[Gambia (Republic of the)]

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 14 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:	

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	**Information and Communications Act (ICA, 2009)** CHAPTER I – PRELIMINARY, 2. Interpretation "service provider" means an operator; "operator" means a person who owns, operates or provides a regulated information and communications system or information and communications service; CHAPTER III – INFORMATION SOCIETY ISSUES, PART I – INTERPRETATION OF THIS CHAPTER, S.161 "computer system" means a device or combination of devices, including input and output devices, but excluding calculators which are not programmable, and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data that performs logic, arithmetic, data storage and retrieval, communication control and other functions;"data" means electronic representations of information in any form; "traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing in respect of that communication and includes data relating to the routing, duration or time of a communication; "access" in relation to any computer system, means instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources, of the computer system;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	"intercept" in relation to a function of a computer, includes listening to, or recording, a function of a computer, or acquiring the substance, its meaning or purport of that function; "modification" means a modification of the contents of a computer system by the operation of any function of that computer system or any other computer system as a result of which- (a) a programme or data held in the computer system is altered or erased; (b) a programme or data is added to its contents; or (c) an act occurs which impairs the normal operation of the computer system;
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.	**ICA, 2009** CHAPTER III – INFORMATION SOCIETY ISSUES, PART III - COMPUTER MISUSE AND CYBER CRIME, Unauthorized access to computer data163. (1) Subject to subsections (2) and (3), a person who causes a computer system to perform a function, knowing that the access he or she intends to secure is unauthorized, commits an offence and is liable on conviction to a fine of two hundred thousand dalasis or imprisonment for a term not exceeding five years, or to both the fine and imprisonment. (2) A person shall not be liable under subsection (1) where he or she- (a) is a person with a right to control the operation or use of the computer system and exercises such right in good faith; (b) has the express or implied consent of the person, empowered to authorise him or her, to have such an access; (c) has reasonable grounds to believe that he or she had the consent as specified in paragraph (b);

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(d) is acting pursuant to measures that can be taken under this Act; or (e) is acting in reliance of any statutory power arising under any enactment for the purpose of obtaining information, or of taking possession of, any document or other property. (3) An access by a person to a computer system is unauthorized where the person- (a) is not himself or herself entitled to control (b) does not have consent to access by him or herself of the kind in question from any person who is so entitled. (4) For the purposes of this section, it is immaterial that the unauthorized access is not directed at (a) any particular programme or data; (b) a programme or data of any kind; or (c) a programme or data held in any particular computer system. CHAPTER III – INFORMATION SOCIETY ISSUES, PART III - COMPUTER MISUSE AND CYBER CRIME, Access with intent to commit offences 164. (1) A person who causes a computer system to perform any function for the purpose of securing access to any programme or data held in any computer system, with intent to commit an offence under any other enactment, commits an offence and is liable on conviction to a fine of two hundred thousand dalasis or imprisonment for a term not exceeding five years, or to both the fine and imprisonment. (2) For the purposes of this section, it is immaterial that: (a) the access referred to in subsection (1) is authorized or unauthorized; (b) the further offence to which this section applies is committed at the same time when the access is secured or at any other time.
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	**ICA, 2009** CHAPTER III – INFORMATION SOCIETY ISSUES, PART III - COMPUTER MISUSE AND CYBER CRIME, Unauthorized access to and interception of computer service

