Monaco

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Version 5 May 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.

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

State:	
Signature of the Budapest Convention:	02/05/2013
Ratification/accession:	17/03/2017

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; a) 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.	**Article 389-1 (Créé par la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique)** Est qualifié de **système d'information**, 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 informatiques ainsi que les données informatiques stockées, traitées, récupérées ou transmises par ce dispositif ou cet ensemble de dispositifs en vue du fonctionnement, de l'utilisation, de la protection et de la maintenance de celui-ci. Est qualifiée de **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. **Loi n° 1.383 du 2 août 2011 sur l'Economie Numérique** «**fournisseur**»: toute personne morale ou physique proposant dans le cadre de son activité professionnelle la fourniture de biens ou de services par la mise en œuvre d'une ou plusieurs techniques de communication à distance utilisant des moyens électroniques **Article 389-11-1 (Créé par la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique)** **Les opérateurs et les prestataires de services** chargés de l'exploitation des réseaux et des services de télécommunications et de communications

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	électroniques, sont tenus d'effacer ou de rendre anonyme toute donnée relative au trafic, sous réserve des dispositions des articles 389-11-2 à 389-11-5. Sont qualifiées de « **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, la durée de la communication ou le type de service sous-jacent.
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.	**Code pénal Article 389-1 (Créé par la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique)** Est qualifié **d'accès frauduleux**, toute action de pénétration ou d'intrusion irrégulière, par quelque moyen que ce soit, dans tout ou partie d'un système d'information consistant à consulter des données ou des informations, à créer une menace ou à attenter à la sécurité, la confidentialité, l'intégrité, la disponibilité d'un système d'information ou des données qui y sont intégrées ou stockées.
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.	**Code pénal Article 389-5 (Créé par la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique)** Quiconque aura, frauduleusement, intercepté par des moyens techniques, des données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système d'information, y compris les émissions électromagnétiques provenant d'un système d'information transportant de telles données informatiques, sera puni d'un emprisonnement de trois ans et de l'amende prévue au chiffre 4 de l'article 26.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Code pénal Article 389-4 (Créé par la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique)** Quiconque aura, frauduleusement, fait usage de données informatiques volontairement endommagées, effacées, détériorées, modifiées, ou altérées sera puni d'un emprisonnement de cinq ans et de l'amende prévue au chiffre 4 de l'article 26.
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.	**Code pénal Article 389-2 (Créé par la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique)** Quiconque aura, frauduleusement, entravé ou altéré le fonctionnement de tout ou partie d'un système d'information, sera puni d'un emprisonnement de cinq ans et de l'amende prévue au chiffre 4 de l'article 26. Est qualifiée d'entrave au fonctionnement d'un système d'information, toute action ayant pour effet, objet ou finalité de paralyser un système d'information par l'introduction, la transmission, l'endommagement, l'effacement, la modification, l'altération ou la suppression de données informatiques. Est qualifiée d'altération du fonctionnement d'un système d'information, toute action consistant à fausser le fonctionnement dudit système pour lui faire produire un résultat autre que celui pour lequel il est normalement conçu et utilisé.
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,	**Code pénal Article 389-6 (Créé par la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique)** Est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée, le fait, frauduleusement, de produire, importer, détenir, offrir, céder, diffuser, obtenir en vue d'utiliser ou mettre à disposition: 1. un équipement, un dispositif, y compris un programme informatique, ou toute donnée principalement conçus ou adaptés pour permettre la commission d'une ou plusieurs des infractions prévues aux articles 389-1 à 389-5;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	2. un mot de passe, un code d'accès ou des données informatiques similaires permettant d'accéder à tout ou partie d'un système d'information pour commettre l'une des infractions prévues aux articles 389-1 à 389-5. Le présent article est sans application lorsque la production, l'importation, la détention, l'offre, la cession, la diffusion ou la mise à disposition n'a pas pour but de commettre l'une des infractions visées aux articles 389-1 à 389-5, comme dans le cas d'essai autorisé, de la recherche ou de protection d'un système d'information.
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.	**Code pénal Article 389-7 (Créé par la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique)** Quiconque aura, frauduleusement, introduit, altéré, effacé ou supprimé des données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles, sera puni d'un emprisonnement de cinq ans et de l'amende prévue au chiffre 4 de l'article 26.

