Cameroon

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 08 February 2022

[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	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	**Law N° 2010/012 of 21 December 2010 relating to cybersecurity and cybercriminality in Cameroon** **Part 1, General Provisions Section 4**. Within the meaning of this law and its implementing instruments, the following definitions shall be accepted: (1) Illegal access : unauthorized intentional access to all or part of an electronic communication network, an information system or terminal equipment; (25) Content**:** all information relating to data belonging to individuals or legal entities, transmitted or received through electronic communication networks and information systems; ((41) Data: representation of facts, information or concepts in a form suitable for processing by terminal equipment, including a program allowing it to perform a function;(43) Traffic data: data relating to an electronic communication indicating the origin, destination, route, time, date, size and duration or type of underlying service; (46) Provider of electronic communication services : natural person or corporate body providing services consisting entirely or mainly in the provision of electronic communications; (49) Unlawful interception: illegal or unauthorized access to the data of an electronic communication's network, an information system or a terminal equipment; (51) Intentional intrusion: intentional and unauthorized access to an electronic communication's network or an information system with the intent of causing harm or deriving economic, financial ,industrial , or security benefit or sovereignty;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	72) Information system: devices or group of interconnected or related devices performing, by itself or by one or many of its components, automatic data processing, in line with a program; Definitions related to electronic communication can be found in several other legislative texts: ▸ Law N° 2010/013 of 21 December 2010 and its amendment of April 2015 (in French only);Directive No. 07/08-UEAC-133-CM-18 of 19 December 19 2008 on the Legal Framework for the Protection of Users of Electronic Communications Networks and Services within CEMAC (in French only);
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 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.	**Law N° 2010/012 of 21 December 2010 relating to cybersecurity and cybercriminality in Cameroon** **Part III Cybercriminality, Chapter II Offences and Penalties, Section 65.** (1) Whoever, without any right or authorization, proceeds by electronic means to intercept or not during transmission, intended for, whether or not within an electronic communication network, an information system or a terminal device shall be punished with imprisonment for from 05 (five) to 10 (ten) years or a fine of from 5.000.000 (five million) to 10.000.000 (ten million) CFA francs or both such fine and imprisonment. (2) Any unauthorized access to all or part of an electronic communication network or an information system or a terminal device shall be liable to the same sanctions in accordance with Subsection 1 above.(3) The penalties provided for in Subsection 1 above, shall be doubled where unauthorized access violates the integrity, confidentiality, availability of the electronic communication network or the information system. (4) Whoever, without any right, allows access to an electronic communication network or an information system as an intellectual challenge shall be punished in accordance with Subsection 1 above.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Section 69. Whoever accesses all or part of an electronic communication network, an information system or terminal equipment without authorization and in violation of security measures in order to obtain information or data relating to an information system connected to another information system shall be punished with imprisonment for from 05 (five) to 10 (ten) years or a fine of from 10 000 000 (ten million) to 100,000,000 (one hundred thousand million) CFA francs or both of such fine and imprisonment.
Article 3 – Illegal interception 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.	**Law N° 2010/012 of 21 December 2010 relating to cybersecurity and cybercriminality in Cameroon** Part III Cybercriminality, Chapter II Offences and Penalities **Section 65.** (1) Whoever, without any right or authorization, proceeds by electronic means to intercept or not during transmission, intended for, whether or not within an electronic communication network, an information system or a terminal device shall be punished with imprisonment for from 05 (five) to 10 (ten) years or a fine of from 5.000.000 (five million) to 10.000.000 (ten million) CFA francs or both such fine and imprisonment.
Article 4 – Data interference 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. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Law N° 2010/012 of 21 December 2010 relating to cybersecurity and cybercriminality in Cameroon** Part III Cybercriminality, Chapter II Offences and Penalties **Section 71.** Whoever without permission, introduces data into an information system or an electronic communication network in order to delete or change the data contained therein, shall be punished with imprisonment for from 02 (two) to 05 (five) years and a fine of from 1 000 000 (one million) to 25 000 000 (twenty five million) FCFA francs. **Section 72.**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Whoever without authorization and for financial gain, uses any means to introduce, alter, erase or delete electronic data such as to cause damage to someone else's property shall be punished with the penalties provided for in Section 66 above. **Section 86.** (2) Whoever causes serious disturbance or disruption on an electronic communication, or whoever uses electronic communication network or an information system with the intention of breaching the integrity of the data, shall be punishable with the penalties provided for in Subsection 1 above. **Section 87.** Authors of the offences provided for in Section 86 above shall be punishable with the following additional penalties: - seizure, in accordance with the conditions laid down in Section 35 of the Penal Code, of any object used or intended to be used to commit the offence or considered to be the proceed thereof, with the exception of objects likely to be restituted; - prohibition, in accordance with the conditions laid down in Section 36 of the Penal Code, for a period of not less than 05 (five) years from the holding of a public office or carrying out a socio-professional activity where the offence was committed in the discharge or during the discharge of one's duties; - closure, in accordance with the conditions laid down in \ Section 34 of the Penal Code, for a period of not less than 05 (five) years, of establishments or of one or more of the establishments of the company that was used to commit the offence; - barring, for a period of not less than 05 (five) years, from public contracts.
