[Ivory Coast]

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version [25.02.2022]

[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:	
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	Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité **Chapitre 1 : Définitions** **système d'information ou Système informatique** : tout dispositif isolé ou non, tout ensemble de dispositifs interconnectés assurant en tout ou partie, un traitement automatisé de données en exécution d'un programme (article 1er de la loi). **données informatiques ou données** : toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire exécuter une fonction par un système d'information (article 1er de la loi). **données relatives aux abonnés :** «toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir sur la base d'un contrat ou d'un arrangement de services : - le type de service de communication, les dispositions techniques prises à cet égard et la période de service ; - l'identité, l'adresse postale ou géographique, le numéro de téléphone et tout autre numéro d'accès, les informations relatives à la localisation, la facturation et à l'endroit où se trouvent les équipements de communication». **données relatives au trafic** : toutes données ayant trait à une communication passant par un système d'information, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent ; **mineur**: toute personne âgée de moins de dix-huit ans, conformément au code pénal ; **pornographie infantile**: toute donnée quelle qu'en soit la nature ou la forme représentant de manière visuelle un enfant de moins de dix-huit ans se livrant à un agissement sexuellement explicite ou des images représentant un enfant de moins de quinze ans se livrant à un comportement sexuellement explicite ;
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.	Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité **Article 4 :** « Est puni d'un à deux ans d'emprisonnement et de 5.000.000 à 10.000.000 de francs CFA d'amende, quiconque accède ou tente d'accéder frauduleusement à tout ou partie d'un système d'information. » **Article 5:** «Est puni d'un à deux ans d'emprisonnement et de 5.000.000 à 10.000.000 de francs CFA d'amende, quiconque se maintient ou tente de se maintenir frauduleusement dans tout ou partie d'un système d'information. »
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.	Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité **Article 8**: «Est puni de cinq à dix ans d'emprisonnement et de 40.000.000 à 60.000.000 de francs CFA d'amende, quiconque intercepte ou tente d'intercepter frauduleusement par des moyens techniques des données informatiques lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système d'information». **Article 31**: «Est puni d'un emprisonnement d'un à cinq ans et de 1.000.000 de francs CFA d'amende, quiconque de mauvaise foi, ouvre, supprime, retarde ou détourne des correspondances électroniques arrivées ou non à destination et adressées à un tiers, ou en prend frauduleusement connaissance.

Back to the Table of Contents

Commented [SM1]: Please add for each section so a reader only looking at one part knows which domestic legislation is being referred to.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Est puni des mêmes peines, **quiconque de mauvaise foi, intercepte**, détourne, utilise ou divulgue des correspondances électroniques émises, transmises ou reçues par la voie des télécommunications ou procède à l'installation d'appareils conçus pour réaliser de telles interceptions»
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.	Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité **Article 9**: «Est puni de cinq à dix ans d'emprisonnement et de 40.000.000 à 60.000.000 de francs CFA d'amende, quiconque altère ou tente d'altérer, modifie ou tente de modifier, supprime ou tente de supprimer frauduleusement des données informatiques».
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	Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité **Article 6**: «Est puni d'un à cinq ans d'emprisonnement et de 10.000.000 à 40.000.000 de francs CFA d'amende, quiconque entrave, fausse ou tente d'entraver ou de fausser frauduleusement le fonctionnement d'un système d'information». **Article 7 :** « Est puni d'un à cinq ans d'emprisonnement et de 10.000.000 à 40.000.000 de francs CFA d'amende, quiconque introduit ou tente d'introduire frauduleusement des données dans un système d'information. » **Article 30**: «Lorsque les faits punis par la présente loi portent sur un système d'information ou un programme de traitement de données protégé par un code d'accès secret, la peine encourue ne peut être inférieure à dix ans d'emprisonnement».
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:	Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité **Article 13**: «Est puni de un an à deux ans d'emprisonnement et de 10.000.000 à 50.000.000 de francs CFA d'amende, quiconque, dans l'intention de commettre l'une des infractions prévues par la présente loi produit, vend, importe, détient, diffuse, offre, cède ou met à disposition, en connaissance de cause :