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.	**Code pénal Article 389-8 (Créé par la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique)** Quiconque aura, frauduleusement, causé un préjudice patrimonial à autrui par l'introduction, l'altération, l'effacement ou la suppression de données informatiques ou par toute forme d'atteinte au fonctionnement d'un système d'information, dans l'intention, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui sera puni d'une peine d'emprisonnement de cinq ans et de l'amende prévue au chiffre 4 de l'article 26 dont le maximum peut être porté jusqu'au montant du profit éventuellement réalisé.
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;	**Code pénal Article 294-3 - (Créé par la loi n° 1.344 du 26 décembre 2007)** Le fait, en vue de sa diffusion, de fixer, d'enregistrer, de produire, de se procurer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni d'un emprisonnement de trois à cinq ans et de l'amende prévue au chiffre 3 de l'article 26. La tentative est punie des mêmes peines. Le fait, sciemment, d'offrir ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines. Le fait de détenir sciemment une telle image ou représentation est puni de six mois à deux ans d'emprisonnement et de l'amende prévue au chiffre 2 de l'article 26. Le fait d'accéder, en connaissance de cause, à une telle image ou représentation, est puni des mêmes peines. Les peines sont portées de cinq à dix ans d'emprisonnement et à l'amende prévue au chiffre 4 de l'article 26 lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation d'un mineur à destination d'un public non déterminé, un réseau de communications électroniques. Les dispositions du présent article sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	sauf s'il est établi que cette personne était âgée de dix-huit ans accomplis au jour de la fixation ou de l'enregistrement de son image. Au sens du présent article, sont considérées comme des images à caractère pornographique : 1) l'image ou la représentation d'un mineur subissant ou se livrant à un comportement sexuellement explicite ; 2) l'image ou la représentation d'une personne qui apparaît comme un mineur subissant ou se livrant à un comportement sexuellement explicite ; 3) l'image réaliste représentant un mineur se livrant à un comportement sexuellement explicite. L'expression "image réaliste" désigne, notamment, l'image altérée d'une personne physique, en tout ou partie créée par des méthodes numériques. Les dispositions du présent article ne s'appliquent pas si les images ou représentations d'images ont été collectées pour la constatation, la recherche ou la poursuite des infractions pénales.
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	Le droit de la propriété intellectuelle monégasque est régi par quatre lois principales : 1. la Loi n° 1058 du 10 juin 1983 sur les marques de fabrique, de commerce ou de service; 2. les lois n° 606 et 607 du 20 juin 1955 sur les brevets d'invention et sur les dessins et modèles; 3. la Loi n° 491 du 24 novembre 1948 sur la protection des œuvres littéraires et artistiques. La réglementation nationale sur les brevets d'invention a été mise à jour par l'Ordonnance Souveraine n° 6.337 et l'Arrêté Ministériel n° 2017-217 du 5 avril 2017. L'Ordonnance Souveraine n° 6.874 du 29 mars 2018 a harmonisé les procédures au sein des trois domaines de propriété industrielle : brevets d'invention ; dessins et modèles ; marques de fabrique, de commerce ou de service.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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.	**Code pénal Article 389-10 (Créé par la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique)** Quiconque tente de commettre une des infractions prévues aux articles 389-1 à 389-9 est puni des peines prévues pour l'infraction elle-même.
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;	**Code pénal Article 4-4 - (Créé par la loi n° 1.349 du 25 juin 2008)** Toute personne morale, à l'exclusion de l'État, de la commune et des établissements publics, est pénalement responsable comme auteur ou complice, selon les distinctions déterminées aux articles 29-1 à 29-6, de tout crime, délit ou contravention lorsqu'ils ont été commis pour son compte, par l'un de ses organes ou représentants.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	L'action est dirigée contre la personne morale prise en la personne de son représentant légal. La responsabilité pénale de la personne morale n'exclut pas celle, en qualité de co-auteurs ou complices, des personnes la représentant au moment des faits. En ce cas, s'il y a contrariété d'intérêts, ces personnes peuvent saisir par requête le président du tribunal de première instance, aux fins de désignation d'un mandataire ad hoc pour représenter la personne morale.
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.	**Code pénal Article 389-11 (Créé par la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique)** Les peines encourues par les personnes morales sont: 1) l'amende, suivant les modalités prévues par l'article 29-2; l'affichage ou la diffusion de la décision prononcée suivant les modalités prévues à l'article 30; 2) les peines mentionnées aux articles 29-3 et 29-4. En matière correctionnelle, lorsqu'aucune peine d'amende n'est prévue à l'encontre des personnes physiques, l'amende encourue par les personnes morales est de 1.000.000 euros.
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;	**Loi n° 1.449 du 4 juillet 2017 portant diverses mesures relatives à la procédure pénale.** **Art. 19-2 de la Loi n° 1.482 du 17 décembre 2019 pour une Principauté numérique, modifiant la loi n° 1.383 du 2 août 2011 sur l'économie numérique, article 28-9** L'acquisition, la détention, la fabrication, l'importation, l'exposition, l'offre, la location ou la vente de tout appareil ou dispositif matériels et logiciels, de nature à permettre l'interception, l'écoute, l'analyse, la retransmission, l'enregistrement ou le traitement de correspondances émises, transmises ou reçues sur des