Article 5 – System interference 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	**Law N° 2010/012 of 21 December 2010 relating to cybersecurity and cybercriminality in Cameroon** Part III Cybercriminality, Chapter II Offences and Penalties **Section 66.** (1) Whoever causes disturbance or disruption of the functioning of an electronic communication network or a terminal device by introducing, transmitting, destroying, erasing, deteriorating, altering, deleting data or rendering data

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	inaccessible shall be punished with imprisonment for from 02 (two) to 05 (five) years or a fine of from 1.000.000 (one million) to 2.000.000 (two million) CFA francs or both of such fine an imprisonment. **Section 67.** Causing serious disturbance or disruption of the functioning of an electronic communication network or terminal equipment by introducing, transmitting, changing, deleting or altering data shall constitute a breach of the integrity of an electronic communication network or an information system and shall be punishable in accordance with Section 66 above. **Section 68.** (1) Whoever fraudulently gains access or remains in all or part of an electronic communication network or an information system by transmitting, destroying, causing serious disturbance or disruption to the functioning of the said system or network shall be punished with imprisonment for from 05 (five) to 10 (ten) years or a fine of from 10.000.000 (ten million) to 50.000.000 (fifty million) CFA francs or both of such fine and imprisonment. (2) The same penalties provided for in subsection 1 above shall be doubled where such acts result in the deletion or change to the data contained in the information system or a change in its functioning.
Article 6 – Misuse of devices 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: a the production, sale, procurement for use, import, distribution or otherwise making available of: 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; 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	**Law N° 2010/012 of 21 December 2010 relating to cybersecurity and cybercriminality in Cameroon** Part III Cybercriminality, Chapter II Offences and Penalities **Section 66.** (2) Whoever uses the deceptive or undesirable software to carry out operations on a user's terminal device without first informing the latter of the true character of the operation which the said software is likely to damage shall be punishable with the same penalties **Section 86.**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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. 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.	(1) The penalties provided for in section 71 above shall apply against whoever imports, keeps, offers, transfers, sells or provides, in any form whatsoever, a computer program, a password, an access code or any similar computer data designed and/or specially adapted to facilitate access to all or part of an electronic communication or an information system.
Title 2 – Computer-related offences	
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.	**Law N° 2010/012 of 21 December 2010 relating to cybersecurity and cybercriminality in Cameroon** Part III Cybercriminality, Chapter II Offences and Penalties **Section 71.** Whoever without permission, introduces data into an information system or an electronic communication network in order to delete or change the data contained therein, shall be punished with imprisonment for from 02 (two) to 05 (five) years and a fine of from 1 000 000 (one million) to 25 000 000 (twenty five million) FCFA francs. **Section 72.** Whoever without authorization and for financial gain, uses any means to introduce, alter, erase or delete electronic data such as to cause damage to someone else's property shall be punished with the penalties provided for in

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Section 66 above. **Section 86.** (2) Whoever causes serious disturbance or disruption on an electronic communication, or whoever uses electronic communication network or an information system with the intention of breaching the integrity of the data, shall be punishable with the penalties provided for in Subsection 1 above.
Article 8 – Computer-related fraud 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: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**Law N° 2010/012 of 21 December 2010 relating to cybersecurity and cybercriminality in Cameroon** Part III Cybercriminality, Chapter II Offences and Penalities **Section 73.** (1) Whoever uses an information system or a counterfeit communication network to falsify payment, credit or cash withdrawal card or uses or attempts to use, in full knowledge of the facts, a counterfeit or falsified payment, credit or withdrawal card shall be punished with imprisonment for from 02 (two) to 10 (ten) years and a fine of from 25,000,000 (twenty five million) to 50 000 000 (fifty million) CFA francs or both of such fine and imprisonment.
