Congo, Republic of

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Version 25 June 2020

Table of contents

[reference to the provisions of the Budapest Convention]

This profile has been prepared by the Cybercrime Programme Office (C-PROC) of the Council of Europe in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Budapest Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the State covered or of the Council of Europe.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime

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

BUDAPEST CONVENTION	**DOMESTIC LEGISLATION**
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	LA LOI N° 27-2020 DU 05 JUIN 2020 PORTANT LUTTE CONTRE LA CYBERCRIMINALITE TITRE I : DISPOSITIONS GENERALES Chapitre 1 : Des atteintes à la confidentialité des systèmes d'information Article 3 : Au sens de la présente loi, on entend par : ▪ Accès dérobé : mécanisme permettant de dissimuler l'accès à des données ou à un système d'information sans l'autorisation de l'utilisateur légitime ; ▪ Communication au public par voie électronique : toute mise à la disposition du public ou d'une catégorie de public, par un procédé de communications électroniques ou magnétiques, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature ; ▪ Communications électroniques : émission, transmission ou réception de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique ; ▪ Cybercriminalité : ensemble des infractions s'effectuant à travers le cyberespace par des moyens autres que ceux habituellement mis en œuvre, et de manière complémentaire à la criminalité classique ; ▪ Données informatiques : 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 en sorte qu'un système informatique exécute une fonction ; ▪ Données à caractère personnel : toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique ; ▪ 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: - le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ; - l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ; - toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services. ▪ 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, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent ; ▪ Matériel xénophobe : tout écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence contre une personne ou un groupe de personnes, en raison de la couleur, de l'ascendance ou de l'origine nationale ou ethnique ou de la religion, dans la mesure où ce dernier sert de prétexte à l'un ou à l'autre de ces éléments ou qui incite à de tels actes ; ▪ Pornographie infantile : toute donnée, quelle qu'en soit la nature ou la forme ou le support, représentant : - un enfant se livrant à un comportement sexuellement explicite ; - une personne qui apparaît comme un enfant se livrant à un comportement sexuellement explicite ; - des images réalistes représentant un enfant se livrant à un comportement sexuellement explicite. ▪ Programme informatique : séquence d'instructions qui spécifie, étape par étape, les opérations à effectuer par un ordinateur ou une composante d'ordinateur pour obtenir un résultat ;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	▪ Système d'information : ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) qui permet de collecter, de regrouper, de classifier, de traiter et de diffuser l'information ; ▪ Système informatique : tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données ; ▪ Technologies de l'information et de la communication : désigne les technologies employées pour recueillir, stocker, utiliser et envoyer des informations ainsi que celles qui impliquent l'utilisation des ordinateurs ou de tout système de communication, y compris de télécommunication.
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.	TITRE II : DES INFRACTIONS LIEES AUX TECHNOLOGIES DE L'INFORMATIONET DE LA COMMUNICATION Chapitre 1 : Des atteintes à la confidentialité des systèmes d'information Article 4 : Quiconque accède ou tente d'accéder frauduleusement à tout ou partie d'un système d'information est puni d'un emprisonnement de six mois au moins à trois ans au plus et d'une amende d'un million (1 000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement. Est puni des mêmes peines, quiconque se procure ou tente de se procurer frauduleusement, pour soi-même ou pour autrui, un avantage quelconque en s'introduisant dans 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	Chapitre 4 : De l'interception frauduleuse de données d'un système d'information Article 8 : Quiconque intercepte ou tente d'intercepter frauduleusement, par des moyens techniques, des données d'un système d'information lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	système d'information, est puni d'un emprisonnement d'un an au moins à cinq ans au plus et d'une amende de cinq millions (5 000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement.
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.	Chapitre 5 : Des atteintes à l'intégrité des données d'un système d'information Article 9 : Quiconque endommage ou tente d'endommager, efface ou tente d'effacer, détériore ou tente de détériorer, altère ou tente d'altérer, supprime ou tente de supprimer, frauduleusement des données d'un système d'information, est puni d'un emprisonnement d'un an au moins à cinq ans au plus et d'une amende de cinq millions (5 000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement.
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	
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	Chapitre 7 : De l'abus de dispositifs et de l'association de malfaiteurs informatiques Article 25 : Quiconque produit, vend, importe, détient, diffuse, offre, cède ou met à disposition un équipement, un programme informatique, tout dispositif ou donnée conçue ou spécialement adaptée pour commettre une ou plusieurs des infractions prévues aux articles 3 à 10 de la présente loi ou un mot de passe, un code d'accès ou des données informatisées similaires permettant d'accéder à tout ou partie d'un système d'information, est puni soit des peines prévues pour l'infraction elle-même, soit en cas de pluralité d'infractions, des peines prévues pour l'infraction la plus sévèrement réprimée.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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.	Chapitre 5 : Des atteintes à l'intégrité des données d'un système d'information Article 10 : Quiconque produit ou fabrique un ensemble de données numérisées par l'introduction, l'effacement ou la suppression frauduleuse de données informatisées stockées, traitées ou transmises par un système d'information, engendrant des données contrefaites, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient originales, est puni d'un emprisonnement d'un an au moins à cinq ans au plus et d'une amende de cinq millions (5 000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement.