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.	réseaux de communications électroniques, opérations pouvant constituer l'infraction prévue par les articles 343, 344, 389-1 à 389-5 du Code pénal, figurant sur une liste établie par arrêté ministériel est soumise à une autorisation délivrée par le Ministre d'État dans les conditions définies par ordonnance souveraine.
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.	**Loi n° 1.474 du 2 juillet 2019 relative à la sauvegarde de justice, au mandat de protection future et à l'exercice de l'activité de mandataire judiciaire à la protection des personnes.**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Code de procédure pénal, Article 268-10 - (Créé par la loi n° 1.435 du 8 novembre 2016)** Sur demande de l'officier de police judiciaire, qui peut intervenir par voie informatique, les organismes publics ou les personnes morales de droit privé mettent à sa disposition les informations utiles à la manifestation de la vérité, à l'exception de celles protégées par un secret prévu par la loi, contenues dans le ou les systèmes informatiques ou traitements d'informations nominatives qu'ils administrent. L'officier de police judiciaire, intervenant sur réquisition du procureur général ou sur autorisation expresse du juge d'instruction, peut requérir des opérateurs et des prestataires de services chargés de l'exploitation des réseaux et des services de télécommunications et de communications électroniques de prendre, sans délai, toutes mesures propres à assurer la préservation, pour une durée ne pouvant excéder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs et prestataires. Le fait, pour l'une des personnes visées à l'alinéa précédent, de refuser de répondre sans motif légitime à ces réquisitions est puni d'une peine d'un an d'emprisonnement et de l'amende prévue au chiffre 4 de l'article 26 du Code pénal . Les organismes ou personnes visés au présent article mettent à disposition les informations demandées ou requises par voie informatique dans les meilleurs délais. La peine encourue par les personnes morales est l'amende suivant les modalités prévues par l'article 29-2 du Code penal.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Une ordonnance souveraine détermine les catégories d'organismes visés au premier alinéa ainsi que les modalités d'interrogation, de transmission et de traitement des informations demandées ou requises.
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;	

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 necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.	**Code de procédure pénal, Article 255 - (Créé par la loi n° 1.435 du 8 novembre 2016)** Il procède, en opérant les perquisitions nécessaires, à la saisie des documents, données informatiques, papiers, lettres ou autres objets en la possession des personnes qui paraissent avoir participé aux faits incriminés ou qui sont susceptibles de détenir les pièces, informations ou objets s'y rapportant. Ces opérations ont lieu en présence des personnes chez lesquelles les perquisitions sont effectuées et, en cas d'empêchement, en présence d'un fondé de pouvoir désigné par elles ou, à défaut, de deux témoins. Il en est dressé procès-verbal. Le procureur général peut rechercher et saisir à la poste les lettres et lui interdire de délivrer au destinataire des télégrammes émanant de l'inculpé ou à lui adressés. Les documents, données informatiques, papiers, lettres ou autres objets saisis sont placés sous scellés après inventaire. Cependant, si leur inventaire sur place présente des difficultés, ils font l'objet de scellés fermés provisoires jusqu'au moment de leur inventaire et de leur mise sous scellés définitifs et ce, en présence des personnes qui ont assisté à la perquisition suivant les modalités prévues au deuxième alinéa. Le procureur général peut procéder à l'ouverture des scellés. Il en dresse inventaire dans un rapport qui doit mentionner toute ouverture ou réouverture des scellés. Lorsque les opérations sont terminées, le rapport et les scellés sont déposés au greffe général. Ce dépôt est constaté par procès-verbal. Lorsque la saisie porte sur des pièces de monnaie ou des billets de banque, ayant cours légal dans la Principauté ou à l'étranger, contrefaits, il doit transmettre pour