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; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium.	**Law N° 2010/012 of 21 December 2010 relating to cybersecurity and cybercriminality in Cameroon** Part III Cybercriminality, Chapter II Offences and Penalities **Section 76.** Whoever uses electronic communications or an information system to design, carry or publish a child pornography message or a message likely to seriously injure the selfrespect of a child shall be punished with imprisonment for from 5 (five) years to 10 (ten) years or a fine of from 5,000,000 (five million) to 10,000,000 CFA francs or both of such fine and imprisonment.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 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. 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.	**Section 80.** (1) Whoever for consideration or free of charge, uses electronic communications or an information system to publish, attach, record or transmit an image showing acts of pedophilia or a minor shall be punished with imprisonment for from 01 (one) to 05 (five) years or a fine of from 5 000 000 (five million) to 10,000,000 (ten million) CFA francs or both of.such fine and imprisonment. (2) Whoever uses electronic means whatsoever to offer, provide or publish, import or export an image or picture portraying pedophilia shall be punished with the penalties provided in Subsection 3 above. (3) Whoever keeps an image or picture portraying pedophilia in an electronic communication network or an information system shall be punished with imprisonment for from 01 (one) to 05 (five) years or a fine of from 5,000,000 (five million) to 10,000,000 (ten million) CFA francs or both of such fine and imprisonment. (4) The penalties provided for in Subsection 3 above shall be doubled where an electronic communication network is used to publish an image or picture of a minor. (5) The provisions of this section shall equally apply to pornographic pictures showing minors. Section 81. (1) The following offences shall be punishable with the penalties provided for in Section 82 below where they are committed using an electronic communication network or an information system: - offering, producing, providing child pornography for publication; - acquiring child pornography for oneself or for someone else using an information system; - where adult persons make sexual proposals to minors below 15 years old or to a person having the features of a minor; - dissemination or transmission of child pornography using an information system. (2) Child pornography shall be any act which visually presents:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	- a minor involved in sexually explicit behavior; - any person with the physical features of a minor involved in sexually explicit acts; - real images of a minor involved in sexually explicit acts. **Section 82.** The penalties provided for in Section 79 above shall be doubled for whoever uses electronic communication devices to commit or attempt to commit any act of indecency on a minor less than 15 (fifteen) years old
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 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. 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. 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	Law No. 2000/011 of December 19, 2000 on Copyright and Neighbouring Rights, Part VI, Infringement, Penalties and Procedures **Section 80.** The following shall constitute forgery: (a) any exploitation of a literary or artistic work done in violation of this law, through performance, reproduction, transformation or distribution by any means whatsoever; (b) any reproduction, communication or supply to the public through sale, exchange, rental of a recording, a phonogram, videogram, undertaken without the authorization of the performer, phonogram or videogram producer, or the audiovisual communication firm, where such authorization is required; (c) any infringement of moral rights through violation of the right of disclosure, the right of authorship or the right to respect of a literary or artistic work; (d) any infringement of the right of authorship and the right of integrity of a performance. **Section 81.** (1) The following shall also be considered forgery: (a) the importation, exportation, sale or putting up for sale of forged objects; (b) the importation or exportation of phonograms or videograms produced without the authorization of their performer or producer, where such authorization is required;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	(c) manufacturing or importing, with the intention of selling or renting or setting up equipment, material, device or instrument entirely or partially designed to fraudulently record programmes broadcast where such programmes are reserved for a specific public that receives them in return for a fee paid to their operator or his legal representatives; (d) the fraudulent neutralization of effective technical measures used by owners of copyrights or neighbouring rights to protect their works against unauthorized acts; (e) allowing the irregular reproduction or performance in one's establishment of works protected by this law; (f) failure to pay or unjustified late payment of a fee as provided for by this law; (g) carrying out the following acts, knowingly or, for civil sanctions, having good reason to believe that this act will lead to, enable, facilitate or conceal infringement of a right provided for in this law:— unauthorized removal or alteration of any electronic information relating to the copyright regime;— the distribution, importation for distribution, unauthorized communication of originals or copies of works, performances, videograms, phonograms, programmes, while knowing that the electronic information relating to the copyright regime has been removed or altered without authorization. (2) "Information on copyright regime" shall mean information that helps to identify the work, performance, videogram, phonogram or programme, or information on the conditions of use of such productions and any number or code representing such information where one of these elements of information is attached to a copy of a production or is linked to the communication of a production to the public. **Section 82.** (1) The offences referred to in Sections 80 and 81 [shall] be punishable by imprisonment of from 5 (five) to 10 (ten) years or a fine of from 500,000 to 10,000,000 CFA francs or both such imprisonment and fine. (2) The penalties provided for in this section shall be doubled where the offender is a partner of the owner of the infringed right.