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	165. (1) Subject to subsection (5), a person who, by any means, knowingly – (a) secures access to any computer system for the purpose of obtaining, directly or indirectly, any computer service; or (b) intercepts or causes to be intercepted, directly or indirectly, any function of, or any data within a computer system, commits an offence. (2) A person convicted for an offence under subsection (1) is liable on conviction, in the case of – (a) an individual, to a fine of two hundred thousand dalasis or imprisonment for a term not exceeding five years, or to both the fine and imprisonment; (b) a body corporate, to a fine of not less than five hundred thousand dalasis. (3) Where as a result of the commission of an offence under subsection (1), the operation of the computer system, is impaired, or data contained in the computer system is suppressed or modified, a person convicted of the offence is liable to a further fine of five hundred thousand dalasis. (4) For the purpose of this section, it is immaterial that the unauthorized access or interception is not directed at - (a) any particular programme or data; (b) a programme or data of any kind; or (c) a programme or data held in any particular computer system. (5) A person is not liable under subsection (1) if he or she- (a) has the express or implied consent of both the person who sent the data and the intended recipient of the data; or (b) is acting in reliance of any statutory power.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**ICA, 2009** CHAPTER III – INFORMATION SOCIETY ISSUES, PART III - COMPUTER MISUSE AND CYBER CRIME, Unauthorized modification of computer material166. (1) Subject to subsections (3) and (4), a person who, knowingly does an act which causes an unauthorized modification of data held in any computer system commits an offence and is liable on conviction in the case of- (a) an individual, to a fine of two hundred thousand dalasis or imprisonment for a term not exceeding five years, or to both the fine and imprisonment; (b) a body corporate, to a fine of not less than five hundred thousand dalasis. (2) Where as a result of the commission of an offence under this section (a) the operation of the computer system; (b) access to any program or data held in any computer; or (c) the operation of any program or the reliability of any data, is suppressed, modified or otherwise impaired, a person convicted for the offence is liable to a further fine of five hundred thousand dalasis. (3) A person is not liable under this section where he or she is acting (a) pursuant to measures that can be taken under this Act; or (b) in reliance of any other statutory power. (4) A modification is unauthorized if (a) the person whose act causes it is not himself or herself entitled to determine whether the modification should be made; and (b) he or she does not have consent to the modification from any person who is so entitled. (5) For the purposes of this section, it is immaterial whether an unauthorized modification or any intended effect of it, is permanent or merely temporary.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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	**ICA, 2009** CHAPTER III – INFORMATION SOCIETY ISSUES, PART III - COMPUTER MISUSE AND CYBER CRIME, Damaging or denying access to computer system167. (1) A person who, without lawful authority or lawful excuse, does an act which causes directly or indirectly- (a) a degradation, failure, interruption or obstruction of the operation of a computer system; or (b) a denial of access to, or impairment of any program or data stored in, the computer system, commits an offence. (2) A person who commits an offence under subsection (1) is liable on conviction, in the case of-(a) an individual, to a fine of two hundred thousand dalasis or imprisonment for a term not exceeding five years, or to both the fine and imprisonment; (b) a body corporate, to fine of not less than five hundred thousand dalasis.
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 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.	**ICA, 2009** CHAPTER III – INFORMATION SOCIETY ISSUES, PART III - COMPUTER MISUSE AND CYBER CRIME, Unlawful possession of devices and data 168. (1) A person who knowingly manufactures, sells, procures for use, imports, distributes or otherwise makes available, a computer system or any other device, designed or adapted primarily for the purpose of committing an offence under subsections (3) to (8), commits an offence. (2) A person who knowingly receives, or is in possession of, without sufficient excuse or justification, one or more of the devices mentioned in subsection (1) commits an offence. (3) A person who is found in possession of any data or programme with the intention that the data or programme be used, by the person himself or herself or another person, to commit or facilitate the commission of an offence under

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	this Act, commits an offence. (4) For the purposes of subsection (3), possession of any data or programme includes (a) having possession of computer system or data storage device that holds or contains the data or programme; (b) having possession of a document in which the data or programme is recorded; or (c) having control of data or programme that is in the possession of another person. (5) A person who commits an offence under this section is liable on conviction, in the case of (a) an individual, to a fine of two hundred thousand dalasis or imprisonment for a term not exceeding five years, or to both the fine and imprisonment; and (b) a body corporate, to a fine of not less than five hundred thousand dalasis. **ICA, 2009** CHAPTER III – INFORMATION SOCIETY ISSUES, PART III - COMPUTER MISUSE AND CYBER CRIME, Unlawful possession of devices and data 169. (1) A person who, knowingly discloses any password, access code, or any other means of gaining access to any program or data held in any computer system – (a) for any wrongful gain; (b) for any unlawful purpose; or (c) knowing that it is likely to cause prejudice to any person, commits an offence. (2) A person who commits an offence under subsection (1) is liable on conviction, in the case of- (a) an individual, to a fine of two hundred thousand dalasis or imprisonment for a term not exceeding five years, or to both the fine and imprisonment; (b) a body corporate, to a fine of not less than five hundred thousand