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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.	- un équipement, un dispositif ou un programme informatique - un mot de passe, un code d'accès ou des données informatiques similaires». **Article 29**: «Lorsqu'elle est faite intentionnellement et sans droit, la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission d'un vol d'information, ou l'usage d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système d'information, dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions prévues par de la présente loi, est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée d'entre elles». **Article 30**: «Lorsque les faits punis par la présente loi portent sur un système d'information ou un programme de traitement de données protégé par un code d'accès secret, la peine encourue ne peut être inférieure à dix ans d'emprisonnement».
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.	Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité **Article 10**: «Est puni de cinq à dix ans d'emprisonnement et de 40.000.000 à 60.000.000 de francs CFA d'amende, quiconque produit ou fabrique un ensemble de données par l'introduction, la modification, l'altération ou la suppression frauduleuse de données informatiques, engendrant des données contrefaites, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient originales».

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité **Article 11 :** « Est puni d'un à cinq ans d'emprisonnement et de 20.000.000 à 40.000.000 de francs CFA d'amende, quiconque fait usage, en connaissance de cause, de données informatiques frauduleusement obtenues. » **Article 12**: «Est puni de un à cinq ans d'emprisonnement et de 30.000.000 à 50.000.000 de francs CFA d'amende, quiconque obtient frauduleusement, pour soi-même ou pour autrui, un avantage quelconque, par l'introduction, l'utilisation, la modification, l'altération ou la suppression de données informatiques ou par toute forme d'atteinte au système d'information».
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	Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité **Article 15**: «Est puni de deux à cinq ans d'emprisonnement et de 75.000.000 à 100.000.000 de francs CFA d'amende, quiconque produit, enregistre, offre, met à disposition, diffuse, transmet une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système d'information ou d'un moyen de stockage de données informatiques». **Article 16**: «Est puni de deux à cinq ans d'emprisonnement et de 75.000.000 à 100.000.000 de francs CFA d'amende, quiconque se procure ou procure à autrui, importe ou fait importer, exporte ou fait exporter une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système d'information ou d'un moyen de stockage de données informatiques». **Article 17**: «Est puni de un à trois ans d'emprisonnement et de 20.000.000 à 40.000.000 de francs CFA d'amende, quiconque possède intentionnellement une image ou une représentation présentant un caractère de pornographie infantile dans un système d'information ou dans un moyen de stockage de données informatiques».