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.	Article 11 : Est puni d'un emprisonnement d'un an au moins à cinq ans au plus et d'une amende de cinq millions (5 000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement, quiconque obtient frauduleusement, pour soi-même ou pour autrui, un avantage quelconque, par l'introduction, l'altération, l'effacement ou la suppression de données informatisées.
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	Chapitre 8 : De la pornographie infantile Article 27 : 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, commet un crime punissable de la réclusion de cinq ans au moins à dix ans au plus. Article 28 : 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, commet un crime punissable de la réclusion de cinq ans au moins à dix ans au plus. Article 29 : Quiconque possède une image ou une représentation présentant un caractère de pornographie infantile dans un système d'information ou dans un moyen quelconque de stockage de données informatisées, commet un crime punissable d'un emprisonnement de cinq ans au moins à dix ans au plus.

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.	Chapitre 16 : Des atteintes au droit d'auteur et aux droits voisins Article 70 : Quiconque commet délibérément, à une échelle commerciale et au moyen d'un système d'information, une atteinte au droit d'auteur et aux droits voisins définis par la loi sur le droit d'auteur et les droits voisins, conformément aux obligations que l'Etat a souscrites, à l'exception de tout droit moral conféré par ces conventions, est puni d'un emprisonnement de six mois au moins à cinq ans au plus et d'une amende de cinq cent mille (500 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	.
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	Chapitre 20 : De la responsabilité pénale des personnes morales Article 78 :Les personnes morales autres que l'État, les collectivités locales et les établissements publics sont pénalement responsables des infractions prévues par la présente loi, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé : - sur un pouvoir de représentation de la personne morale; - sur une autorité pour prendre des décisions au nom de la personne morale; - sur une autorité pour exercer un contrôle au sein de la personne morale. Article 79 : Les personnes morales visées à l'article 77 ci-dessus peuvent être tenues pour responsables lorsque l'absence de surveillance ou de contrôle de la part de leurs organes ou représentants a rendu possible la commission des infractions établies en application de la présente loi pour le compte de ladite personne morale par une personne physique agissant sous leur autorité.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	Chapitre 7 : De l'abus de dispositifs et de l'association de malfaiteurs informatiques Article 26 : Quiconque participe à une association formée ou à une entente établie en vue de préparer ou de commettre une ou plusieurs des infractions prévues par la présente loi, est puni soit des peines prévues pour l'infraction elle-même, soit en cas de pluralité d'infractions, des peines prévues pour l'infraction la plus sévèrement réprimée. Lorsqu'elles ont été commises en bande organisée, les infractions prévues par la présente loi sont punies du maximum de la peine correspondante. Chapitre 8 : De la pornographie infantile Article 27 : 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, commet un crime punissable de la réclusion de cinq ans au moins à dix ans au plus. Article 29 : Quiconque possède une image ou une représentation présentant un caractère de pornographie infantile dans un système d'information ou dans un moyen quelconque de stockage de données informatisées, commet un crime punissable d'un emprisonnement de cinq ans au moins à dix ans au plus. Chapitre 20 : De la responsabilité pénale des personnes morales Article 81 : Peuvent être prononcées contre les personnes morales, les peines suivantes : - l'amende égale au quintuple de celle prévue pour les personnes physiques par la loi qui réprime l'infraction ; - la dissolution, lorsque la personne morale a été créée ou détournée de son objet pour commettre les faits incriminés ; - l'interdiction définitive ou temporaire, ne pouvant dépasser une durée de cinq ans, d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ; - la fermeture définitive ou temporaire, ne pouvant dépasser une durée de cinq ans, d'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	- l’exclusion des marchés publics à titre définitif ou pour une durée de cinq ans au plus ; - l’interdiction à titre définitif ou pour une durée de cinq ans au plus de faire appel public à l’épargne ; - l’interdiction pour une durée de cinq ans au plus d’émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ou d’utiliser des cartes de paiement ; - la confiscation de la chose qui a servi ou était destinée à commettre l’infraction ou de la chose qui en est le produit ; - l’affichage de la décision prononcée ou la diffusion de celle-ci soit par la presse écrite soit par tout moyen de communication au public par voie électronique.
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:	TITRE I : DISPOSITIONS GENERALES Chapitre 1 : De l’objet et du champ d’application Article 2 : Les dispositions de la présente loi sont applicables à toutes les personnes, quelle que soit leur nationalité, ayant commis une infraction par le biais des technologies de l’information et de la communication en République du Congo.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	Constitution de 2015 de la République du Congo Préambule. Le Peuple congolais, […] Déclare partie intégrante de la présente Constitution les principes fondamentaux proclamés et garantis par : - la Charte des Nations unies du 24 octobre 1945 ; - la Déclaration universelle des droits de l'homme du 10 décembre 1948 ; - la Charte africaine des droits de l'homme et des peuples du 26 juin 1981 ; - la Charte de l'unité nationale et la Charte des droits et des libertés adoptées par la Conférence nationale souveraine, le 29 mai 1991 ; - tous les textes internationaux pertinents dûment ratifiés relatifs aux droits humains ; Titre II. Des droits, libertés et devoirs des citoyens. Sous-titre I. Des droits et libertés. Article 8 La personne humaine est sacrée et a droit à la vie. L'État a l'obligation de la respecter et de la protéger. Chaque citoyen a le droit au plein épanouissement de sa personne dans le respect des droits d'autrui, de l'ordre public, de la morale et des bonnes moeurs.