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	dalasis.
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.	**ICA, 2009** CHAPTER III – INFORMATION SOCIETY ISSUES, PART III - COMPUTER MISUSE AND CYBER CRIME, Unlawful possession of devices and data 173.(2) A person who performs any of the acts described in this Part for the purpose of obtaining any unlawful advantage by causing fake data to be produced with the intent that it be considered or acted on as if it were authentic, commits of an offence. (3) A person who commits an offence under this section is liable on conviction, in the case of (a) an individual, to a fine of two hundred thousand dalasis or imprisonment for a term not exceeding five years, or to both the fine and imprisonment; (b) a body corporate, to a fine of not less than five hundred thousand dalasis.
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.	**ICA, 2009** CHAPTER III – INFORMATION SOCIETY ISSUES, PART III - COMPUTER MISUSE AND CYBER CRIME, Unlawful possession of devices and data 173. (1) A person who performs or threatens to perform any of the acts described in this Part for the purpose of obtaining an unlawful proprietary advantage by undertaking to cease or desist from the act, or by undertaking to restore any damage caused as a result of those acts, commits of an offence. (3) A person who commits an offence under this section is liable on conviction, in the case of- (a) an individual, to a fine of two hundred thousand dalasis or imprisonment for a term not exceeding five years, or to both the fine and imprisonment; (b) a body corporate, to a fine of not less than five hundred thousand dalasis