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	analyse et identification au moins un exemplaire de chaque type de pièces ou billets suspectés de faux à l'autorité qui sera désignée par ordonnance souveraine. Les dispositions du précédent alinéa ne sont pas applicables lorsqu'il n'existe qu'un seul exemplaire de type de pièces ou billets nécessaire à la manifestation de la vérité. Le procureur général ou, sous sa responsabilité, les officiers de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système d'information implanté sur les lieux où se déroule la perquisition, à des données intéressant l'instruction en cours et stockées dans ledit système ou 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 préalablement avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système d'informations situé en dehors du territoire national, elles sont recueillies par le procureur général, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur. Ainsi, il est procédé à la saisie des données informatiques nécessaires à la manifestation de la vérité en plaçant sous scellés soit le support physique de ces données, soit une copie réalisée en présence des personnes qui assistent à la perquisition. Si une copie est réalisée, il peut être procédé, sur instruction du procureur général, à l'effacement définitif, sur le support physique qui n'a pas été placé sous scellés, des données informatiques dont la détention ou l'usage est illégal ou dangereux pour la sécurité des personnes ou des biens. Le procureur général ne conserve que la saisie des documents, données informatiques, papiers, lettres ou autres objets utiles à la manifestation de la vérité. En outre, il pourra ordonner à toute personne connaissant le fonctionnement du système d'information ou les mesures appliquées pour protéger les données informatiques qu'il contient, de fournir toutes les informations raisonnablement nécessaires pour l'application du présent article.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Dans les lieux où un crime a été commis, il est interdit, sous peine de l'amende prévue au chiffre 1 de l'article 26, à toute personne non habilitée, de modifier avant les premières opérations de l'enquête judiciaire l'état des lieux et d'y effectuer des prélèvements quelconques. Toutefois, exception est faite lorsque ces modifications ou ces prélèvements sont commandés par les exigences de la sécurité ou de la salubrité publique, ou par les soins à donner aux victimes.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 21 – Interception of content data	**Loi n. 1.430 du 13/07/2016 portant diverses mesures relatives à la préservation de la sécurité nationale**

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Article 9 -** Les interceptions de correspondances émises par voie de communications électroniques autres que celles pratiquées à la demande de l'autorité judiciaire et sous son contrôle sont interdites sous peine d'un à cinq ans d'emprisonnement et de l'amende prévue au chiffre 4 de l'article 26 du Code pénal. De telles interceptions peuvent toutefois, à titre exceptionnel, être autorisées par le Ministre d'État dans les conditions prévues aux articles 14 à 16, lorsqu'elles ont pour finalité exclusive la recherche de renseignements intéressant: 1. la prévention du terrorisme, de la criminalité et de la délinquance organisées ainsi que de la prolifération des armes de destruction massive; 2. la défense des intérêts stratégiques de la politique extérieure de la Principauté, le respect de ses engagements internationaux, ainsi que la prévention de toute forme d'ingérence étrangère; 3. la sauvegarde des intérêts fondamentaux suivants de la Principauté : le maintien de son indépendance et de ses institutions, l'intégrité de son territoire, la sécurité et la sauvegarde de sa population, ainsi que la protection des éléments essentiels de son potentiel scientifique et économique. La mise en œuvre de ces interceptions ne peut concerner les lieux et les personnes visés à l'article 106-8 du Code de procédure pénale ni le véhicule, le bureau ou le domicile de ces mêmes personnes. Elle ne peut concerner non plus les locaux d'une entreprise de presse, d'une entreprise de communication audiovisuelle, d'une entreprise de communication au public en ligne, d'une agence de presse, les véhicules professionnels de ces entreprises ou agences ou le domicile d'un journaliste. Toutefois, par dérogation à l'alinéa précédent, et pour les finalités mentionnées au deuxième alinéa, lesdites interceptions peuvent être mises en œuvre après avis de la Commission visée à l'article 16, rendu préalablement à l'autorisation du Ministre d'État. **Article 10 -** Pour la réalisation des finalités mentionnées au deuxième alinéa de l'article 9, peut être autorisé, à titre exceptionnel, le recueil sur demande, auprès des opérateurs et prestataires de services chargés de l'exploitation des réseaux

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	et des services de télécommunications et de communications électroniques, des informations ou documents traités ou conservés, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications. Le recueil desdites informations et documents, y compris ceux relatifs à des personnes préalablement identifiées, peut être opéré, en temps réel, par accès direct aux réseaux des opérateurs et prestataires de services. Les modalités d'application du présent article sont définies par arrêté ministériel. **Article 11 -** Pour les seuls besoins de la prévention du terrorisme et sur demande du Directeur de la Sûreté Publique, le Ministre d'État peut imposer aux opérateurs et personnes mentionnées au premier alinéa de l'article 10, la mise en œuvre sur leurs réseaux, de traitements automatisés utilisant exclusivement les informations et documents visés à l'article 10, destinés à détecter des connexions susceptibles de révéler une menace terroriste sans permettre l'identification des personnes auxquelles les informations ou documents se rapportent. Si ladite menace est avérée, le Ministre d'État peut décider de la levée de l'anonymat des données, informations et documents y afférents dans les conditions prévues aux articles 14 à 16.
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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	**Loi n°1.222 du 28 décembre 1999 relative à l'extradition**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. 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	**Ordonnance n. 1.088 du 04/05/2007 rendant exécutoire la Convention européenne d'entraide judiciaire en matière pénale 20/04/1959**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:	

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 it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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: 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.	

Back to the Table of Contents

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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	Conformément à l'article 35 de la Convention de Budapest, un point de contact 24/7 a été établi dans le cadre du bureau d'INTERPOL, division de la police judiciaire.
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