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Article 9. La liberté de la personne humaine est inviolable. Nul ne peut être arbitrairement accusé, arrêté ou détenu. Tout prévenu est présumé innocent jusqu'à ce que sa culpabilité ait été établie à la suite d'un procès juste et équitable garantissant les droits de la défense. Les droits de la victime sont également garantis. Article 11. Toute personne arrêtée est informée du motif de son arrestation et de ses droits dans une langue qu'elle comprend. Tout acte de torture, tout traitement cruel, inhumain ou dégradant est interdit. Le pouvoir judiciaire, gardien des libertés individuelles, assure le respect de ce principe dans les conditions fixées par la loi. Article 15. Tous les citoyens congolais sont égaux devant la loi et ont droit à la protection de l'État. Nul ne peut être favorisé ou désavantagé en raison de son origine familiale, ethnique, de sa condition sociale, de ses convictions politiques, religieuses, philosophiques ou autres. Article 20. Le domicile est inviolable. Il ne peut être ordonné de perquisition que dans les formes et les conditions prévues par la loi. Article 25. Tout citoyen a le droit d'exprimer et de diffuser librement son opinion par la parole, l'écrit, l'image ou par tout autre moyen de communication. La liberté de l'information et de la communication est garantie. Elle s'exerce dans le respect de la loi. La censure est prohibée. L'accès aux sources d'information est libre et protégé dans les conditions déterminées par la loi. Article 26.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Le secret des correspondances, des télécommunications ou de toute autre forme de communication ne peut être violé, sauf dans les cas et les conditions prévus par la loi. Article 35. Tout citoyen a droit à la protection des intérêts moraux et matériels découlant de toute œuvre scientifique, littéraire ou artistique dont il est l'auteur. La mise sous séquestre, la saisie, la confiscation, l'interdiction de tout ou partie de toute publication, de tout enregistrement ou d'autres moyens d'information ou de communication ne peut se faire qu'en vertu d'une décision de justice. Article 47. Tout citoyen qui subit un préjudice du fait de l'administration a le droit d'agir en justice, dans les formes déterminées par la loi.
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.	TITRE III : DE LA PROCEDURE EN MATIERE D'INFRACTIONS COMMISES PAR LE BIAIS DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION Chapitre 4 : De la conservation rapide des données informatiques stockées Article 98 : Si les nécessités de l'enquête l'exigent, notamment lorsqu'il y a des raisons de penser que des données informatisées archivées dans un système d'information sont particulièrement susceptibles de perte ou de modification, le procureur de la République ou le juge d'instruction peut faire injonction à toute personne de conserver et de protéger l'intégrité des données en sa possession ou sous son contrôle, pendant une durée de deux ans maximum, pour la bonne marche des investigations judiciaires. Le gardien des données ou toute autre personne chargée de les conserver est tenu de garder le secret sur la mise en œuvre desdites procédures, sous peine des sanctions pénales encourues en matière de violation du secret professionnel.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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;	Chapitre 5 : De l'injonction de produire Article 99 : Si les nécessités de l'enquête l'exigent, le procureur de la République ou le juge d'instruction peut faire injonction à toute personne présente sur le territoire congolais de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système d'information ou un support de stockage informatique. L'injonction de produire peut être adressée, dans les mêmes conditions susmentionnées, à un fournisseur de services offrant des prestations au Congo, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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	Chapitre 2 : De la perquisition et saisie informatique Article 88 :Lorsque des données stockées dans un système d'information ou dans un support permettant de conserver des données informatisées sur le territoire congolais sont utiles à la manifestation de la vérité, le procureur de la République ou le juge d'instruction peut ordonner une perquisition ou accéder à un système d'information ou à une partie de celui-ci ou dans un autre système d'information, dès lors que ces données sont accessibles à partir du système initial ou disponible pour le système initial. S'il est préalablement établi que ces données, accessibles à partir du système initial ou disponible pour le système initial, sont stockées dans un autre système d'information situé en dehors du territoire national, elles sont recueillies par le procureur de la République ou le juge d'instruction, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur. Article 89 : Lorsque le procureur de la République ou le juge d'instruction découvre dans un système d'information des données stockées qui sont utiles pour la manifestation de la vérité, mais que la saisie du support ne paraît pas souhaitable, ces données, de même que celles qui sont nécessaires pour les comprendre, sont copiées sur des supports de stockage informatique pouvant être saisis et placés sous scellés. Le procureur de la République ou le juge d'instruction désigne toute personne qualifiée pour utiliser les moyens techniques appropriés afin d'empêcher l'accès aux données visées à l'article 4 de la présente loi dans le système d'information ou aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système d'information et de garantir leur intégrité. Lorsque, pour des raisons techniques ou en raison du volume des données, la mesure prévue à l'alinéa 2 du présent article ne peut être prise, le procureur de la République ou le juge d'instruction utilise les moyens techniques appropriés