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	
Article 12 – Corporate liability 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: 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. 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. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	**Law N° 2010/012 of 21 December 2010 relating to cybersecurity and cybercriminality in Cameroon** Part III Cybercriminality, Chapter II Offences and Penalities **Section 64.** (1) Corporate bodies shall be criminally liable for offences committed on their account by their management structures. (2) The criminal liability of corporate bodies shall not preclude that of natural persons who commit such offences or are accomplices. (3) The penalties to be meted out on defaulting corporate bodies shall be fines of from 5 000 000 (five million) to 50 000 000 (fifty million) CFA francs. (4) The penalties provided for in Subsection 3 above, notwithstanding one of the following other penalties may equally be meted out on corporate bodies: **-** dissolution in case of a crime or felony punishable with respect to natural persons with imprisonment of 03 (three) years and above and where the corporate body has departed from its declared object to aid and abet the incriminating acts; - definitive prohibition or temporary prohibition for a period not less than 05 (five) years, from directly or indirectly carrying out one or more professional or corporate activities;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	- temporary closure for a period of not less than 05 (five) years under the conditions laid down in Section 34 of the Penal Code of the establishments or one or more establishments of the company that was used to commit the incriminating acts; - barring from bidding for public contracts either definitively or for a period of not less than 05 (five) years; - barring from offering for public issues either definitively or for a period of not less than 05 (five) years; - prohibition for a period of not less than 05 (five) years from issuing cheques other than those to be used by the drawer to withdraw money from the drawer or certified checks or from using payment cards; - seizure of the device used or intended to be used in committing the offence or the proceeds of the offence; - publication or dissemination of the decision taken either through the print media or through any electronic means of communication to the public.
Article 13 – Sanctions and measures 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. 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.	**Law N° 2010/012 of 21 December 2010 relating to cybersecurity and cybercriminality in Cameroon** Part III Cybercriminality, Chapter II Offences and Penalities Sanctions are set out under the article criminalising each offence.
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:	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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: 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, 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 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.	**Law No. 96-06 of 18 January 1996 to amend the Constitution of 2 June 1972** (Constitution of the Republic of Cameroon) Preamble We, people of Cameroon, Declare that the human person, without distinction as to race, religion, sex or belief, possesses inalienable and sacred rights; Affirm our attachment to the fundamental freedoms enshrined in the Universal Declaration of Human Rights, the Charter of the United Nations and The African

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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.	Charter on Human and Peoples' Rights, and all duly ratified international conventions relating thereto, in particular, to the following principles: - all persons shall have equal rights and obligations. The State shall provide all its citizens with the conditions necessary for their development; (..) - freedom and security shall be guaranteed to each individual, subject to respect for the rights of others and the higher interests of the State; (..) - the privacy of all correspondence is inviolate. No interference may be allowed except by virtue of decisions emanating from the Judicial Power; - no person may be compelled to do what the law does not prescribe; - no person may be prosecuted, arrested or detained except in the cases and according to the manner determined by law; - the law may not have retrospective effect. No person may be judged and punished, except by virtue of a law enacted and published before the offence committed; - The law shall ensure the right of every person to a fair hearing before the courts; - every accused person is presumed innocent until found guilty during a hearing conducted in strict compliance with the rights of defence; (..) - the freedom of communication, of expression, of the press, of assembly, of association, and of trade unionism, as well as the right to strike shall be guaranteed under the conditions fixed by law; Part One, The State and Sovereignty, Article one 2) The Republic of Cameroon shall be a decentralized unitary State. It shall be one and indivisible, secular, democratic and dedicated to social service. It shall recognize and protect traditional values that conform to democratic principles, human rights and the law. It shall ensure the equality of all citizens before the law. **Law N° 2010/012 of 21 December 2010 relating to cybersecurity and cybercriminality in Cameroon** Part 1 General Provisions Section 1: This law governs the security framework of electronic communication networks and information systems, defines and punishes offences related to the use of information and communication technologies in Cameroon. Accordingly, it seeks notably to: - build trust in electronic communication networks and information systems;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	- establish the legal regime of digital evidence, security, cryptography and electronic certification activities; - protect basic human rights, in particular the right to human dignity, honour and respect of privacy, as well as the legitimate interests of corporate bodies. CHAPTER IX Protection of electronic communication networks, Information systems and personal privacy, IV-Protection of privacy **Section 41.** Every individual shall have the right to the protection of their privacy. Judges may take any protective measures notably, sequestration or seizure to avoid or end the invasion of privacy.