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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 from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité **Article 33**: «Sont punies d'une peine d'emprisonnement de un à dix ans et d'une amende de 500.000 à 100.000.000 de francs CFA, toutes les atteintes à la propriété intellectuelle commises au moyen d'un système d'information. Constitue une atteinte à la propriété intellectuelle : - le fait, sans autorisation de l'auteur ou de ses ayants droit, de reproduire, de représenter ou de mettre à la disposition du public sur un système d'information ou un support numérique ou analogique, intégralement ou partiellement une œuvre de l'esprit protégée par le droit d'auteur ou un droit voisin ; - le fait, sans autorisation de l'auteur ou de ses ayants droit, de traduire ou d'adapter une œuvre de l'esprit par le biais d'un programme informatique ou de mettre cette traduction ou adaptation sur un système d'information ou un support numérique ou analogique à la disposition du public ; - le fait, sans autorisation de l'auteur ou de ses ayants droit, de reproduire, d'utiliser, de vendre, de dénaturer, de dénigrer une marque, une raison sociale, un nom commercial, un nom de domaine Internet ou tout autre signe distinctif appartenant à un tiers par le biais d'un système d'information ouvert au public ou par le biais d'un programme informatique ou sur un support numérique ou analogique ; - le fait, en toute connaissance de cause, d'exploiter par reproduction ou par représentation une œuvre de l'esprit mise de façon illicite à disposition du public sur un réseau de communication électronique ;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	- le fait, en toute connaissance de cause, sans droit, de vendre ou de mettre à disposition du public par reproduction ou par représentation un bien ou un produit protégé par un brevet d'invention». **Article 34**: «Ne constituent pas une atteinte à la propriété intellectuelle lorsqu'elles sont réalisées par le biais d'un système ou un programme informatique ou électronique : - les copies ou reproductions d'œuvres de l'esprit strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective, à l'exclusion des copies des œuvres d'art destinées à être utilisées pour des fins identiques ou similaires à celles pour lesquelles l'œuvre originale a été créée ; - les analyses et courtes citations, sous réserve que soient clairement indiqués le nom de l'auteur de l'œuvre et la source, justifiées par le caractère critique, polémique, pédagogique, scientifique ou d'information de l'œuvre à laquelle elles sont incorporées. - la parodie et la caricature de l'œuvre originale réalisée sans intention de nuire à l'image et à l'honorabilité de l'auteur de ladite œuvre ; - les copies ou reproductions provisoires présentant un caractère transitoire et accessoire lorsqu'elles sont une partie intégrante et essentielle d'un procédé technique et qu'elles ont pour objet de permettre la transmission ou l'utilisation licite de l'œuvre sur un système d'information ou électronique ; - la reproduction et la représentation réalisée à des fins non lucratives par des personnes morales de droit public et par des établissements ouverts au public, tels que les bibliothèques, les services d'archives, les musées, les centres de documentation et les espaces culturels multimédias, en vue d'une consultation strictement personnelle de l'œuvre par des personnes atteintes d'une ou de plusieurs déficiences des fonctions motrices, physiques, sensorielles, mentales, cognitives ou psychiques dont le niveau d'incapacité est reconnu dans un certificat médical dûment établi ; - la reproduction d'une œuvre, effectuée à des fins de conservation ou destinée à préserver les conditions de sa consultation sur place par des bibliothèques accessibles au public, par des musées ou par des services d'archives, sous réserve que ceux-ci ne recherchent aucun avantage économique ou commercial ;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	- la reproduction et la représentation d'œuvre de l'esprit réalisée à des fins exclusivement pédagogiques par les enseignants et les chercheurs dans le cadre strict de leurs enseignements ou de leurs recherches pour leurs élèves et étudiants ou pour d'autres enseignants et chercheurs directement concernés, sous réserve que cette reproduction ou représentation ne donne lieu à aucune exploitation commerciale ou lucrative». **Article 35**: «L'auteur d'une œuvre de l'esprit ou ses ayants droit peuvent faire obstacle à la copie de l'œuvre en limitant le droit de copie reconnue par la présente loi, notamment, par la mise en œuvre de mesures techniques de protection lorsque la mise en œuvre du droit de copie porte atteinte à l'exploitation normale de l'œuvre ou cause un préjudice injustifié aux intérêts de l'auteur. On entend par mesure technique de protection, toute technologie, dispositif, composant qui, dans le cadre normal de son fonctionnement, accomplit la fonction de contrôle des utilisations de l'œuvre ou de limitation des copies de l'œuvre considérée. L'usager doit être clairement informé de l'existence des mesures techniques de protection sur l'œuvre qu'il acquiert ou utilise et sur les fonctions de ces mesures techniques, notamment si elles interdisent ou non l'usage de l'œuvre sur d'autres systèmes d'information ou d'exploitation ». **Article 36**:«Le titulaire d'un service d'accès à Internet ou à tout réseau de communication électronique est tenu de veiller à ce que cet accès ne soit pas utilisé à des fins manifestement illicites, notamment de reproduction ou de représentation d'œuvres de l'esprit sans l'autorisation de leurs auteurs ou leurs ayants droit. En cas de non-respect de cette obligation, il peut être poursuivi pour complicité par fourniture de moyen»
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	**TENTATIVE** Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité **Article 4**: «Est puni de un à deux ans d'emprisonnement et de 5.000.000 à 10.000.000 de francs CFA d'amende, quiconque accède ou **tente** d'accéder frauduleusement à tout ou partie d'un système d'information».

