Luxembourg

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 01 May 2020

[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.

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

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	
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	**Code pénal Art. 509-1** (L. 14 août 2000) Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement ou de transmission automatisé de

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	données sera puni d'un emprisonnement de deux mois à deux ans et d'une amende de 500 euros à 25.000 euros ou de l'une de ces deux peines. Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de quatre mois à deux ans et l'amende de 1.250 euros à 25.000 euros.
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 Art. 509-3** (L. 14 août 2000) Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement ou de transmission automatisé ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1.250 euros à 12.500 euros ou de l'une de ces deux peines. (L. 18 juillet 2014) Sera puni des mêmes peines celui qui aura intentionnellement et au mépris des droits d'autrui, intercepté des données lors de transmissions non publiques à destination, en provenance ou à l'intérieur d'un système de traitement ou de transmission automatisé de données.
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 Art. 509-3** (L. 14 août 2000) Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement ou de transmission automatisé ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1.250 euros à 12.500 euros ou de l'une de ces deux peines. (L. 18 juillet 2014) Sera puni des mêmes peines celui qui aura intentionnellement et au mépris des droits d'autrui, intercepté des données lors de transmissions non publiques à destination, en provenance ou à l'intérieur d'un système de traitement ou de transmission automatisé de données.
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	**Code pénal Art. 509-2** (L. 15 juillet 1993) Quiconque aura, intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement ou de transmission automatisé de données sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1.250 euros à 12.500 euros ou de l'une de ces

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	deux peines
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 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.	**Code pénal** Art. 509-5 (L. 18 juillet 2014) Sera puni de 4 mois à cinq ans d'emprisonnement et d'une amende de 1.250 euros à 30.000 euros quiconque aura, dans une intention frauduleuse, produit, vendu, obtenu, détenu, importé, diffusé ou mis à disposition, • – un dispositif informatique destiné à commettre l'une des infractions visées aux articles 509-1 à 509-4; ou • – toute clef électronique permettant d'accéder, au mépris des droits d'autrui, à tout ou à partie d'un système de traitement ou de transmission automatisé de données.
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	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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 Art. 509-4** (L. 10 novembre 2006) Lorsque dans les cas visés aux articles 509-1 à 509-3, il y a eu transfert d'argent ou de valeur monétaire, causant ainsi une perte de propriété à un tiers dans un but de procurer un avantage économique à la personne qui commet l'infraction ou à une tierce personne, la peine encourue sera un emprisonnement de quatre mois à cinq ans et une amende de 1.250 euros à 30.000 euros.
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.	**Code pénal Art. 379** (L. 21 février 2013) Sera puni d'un emprisonnement d'un à cinq ans et d'une amende de 251 à 50.000 euros: 1° quiconque aura excité, facilité ou favorisé la débauche, la corruption ou la prostitution d'un mineur âgé de moins de dix-huit ans; 2° quiconque aura recruté, exploité, contraint, forcé, menacé ou eu recours à un mineur âgé de moins de dix-huit ans à des fins de prostitution, aux fins de la production de spectacles ou de matériel à caractère pornographique ou aux fins de participation à de tels spectacles, aura favorisé une telle action ou en aura tiré profit; 3° quiconque aura assisté à des spectacles pornographiques impliquant la participation d'un mineur âgé de moins de dix-huit ans;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	4° quiconque aura contraint ou forcé un mineur âgé de moins de dix-huit ans à se livrer à des activités sexuelles avec un tiers ou de le menacer à de telles fins. La tentative sera punie d'un emprisonnement de six mois à trois ans. Le fait sera puni de la réclusion de cinq à dix ans s'il a été commis envers un mineur âgé de moins de seize ans, et de la réclusion de dix à quinze ans s'il a été commis envers un mineur de moins de onze ans. La tentative sera punie d'un emprisonnement de six mois à quatre ans, si le fait a été commis envers un mineur âgé de moins de seize ans et d'un emprisonnement de six mois à cinq ans s'il a été commis envers un mineur de moins de onze ans.
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,	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	
Article 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.	
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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 d'instruction Criminelle Art. 48-25** Lorsqu'il y a des raisons de penser que des données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données, utiles à la manifestation de la vérité, sont susceptibles de perte ou de modification, le procureur d'Etat ou le juge d'instruction saisi peut faire procéder à la conservation rapide et immédiate, pendant un délai qui ne peut excéder 90 jours, de ces données.
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.	**Code d'instruction Criminelle Art. 67-1 (L. 18 juillet 2014)** (1) Lorsque le juge d'instruction estime qu'il existe des circonstances qui rendent le repérage de télécommunications ou la localisation de l'origine ou de la destination de télécommunications nécessaire à la manifestation de la vérité, et si les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement, il peut faire procéder, en requérant au besoin le concours technique de l'opérateur de télécommunications et/ou du fournisseur d'un service de télécommunications: 1. au repérage des données d'appel de moyens de télécommunication à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	2. à la localisation de l'origine ou de la destination de télécommunications. Dans les cas visés à l'alinéa 1, pour chaque moyen de télécommunication dont les données d'appel sont repérées ou dont l'origine ou la destination de la télécommunication est localisée, le jour, l'heure, la durée et, si nécessaire, le lieu de la télécommunication sont indiqués et consignés dans un procès-verbal. Le juge d'instruction indique les circonstances de fait de la cause qui justifient la mesure dans une ordonnance motivée qu'il communique au procureur d'Etat. Il précise la durée durant laquelle elle pourra s'appliquer, cette durée ne pouvant excéder un mois à dater de l'ordonnance, sans préjudice de renouvellement. (2) Chaque opérateur de télécommunications et chaque fournisseur d'un service de télécommunications communique les informations qui ont été demandées dans les meilleurs délais. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal. Toute personne qui refuse de prêter son concours technique aux réquisitions visées dans , est punie d'une amende de 100 à 5.000 euros.
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	**Code d'instruction Criminelle** Art. 66 (L. 18 juillet 2014) (1) Le juge d'instruction opère la saisie de tous les objets, documents, effets, données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données et autres choses visés à l'article 31 (3). (2) Les objets, documents, effets, données et autres choses saisis sont inventoriés dans le procès-verbal. Si leur inventaire sur place présente des difficultés, ils font l'objet de scellés jusqu'au moment de leur inventaire, en présence des personnes qui ont assisté à la perquisition. (3) La saisie des données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données peut se faire, soit par la