Article 16 – Expedited preservation of stored computer data 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. 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. 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. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 17 – Expedited preservation and partial disclosure of traffic data 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 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. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: 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 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. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 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: a the type of communication service used, the technical provisions taken thereto and the period of service; 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;	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 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. 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: 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. 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. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Law N° 2010/012 of 21 December 2010 relating to cybersecurity and cybercriminality in Cameroon** Part III Cybercriminality, Chapter I Procedural law provisions **Section 53.** (1) Cybercriminal-related searches may concern data. Such data may be physical material or copies made in the presence of persons taking part in the search. (2) When a copy of seized data is made, it may, for security reasons be destroyed on the instruction of the State Counsel. (3) On the approval of State Counsel, only objects, documents and data used as evidence may be kept under seal. (4) Persons present during searches may be requested to provide information on any seized objects, document and data. **Section 54.** Searches and seizures shall be carried out in accordance with the provisions of the Criminal Procedure Code, taking into account the loss of validity of evidence. **Section 55.** (1) When it appears that data seized or obtained in the course of an investigation or inquiry has been the subject of transformation, thus hindering clear access or is likely to impair the information it contains, the State Counsel, the Examining Judge or the Court may request any qualified natural person or corporate body to perform technical operations to obtain the clear version of the said data. (2) When a cryptographic means has been employed, judicial authorities may request the secret conversion of the encrypted text. Part 11, Chapter IX Protection of electronic communication networks, Information systems and personal privacy, 1- Protection of electronic communication networks

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Section 25. (1) Network operators and electronic communication service providers shall be bound to conserve traffic connection data for a period of 10 (ten) years. (2) Network operators and electronic communication service providers shall set up mechanisms for monitoring the traffic data of their networks. Such data may be accessible in the course of judicial inquiries. (3) Network operators and electronic communication service providers shall be liable where the use of the data referred to in Sub-section 2 above undermines the individual liberties of users.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: 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: 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	**Law N° 2010/012 of 21 December 2010 relating to cybersecurity and**

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 b compel a service provider, within its existing technical capability: 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, 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.	**cybercriminality in Cameroon** Part II, Chapter IX Protection of electronic communication networks, Information systems and personal privacy, V - Interception of electronic communication **Section 49.** Notwithstanding the provisions of the Criminal Procedure Code, in case of crimes or offences provided for hereunder, criminal investigation officers may intercept record or transcribe any electronic communication. **Section 50**. In the event of encoding, compressing or ciphering of data transmitted by electronic communication networks or electronic communication service providers, clear corresponding interceptions shall be provided to the services that requested them. **Section 51**. The personnel of electronic communication network operators or electronic communication service providers shall be bound to secrecy for any requests they receive.
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 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: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or 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.	**Law N° 2010/012 of 21 December 2010 relating to cybersecurity and cybercriminality in Cameroon** Part III Cybercriminality, Chapter I Procedural law provisions **Section 57.** (1) Cameroonian judicial authorities may set up a rogatory commission at, both the national and international level, any corporate body or natural person to search the elements of cybercrime offences of which at least one of the elements was committed on Cameroonian territory or which one of the offenders or accomplices resides on the said territory.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. 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.	(2) Subject to rules of reciprocity between Cameroon and foreign countries with which it has concluded a judicial cooperation agreement, rogatory commissions shall be executed in accordance with the provisions of the Criminal Procedure Code.
Chapter III – International co-operation	
Article 24 – Extradition 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. 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	Extradition is regulated in the Criminal Procedural Code (Arts. 635-675).

