 – 24/7 Network**
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;
b      the preservation of data pursuant to Articles 29 and 30;
c      the collection of evidence, the provision of legal information, and locating of suspects.
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.

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.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

| | |
|---|---|
| **Article 42 – Reservations**<br>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. | |