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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.	**ICA, 2009** CHAPTER III– INFORMATION SOCIETY ISSUES, PART IV PROTECTION OF CHILDREN, Indecent photographs of children 174. (1) A person who - (a) takes or permits to be taken or to make, an indecent photograph or pseudo-photograph of a child; (b) distributes or shows an indecent photograph or a pseudo-photograph; (c) has in his or her possession an indecent photograph or pseudo-photographs, with a view to it being distributed or shown by himself or herself or any other person; or (d) publishes or causes to be published an advertisement likely to be understood as conveying that the advertiser distributes or shows the indecent photograph or a pseudo-photograph, or intends to do so, commits an offence and liable on conviction to imprisonment for life. (2) Where a person is charged with an offence under subsection (1)(b) or (c), it is a defence for the person to prove that he or she (a) had reasonable grounds for distributing or showing the photograph or pseudo-photograph or having them in his or her possession; and (b) had not himself or herself seen the photograph or pseudo-photograph and did not know, or had any cause to suspect, it to be indecent. (3) Where- (a) the impression conveyed by the pseudo-photograph is that the person shown is a child; or (b) the predominant impression conveyed is that the person shown is a child, notwithstanding that some of the physical characteristics shown are those of an adult, the pseudo-photograph shall be treated for all purposes of this Act as showing a child.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(4) The Court before which a person is convicted of an offence under this section may, in addition to any penalty imposed, order (a) the forfeiture of any apparatus, article or thing which is the subject matter of the offence or is used in connection with the commission of the offence; or (b) that the material subject matter of the offence be no longer stored on and made available through the computer system, or that the material be deleted. (5) An offence under this section shall be considered to be an extraditable crime for which extradition may be granted or obtained
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	**Copyright Act (CA), 2004** CHAPTER III-INFRINGEMENT AND ENFORCEMENT OF COPYRIGHT, Criminal sanctions 53. (1) A person who infringes a right protected under this Act wilfully or by gross negligence and for profitmaking purposes commits an offence and is liable on conviction to a fine of not more than five hundred thousand dalasis and imprisonment for a term of not more than three years or to both the fine and imprisonment. (2) The Court shall fix the amount of the fine, taking into particular account, the defendant's profits attributable to the infringement. (3) The Court may increase up to double the upper limit of the penalties specified in subsection (1), where the defendant has been convicted for a new act of infringement within five years of a previous conviction for an infringement. (4) The Court shall also apply the measures and remedies referred to in sections 51 and 52 in criminal proceedings, if no decision has yet been taken on those remedies in a civil proceeding,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	**Criminal code (CC), 1933 as amended in 2010** CHAPTER V, PARTIES to OFFENCES 23. Principal offenders When an offence is committed, each of the following offenders. persons is deemed to have taken part in committing the offence and to be guilty of the offence, and may be charged with actually committing it, that is to say— (c) every person who aids or abets another person in committing the offence; (d) any person who counsels or procures any other person to commit the offence. In the last-mentioned case he may be charged either with committing the offence or with counselling or procuring its commission. A conviction of counselling or procuring the commission of an offence entails the same consequences in all respects as a conviction of committing the offence. Any person who procures another to do or omit to do any act of such a nature that, if he had himself done the act or made the omission, the act or omission would have constituted an offence on his part, is guilty of an offence of the same kind, and is liable to the same punishment, as if he had himself done the act or made the omission; and he may be charged with doing the act or making the omission. 25. Counselling another to commit an offence (1) When a person counsels another to commit an offence, and an offence is actually committed after the counsel by the person to whom it is given, it is immaterial whether the offence actually committed is the same as that counselled or a different one, or whether the offence is committed in the way counselled or in a different way, provided in either case that the facts constituting the offence actually committed are a probable consequence of carrying out the counsel.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) The person who gave the counsel under subsection (1) is deemed to have counselled the other person to commit the offence actually committed by him or her. 26.Definition of accessories after the fact (1) A person who receives or assists another who is, to his or her knowledge, guilty of an offence, in order to enable him or her to escape punishment, is said to become an accessory after the fact to the offence. (2) A wife does not become an accessory after the fact to an offence of which her husband is guilty by receiving or assisting him in order to enable him to escape punishment, or by receiving or assisting, in her husband's presence and by his authority, another person who is guilty of an offence in the commission of which her husband has taken part, in order to enable that other person to escape punishment; nor does a husband become accessory after the fact to an offence of which his wife is guilty by receiving or assisting her in order to enable her to escape punishment. (3) A person who becomes an accessory after the fact to a felony commits a felony, and is liable on conviction, if no other punishment is provided, to imprisonment for a term of two years. A person who becomes an accessory after the fact to a misdemeanour commits a misdemeanour and is liable on conviction to imprisonment for a term of one year.
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	**ICA, 2009** **CHAPTER V – MISCELLANEOUS, Offences by body corporate** 248. (1) An offence committed by a body corporate is treated as committed by a person who, at the time the offence was committed, was- (a) a director, principal officer, general manager, secretary, or other similar officer of the company; or (b) acting or purporting to act in that capacity. (2) Subsection (1) does not apply to a person if- (a) the offence was committed without that person's consent or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	knowledge; and (b) the person has exercised all diligence to prevent the commission of the offence as ought to have been exercised having regard to the nature of the person's functions and all the circumstances.
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.	The CC contains a specific part on punishments (Chapter VI), which includes imprisonment, fines and compensation. For the sanctions and limits of the sanctions, please see above (pages 2 to 13).
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 **Criminal Procedure Code** **(CPC, as amended in 2005)** provides for certain powers and procedures relating to criminal investigations. Although there is no explicit mention on the application of the said powers and procedures to the cybercrime offences under ICA (2009), they should extend to the offences outlined above.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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.	**THE CONSTITUTION OF THE REPUBLIC OF THE GAMBIA, 1997 (as Amended to 2018)** Chapter IV, PROTECTION OF FUNDAMENTAL RIGHTS AND FREEDOMS, Art.17 Fundamental rights and freedoms (2) Every person in The Gambia, whatever his or her race, colour, gender, language, religion, political or other opinion, national or social origin, property, birth or other status, shall be entitled to the fundamental human rights and freedoms of the individual contained in this Chapter, but subject to respect for the rights and freedoms of others and for the public interest. Art. 23 Privacy (1) No person shall be subject to interference with the privacy of his or her home, correspondence or communications save as is in accordance with law and is necessary in a democratic society in the interests of national security, public safety of the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights and freedoms of others. (2) Searches of the person or the home of individuals shall only be justified (a) where these are authorised by a competent judicial authority;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(b) in cases where delay in obtaining such judicial authority carries with it the danger of prejudicing the objects of the search or the public interest and such procedures as are prescribed by an Act of the National Assembly to preclude abuse are properly satisfied. **ICA, 2009** CHAPTER II – REGULATION OF INFORMATION AND COMMUNICATION SYSTEMS AND SERVICES, Part XIII - Processing of Personal Data and Protection 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.	
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**CPC (1933 as last amended by Act No. 5 of 2005)** PART IV Provisions Relating to All Criminal Investigations, Searches and Search Warrants 93. Search of premises (1) When a police officer has reason to believe that material evidence can be obtained in connection with an offence for which an arrest has been made or authorised, a police officer may search the dwelling or place of business of the person so arrested or of the person for whom the warrant of arrest has been issued and may take possession of anything which might reasonably be used as evidence in a criminal proceeding. [Act No. 1 of 1964.] (2)(a) When a senior police officer has cause to believe that a person has in his or her custody or possession or on any premises owned or occupied by him or her any stolen property or property which has been unlawfully obtained, he or she may by writing under his or her hand authorise a police officer to enter in to and search the premises or any other premises where the person may be, and to seize any such property discovered: Provided that authority shall not be given under this paragraph unless the person in respect of whom the authority is to be issued has been previously convicted of receiving or retaining stolen property or of some other offence involving fraud or dishonesty punishable with imprisonment. (3) Any property seized under the provisions of this section shall be dealt with as if it had been seized under a search warrant. **THE CONSTITUTION OF THE REPUBLIC OF THE GAMBIA, 1997 (as Amended to 2018)** Chapter IV, PROTECTION OF FUNDAMENTAL RIGHTS AND FREEDOMS 23. Privacy (2) Searches of the person or the home of individuals shall only be justified (a) where these are authorised by a competent judicial authority; (b) in cases where delay in obtaining such judicial authority carries with