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 5**: «Est puni de un à deux ans d'emprisonnement et de 5.000.000 à 10.000.000 de francs CFA d'amende, quiconque se maintient ou tente de se maintenir frauduleusement dans tout ou partie d'un système d'information». **Article 6**: «Est puni de un à cinq ans d'emprisonnement et de 10.000.000 à 40.000.000 de francs CFA d'amende, quiconque entrave, fausse ou **tente** d'entraver ou de fausser frauduleusement le fonctionnement d'un système d'information». **Voir également Articles 7, 8, 9, 19, 26, 27, 28** **COMPLICITE** **Article 28: «**Le vol d'information ou la tentative de vol d'information est puni de vingt ans d'emprisonnement et de 10.000.000 de francs CFA d'amende, s'il a été commis dans l'une des deux circonstances ci-après : - lorsque l'auteur ou le **complice** est porteur d'une arme apparente ou cachée ; - lorsque l'auteur ou le **complice** a fait usage d'une arme ayant entraîné des blessures ou la mort de la victime»**.** **Article 36:** «Le titulaire d'un service d'accès à Internet ou à tout réseau de communication électronique est tenu de veiller à ce que cet accès ne soit pas utilisé à des fins manifestement illicites, notamment de reproduction ou de représentation d'œuvres de l'esprit sans l'autorisation de leurs auteurs ou leurs ayants droit. En cas de non-respect de cette obligation, il peut être poursuivi pour **complicité** par fourniture de moyen». **Article 69:**«Toute personne morale, à l'exception de l'Etat est pénalement responsable des infractions prévues par la présente loi, lorsqu'elles sont commises pour son compte par ses représentants. La responsabilité des personnes morales n'exclut pas celle des personnes physiques auteurs ou **complices** des mêmes faits. La peine encourue par les personnes morales responsables est le double de l'amende prévue pour la personne physique ayant commis l'infraction».
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	Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Article 69:** «Toute personne morale, à l'exception de l'Etat est pénalement responsable des infractions prévues par la présente loi, lorsqu'elles sont commises pour son compte par ses représentants. La responsabilité des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits. La peine encourue par les personnes morales responsables est le double de l'amende prévue pour la personne physique ayant commis l'infraction». **Article 24** : « Est puni d'une peine d'emprisonnement de un à cinq ans et de 5.000.000 à 100.000.000 de francs CFA d'amende, quiconque procède au traitement de données à caractère personnel par un moyen frauduleux, déloyal ou illicite. La peine d'amende ne peut être inférieure à 10.000.000 de francs CFA lorsque le traitement frauduleux, déloyal ou illicite a été fait en vue de l'envoi de messages électroniques non sollicités par une **personne morale**, autre que l'Etat ». **Article 40** : « Est puni d'une peine d'emprisonnement de cinq ans et d'une amende de 5.000.000 à 10.000.000 de francs CFA, quiconque ne respecte pas l'interdiction de transfert d'argent. La peine encourue par la **personne morale** responsable est le double de l'amende prévue pour la personne physique ayant commis l'infraction.. ». **Article 46 :** « Les personnes physiques ou morales qui offrent un accès à des services de communication en ligne ou qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent voir leur responsabilité civile ou pénale engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces Services : - si elles n'avaient effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ; - si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible ; - si le retrait de ces données n'a pas été ordonné par un tribunal. »

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Article 55 : « Est puni d'une peine d'emprisonnement de un an à cinq ans et d'une amende de 1.000.000 à 5.000.000 de francs CFA le fait pour une personne physique ou le dirigeant de droit ou de fait d'**une personne morale** exerçant l'une des activités mentionnées à l'article 46 de la présente loi de ne pas satisfaire aux obligations définies à l'article 54 ci-dessus.
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.	Voir les textes des articles cités plus-haut. Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité **Article 70** : « En cas de condamnation au titre de la présente loi, outre la publication de la condamnation ordonnée et exécutée, conformément à l'article 75 du Code pénal, le juge peut prononcer, à titre complémentaire, la confiscation spéciale, la privation de droits et l'interdiction de séjour prévus respectivement aux articles 63, 66 et 80 du Code pénal. »
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures	Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité **CHAPITRE VIII : PROCEDURE PENALE EN MATIERE DE CYBERCRIMINALITE** **Article 71**: «Les officiers de police judiciaire définis à l'article 16 nouveau du code de procédure pénale, les experts agréés auprès des tribunaux et toute autre personne dont les compétences sont requises, serment préalablement prêté, peuvent procéder aux opérations prévues par la présente loi. Les autorités compétentes visées ci-dessus n'ayant pas la qualité d'officier de police judiciaire ne peuvent procéder à une perquisition qu'en présence de ces officiers».