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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	
Article 25 – General principles relating to mutual assistance 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. 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.	**Law N° 2010/012 of 21 December 2010 relating to cybersecurity and cybercriminality in Cameroon** PART III CYBERCRIMINALITY, CHAPTER 1 PROCEDURAL LAW PROVISIONS **Section 59.** (1) For purposes of investigation or examination, the hearing or interrogation of a person and/or confrontation of several persons may be carried out on several locations on the national territory linked by electronic communication means that ensure the confidentiality of transmissions. A report shall be drawn up on the operations carried out in each location. Such operations may be subject to audiovisual and/or sound recording.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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. 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.	(2) According to the prevailing circumstances, their interpretation may be done by means of electronic communication in the course of a hearing, interrogation or confrontation. **(**3) The provisions of this Section shall equally be applicable for the concurrent implementation, on a location on the national territory or on a location situated outside the national territory, of mutual assistance requests from foreign judicial officers or acts of mutual assistance performed outside the national territory, at the request of Cameroonian judicial authorities. (4) Conditions for the implementation of this section shall be defined by regulation
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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	**Law N° 2010/012 of 21 December 2010 relating to cybersecurity and cybercriminality in Cameroon** Part IV Cybercriminality, Chapter II international and mutual judicial assistance **Section 91.** (1) Unless otherwise provided for by an international convention to which Cameroon is signatory, requests for judicial assistance from Cameroonian judicial officers to foreign judicial officers shall be sent through the Ministry in charge of External Relations. Enforcement documents shall be sent to the authorities of the requesting State through the same channel. (2) Requests for mutual judicial assistance from foreign authorities to Cameroonian judicial authorities must be presented through diplomatic channels by the foreign Government concerned. Enforcement documents shall be sent to the authorities of the requesting State through the same channel. (3) In case of emergency, requests for judicial assistance from Cameroonian or foreign authorities may be sent directly to the authorities of the requested State for enforcement. The enforcement documents shall be dispatched to the relevant State authorities under the same conditions (4) Subject to international conventions, request for mutual judicial assistance from foreign authorities to Cameroonian judicial authorities shall be subject to an opinion of foreign Government concerned. Such opinion shall be forwarded to the relevant judicial authorities through diplomatic channels. (5) In case of emergency, requests for mutual judicial assistance from foreign judicial authorities shall be forwarded to the State Counsel or Examining Magistrate with territorial jurisdiction.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(6) Where the State Counsel receives a request for mutual judicial assistance directly from authority, but which can only be enforced by the Examining Magistrate, he shall forward it to the latter for enforcement or refer to the General Prosecutor in the case provided for in section 94 below. (7) Before proceeding to enforce a request for mutual assistance forwarded directly to him, the Examining Magistrate shall immediately communicate same to the State Counsel for an opinion. **Section 92.** (1) Requests for mutual judicial assistance from foreign judicial officers shall be enforced by the State Counsel or Judicial Police Officers or Agents requested for this purpose by the said State Counsel. (2) The requests shall be enforced by the Examining Magistrate or Judicial Police officers acting on the rogatory commission of the Examining Magistrate where they require certain procedural measures which can be ordered or enforced only during a preliminary investigation. **Section 93** (1) Request for mutual judicial assistance from foreign judicial officers shall be enforced in accordance with the procedure laid down by the Criminal Procedure Code. (2) However, where the request for assistance so specifies, it shall be enforced in accordance with the procedure explicitly indicated by the relevant authorities of the requesting State, without such rules violating the rights of the parties or the procedural guarantees provided for by the Criminal Procedure Code. (3) Where the request for mutual assistance cannot be enforced in accordance with the requirements of the requesting Sate, the relevant Cameroonian authorities shall immediately inform the authorities of the requesting State of such impossibility and specify under what conditions the request may be enforced. (4) The relevant Cameroonian authorities and those of the requesting State may subsequently agree on the onward processing of the request, where necessary, by subjecting it to compliance with such conditions.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(5) Irregularity in the transmission of the request for judicial assistance shall not constitute grounds for nullity of actions undertaken in enforcing such a request. **Section 94.** (1) Where the enforcement of a request for judicial assistance from a foreign judicial authority is such as can breach public law and order or negatively affect the essential interests of the Nation, the State Counsel to whom the request is addressed or who is appraised thereof shall forward same to the General Prosecutor who shall transmit to the Minister in charge of Justice and where necessary, inform the State Counsel of such transmission. (2) Where the request is forwarded to the Minister in charge of Justice, he shall inform the requesting authority, where necessary, that it is not possible to totally or partially accede to the request. Such information shall be communicated to the judicial authority concerned and shall block the enforcement of the request for mutual judicial assistance or the return of the enforcement papers.
Article 28 – Confidentiality and limitation on use 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. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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. 2 A request for preservation made under paragraph 1 shall specify: 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; 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:	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	

Back to the Table of Contents