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	saisie du support physique de ces données, soit par une copie de ces données réalisée en présence des personnes qui assistent à la perquisition. Si une copie est réalisée, le juge d'instruction peut ordonner l'effacement définitif sur le support physique, lorsque celui-ci se trouve au Grand- Duché de Luxembourg et qu'il n'a pas été placé sous la main de la justice, des données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données dont la détention ou l'usage est illégal ou dangereux pour la sécurité des personnes ou des biens. (4) Le juge d'instruction peut, par ordonnance motivée, enjoindre à une personne, hormis la personne visée par l'instruction, dont il considère qu'elle a une connaissance particulière du système de traitement ou de transmission automatisé de données ou du mécanisme de protection ou de cryptage, qu'elle lui donne accès au système saisi, aux données saisies contenues dans ce système ou aux données saisies accessibles à partir de ce système ainsi qu'à la compréhension de données saisies protégées ou cryptées. Sous réserve des articles 72, 73 et 76 ci-dessous, la personne désignée est tenue de prêter son concours. (5) Le procès-verbal des perquisitions et des saisies est signé par l'inculpé, par la personne au domicile de laquelle elles ont été opérées et par les personnes qui y ont assisté; en cas de refus de signer, le procès-verbal en fait mention. Il leur est laissé copie du procès-verbal. (6) Les objets, documents, effets, données et autres choses saisis sont déposés au greffe ou confiés à un gardien de saisie. (7) (L. du 1er août 2018) Nul ne peut valablement disposer des biens saisis dans le cadre d'une procédure pénale. À compter de la date à laquelle elle devient opposable et jusqu'à sa mainlevée ou la confiscation du bien saisi, la saisie pénale suspend ou interdit toute procédure civile d'exécution sur le bien objet de la saisie pénale. Pour l'application du présent article, le créancier ayant diligenté une procédure d'exécution antérieurement à la saisie pénale est de plein droit considéré comme