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	Les opérations susceptibles d'être conduites en application du chapitre VIII de la loi font l'objet d'un encadrement font l'objet d'un encadrement juridique. En effet, toutes les mesures ordonnées doivent être conformes au Code de procédure pénale. Ainsi, par exemple, la mise en œuvre de certaines procédures est subordonnée à l'intervention de l'autorité judiciaire.
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	Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité **Article 72 :** « Les données relatives aux abonnés doivent être conservées par les fournisseurs de services. Cette obligation impose aux fournisseurs de services de conserver et de protéger l'intégrité desdites données pendant une durée de dix ans. Lorsqu'il est impossible de retrouver l'auteur d'une communication

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	électronique pour défaut de conservation des données relatives aux abonnés, le fournisseur de services encourt une peine d'amende de 10.000.000 à 50.000.000 de francs CFA. » **Article 73**: «Lorsque dans le cadre d'une enquête ou d'une instruction, il y a des raisons de penser que des données informatiques spécifiées, y compris des données relatives aux abonnés et au trafic, stockées au moyen d'un système d'information, sont susceptibles de perte ou de modification, l'autorité compétente procède ou fait procéder à la conservation immédiate desdites données. La personne physique ou morale à qui injonction est faite, conserve et protège l'intégrité desdites données pendant une durée aussi longue que nécessaire pour les besoins de l'enquête ou de l'instruction».
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.	Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité **Article 73**: «Lorsque dans le cadre d'une enquête ou d'une instruction, il y a des raisons de penser que des données informatiques spécifiées, y compris des données relatives aux abonnés et au trafic, stockées au moyen d'un système d'information, sont susceptibles de perte ou de modification, l'autorité compétente procède ou fait procéder à la conservation immédiate desdites données. La personne physique ou morale à qui injonction est faite, conserve et protège l'intégrité desdites données pendant une durée aussi longue que nécessaire pour les besoins de l'enquête ou de l'instruction».
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:	Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Article 74:** «L'autorité compétente, sur réquisition du procureur ou ordonnance du juge d'instruction, peut requérir : - de toute personne physique ou morale, **l'obligation de communiquer des données spécifiées**, en sa possession ou sous son contrôle, qui sont stockées dans un système d'information ou un support de stockage informatique; - d'un fournisseur de services, de communiquer les données spécifiées relatives au trafic et aux abonnés en sa possession ou sous son contrôle».
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.	Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité **Article 71**: «Les officiers de police judiciaire définis à l'article 16 nouveau du code de procédure pénale, les experts agréés auprès des tribunaux et toute autre personne dont les compétences sont requises, serment préalablement prêté, peuvent procéder aux opérations prévues par la présente loi. Les autorités compétentes visées ci-dessus n'ayant pas la qualité d'officier de police judiciaire ne peuvent procéder à une **perquisition** qu'en présence de ces officiers». **Article 75**: «L'autorité compétente peut, au cours d'une perquisition effectuée dans les conditions prévues par le code de procédure pénale, accéder à un système d'information ou à un support de stockage numérique et à des données