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	it the danger of prejudicing the objects of the search or the public interest and such procedures as are prescribed by an Act of the National Assembly to preclude abuse are properly satisfied.
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 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:	**ICA, 2009** CHAPTER II – REGULATION OF INFORMATION AND COMMUNICATION SYSTEMS AND SERVICES, PART XIII – PROCESSING OF PERSONAL DATA AND PROTECTION OF PRIVACY 138. Intercept (1) The national security agencies and investigating authorities may monitor,

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	intercept and store communications, and the Authority, when exercising its powers conferred relating to frequency monitoring, or may otherwise intrude communication for surveillance purposes. (2) If an alleged threat of murder or physical violence or blackmail occurs, the user or subscriber threatened may in writing authorize the investigating authority to intercept telephone conversations, other information and communications, e-mail messages and any other form of communications on his or her end terminal to investigate and to identify the persons involved in communications within the period of time set in the user's authorization. (3) The Minister may determine that information and communications operators and service providers must implement the capability to allow authorized interception of communications. (4) A determination under subsection (3), may specify the technical requirements for the capability to allow authorized interception of communications.
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. 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	**Criminal code (CC), 1933 as amended in 2010** PART I GENERAL PROVISIONS, CHAPTER II TERRITORIAL APPLICATION OF THIS CODE 4. Extent of jurisdiction of courts of The Gambia (1) The jurisdiction of the courts of The Gambia for the purpose of this Code extends to every place within The Gambia. [Act No. 17 of 1964, Act No. 4 of 1968.] (2) When an act, which if done within The Gambia, would be an offence against this Code, is done by a person in the service of the Government of The Gambia or a statutory body beyond the territorial limits of The Gambia, the person may be tried and punished under this Code in the same manner as if the act had been done within The Gambia. [Act No. 22 of 1974.]

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(3) When an act which, if wholly done within the jurisdiction of the court, would be an offence against this Code, is done partly within and partly beyond the jurisdiction, every person who within the jurisdiction does or makes any part of the act may be tried and punished under this Code in the same manner as if the act had been done wholly within the jurisdiction. [Act No. 22 of 1974.]
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 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	The Gambia has bilateral extradition treaties with various countries (e.g. United States and the United Kingdom), as well as multilateral regional agreements, i.e. ECOWAS Convention A/P.1/8/94 on Extradition. In domestic law, the applicable legislation is the Extradition Act No. 10, 1986 (§§ 2, 5 & 7, LAWS OF THE GAMBIA, Cap. 12:01 (rev. ed. 2009), which permits a person to be extradited for any 'serious offence' except where the tariff is life imprisonment or death penalty. **ICA, 2009** **PART IV – PROTECTION OF CHILDREN** **Indecent photographs of children** **174.** (5) An offence under this section shall be considered to be an extraditable crime for which extradition may be granted or obtained.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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	The Gambia is party to the ECOWAS Convention A/P.1/7/92 on mutual assistance in criminal matters.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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:	

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.	
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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 By a written notification addressed to the Secretary General of the Council of	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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