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	pour empêcher l'accès à ces données dans le système d'information, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système d'information, de même que pour garantir leur intégrité. Article 90 : Lorsqu'il apparaît que les données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait l'objet d'opérations de transformation empêchant d'y accéder en clair ou sont de nature à compromettre les informations qu'elles contiennent, le procureur de la République ou le juge d'instruction peut réquisitionner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair desdites données. Lorsqu'un moyen de cryptographie a été utilisé, les autorités judiciaires peuvent exiger la convention secrète de déchiffrement du cryptogramme. Article 91 : Les personnes physiques ou morales qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité sont tenues de remettre aux officiers de police judiciaire ou aux agents habilités de l'agence nationale de sécurité des systèmes d'information, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies. Les officiers de police judiciaire et les agents habilités de l'agence nationale de sécurité des systèmes d'information peuvent demander aux fournisseurs des prestations visés à l'alinéa 1 ci-dessus de mettre eux-mêmes en œuvre ces conventions, sauf si ceux-ci démontrent qu'ils ne sont pas en mesure de satisfaire à de telles réquisitions. Article 92 :Si les données qui sont liées à l'infraction, soit qu'elles en constituent l'objet, soit qu'elles en ont été le produit, sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes d'informations ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, le procureur de la République ou le juge d'instruction ordonne les mesures conservatoires nécessaires, notamment en désignant toute personne qualifiée avec pour mission d'utiliser tous les moyens techniques appropriés pour rendre ces données inaccessibles. Article 93 : Le procureur de la République informe le responsable du système d'information de la recherche effectuée dans le système d'information et lui communique une copie des données qui ont été copiées, rendues inaccessibles ou retirées.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Article 94 : Le juge compétent peut à tout moment, d'office ou sur la demande de l'intéressé, ordonner main levée de la saisie.
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.	Chapitre 6 : De la collecte en temps réel des données relatives au trafic Article 100 : Si les nécessités de l'enquête l'exigent, le procureur de la République ou le juge d'instruction peut utiliser les moyens techniques appropriés pour collecter ou enregistrer, en temps réel, les données relatives au trafic associées à des communications spécifiques, transmises au moyen d'un système d'information. Le procureur de la République ou le juge d'instruction peut également obliger un fournisseur de services, dans le cadre de ses capacités techniques, à collecter ou à enregistrer, en application des moyens techniques existant, ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données visées à l'alinéa premier du présent article. Article 101 : Le fournisseur de service désigné à l'alinéa 2 de l'article 100 ci-dessus est tenu de garder le secret sur les informations reçues. Toute violation du secret est punie des peines applicables à l'infraction de violation du secret professionnel, conformément au code pénal.
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	

Back to the Table of Contents

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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	
Article 31 – Mutual assistance regarding accessing of stored computer data	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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