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	intéressant l'enquête en cours et stockées dans ledit système ou ledit support se trouvant sur les lieux de la perquisition**.** L'autorité compétente peut également accéder à des données intéressant l'enquête en cours et stockées dans un autre système d'information, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial. S'il est avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système d'information situé hors du territoire national, elles sont recueillies par l'autorité compétente, sous réserve du respect des engagements internationaux». **Article 76 :** « L'autorité compétente peut, dans les conditions prévues par le code de procédure pénale, procéder à la saisie des systèmes informatiques, des supports de stockage informatique ou procéder à la copie des données informatiques nécessaires à la manifestation de la vérité. Si une copie est réalisée dans le cadre de cette procédure, il peut être procédé, sur décision du juge, à l'effacement définitif sur le support physique qui n'a pas été placé sous-main de justice, des données informatiques dont la détention ou l'usage est illégal ou dangereux pour la sécurité des personnes ou des biens. Lorsque les systèmes informatiques ou les supports de stockage informatique sont mis sous scellés, ils ne peuvent être ouverts que selon les modalités prévues par le code de procédure pénale. »
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	Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité **Article 77**: «L'autorité compétente, sur réquisition du procureur ou ordonnance du juge d'instruction, est habilitée : - à collecter ou enregistrer par tout moyen technique les données relatives au trafic ou au contenu associées à des communications spécifiques transmises sur son territoire au moyen d'un système d'information ; - à obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à collecter ou enregistrer par tout moyen technique ou prêter aux autorités compétentes son concours et son assistance pour **collecter ou enregistrer en temps réel**, les données relatives au trafic ou au contenu associées à des communications spécifiques transmises sur son territoire au moyen d'un système d'information.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	Les surcoûts identifiables et spécifiques éventuellement exposés par les fournisseurs de services pour répondre à ces demandes font l'objet d'une compensation financière de l'Etat». **Article 78**: «Est puni d'une peine d'emprisonnement de trois à six mois et de 1.000.000 à 5.000.000 de francs CFA d'amende, **quiconque refuse de déférer à la demande du procureur ou du juge d'instruction**. Lorsqu'il s'agit d'une personne morale, elle encourt une peine d'amende de 10.000.000 à 100.000.000 de francs CFA».
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: 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.	Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité **Article 77**: «L'autorité compétente, sur réquisition du procureur ou ordonnance du juge d'instruction, est habilitée : - à collecter ou enregistrer par tout moyen technique les données relatives au trafic ou au contenu associées à des communications spécifiques transmises sur son territoire au moyen d'un système d'information ; - à obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à collecter ou enregistrer par tout moyen technique ou prêter aux autorités compétentes son concours et son assistance pour **collecter ou enregistrer en temps réel**, les données relatives au trafic ou au contenu associées à des communications spécifiques transmises sur son territoire au moyen d'un système d'information. Les surcoûts identifiables et spécifiques éventuellement exposés par les fournisseurs de services pour répondre à ces demandes font l'objet d'une compensation financière de l'Etat».

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité **Article 41**: «Les juridictions nationales sont compétentes pour constater ou punir les infractions lorsque les activités de jeux d'argent illicites sont offertes à partir du territoire national ou sont accessibles aux utilisateurs des réseaux de communication électronique à partir du territoire national et qu'il existe un lien suffisant, substantiel ou significatif entre la prestation illicite offerte aux utilisateurs des réseaux de communication en ligne et le territoire national, notamment, par la langue utilisée, la monnaie employée, les produits proposés, le nom de domaine utilisé par le site proposant ladite prestation». **Article 75 :** « L'autorité compétente peut, au cours d'une perquisition effectuée dans les conditions prévues par le code de procédure pénale, accéder à un système d'information ou à un support de stockage numérique et à des données intéressant l'enquête en cours et stockées dans ledit système ou ledit support se trouvant sur les lieux de la perquisition. L'autorité compétente peut également accéder à des données intéressant l'enquête en cours et stockées dans un autre système d'information, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial. S'il est avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système d'information situé hors du territoire national, elles sont recueillies par l'autorité compétente, sous réserve du respect des engagements internationaux. » **Article 67 :** « Est coupable de trahison et puni de l'emprisonnement à vie, le fait pour un ivoirien : - de livrer ou de s'assurer de la possession en vue de la livraison à un pays étranger ou à une personne physique ou morale étrangère par le biais d'un système d'information, un renseignement, un document, un procédé ou une donnée informatique qui doit être tenu(e) secret dans l'intérêt de la Défense Nationale, - de détruire ou de laisser détruire un renseignement, un document, un procédé ou une donnée informatique qui doit être tenu (e) secret dans l'intérêt de la Défense Nationale, en vue de favoriser un pays étranger ou une personne physique ou morale étrangère. »

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité **Article 75**: «L'autorité compétente peut, au cours d'une perquisition effectuée dans les conditions prévues par le code de procédure pénale, accéder à un système d'information ou à un support de stockage numérique et à des données intéressant l'enquête en cours et stockées dans ledit système ou ledit support se trouvant sur les lieux de la perquisition. L'autorité compétente peut également accéder à des données intéressant l'enquête en cours et stockées dans un autre système d'information, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial. S'il est avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système d'information situé hors du territoire national, elles sont recueillies par l'autorité compétente, **sous réserve du respect des engagements internationaux**».

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other;	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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