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	titulaire d'une sûreté sur le bien, prenant rang à la date à laquelle cette procédure d'exécution est devenue opposable. Le présent paragraphe est également applicable aux saisies opérées sur base des articles 31 et 47.
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 d'instruction Criminelle Art. 31** (L. 16 juin 1989) (1)En cas de crime flagrant, l'officier de police judiciaire qui en est avisé informe immédiatement le procureur d'Etat, se transporte sans délai sur le lieu du crime et procède à toutes constatations utiles. (2)Il veille à la conservation des indices susceptibles de disparaître et de tout ce qui peut servir à la manifestation de la vérité. (3)(L. 18 juillet 2014) Il saisit les objets, documents, données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données et effets qui ont servi à commettre le crime ou qui étaient destinés à le commettre et ceux qui ont formé l'objet du crime, de même que tout ce qui paraît avoir été le produit du crime, ainsi qu'en général, tout ce qui paraît utile à la manifestation de la vérité ou dont l'utilisation serait de nature à nuire à la bonne marche de l'instruction et tout ce qui est susceptible de confiscation ou de restitution. **Code d'instruction Criminelle Art. 33(L. 18 juillet 2014)** (1)Si la nature du crime est telle que la preuve en puisse être acquise par la saisie des papiers, documents, données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données ou autres objets en la possession des personnes qui paraissent avoir participé au crime ou détenir des pièces, données ou objets relatifs aux faits incriminés, l'officier de police judiciaire se transporte sans désemparer au domicile de ces dernières pour y procéder à une perquisition dont il dresse procès-verbal et opérer la saisie. Cette perquisition peut avoir lieu à toute heure du jour ou de la nuit. (2)Il a seul, avec les personnes désignées à l' article 34 et celles auxquelles il a éventuellement recours en application de l' article 36, le droit de prendre connaissance des papiers, données ou documents avant de procéder à leur saisie.

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.	(3)Toutefois, il a l'obligation de provoquer préalablement toutes mesures utiles pour que soit assuré le respect du secret professionnel et des droits de la défense. (4)Tous objets, données et documents saisis sont immédiatement inventoriés après avoir été présentés, pour reconnaissance, aux personnes qui paraissent avoir participé à l'infraction, si elles sont présentes, ainsi qu'aux personnes visées à l' article suivant. Cependant, si leur inventaire sur place présente des difficultés, ils font l'objet de scellés jusqu'au moment de leur inventaire en présence des personnes qui ont assisté à la perquisition. (5)La saisie des données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données peut se faire, soit par la saisie du support physique de ces données, soit par une copie de ces données réalisée en présence des personnes visées à l' article suivant. Si une copie est réalisée, il peut être procédé, sur demande du Procureur d'Etat, à l'effacement définitif sur le support physique, lorsque celui-ci se trouve au Grand-Duché de Luxembourg et qu'il n'a pas été placé sous la main de la justice, des données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données dont la détention ou l'usage est illégal ou dangereux pour la sécurité des personnes ou des biens
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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: 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.	**Code de procédure pénale** **Art. 88-1.** (L. 26 novembre 1982) (L. du 27 juin 2018) (1) Le juge d'instruction peut, sous les conditions prévues aux articles 88-2 et 88-4, ordonner l'utilisation de moyens techniques de surveillance et de contrôle de toutes les formes de communication. Celle-ci s'effectue au moyen : 1° de la surveillance et du contrôle des télécommunications ainsi que de la correspondance postale ; 2° de la sonorisation et de la fixation d'images de certains lieux ou véhicules ; 3° de la captation de données informatiques. (2) La sonorisation et la fixation d'images de certains lieux ou véhiculés consistent dans la mise en place d'un dispositif technique ayant pour objet, sans le consentement des intéressés, la captation, la fixation, la transmission et l'enregistrement des paroles prononcées par une ou plusieurs personnes à titre privé ou confidentiel, dans un lieu public, un véhicule, un local utilisé à des fins professionnelles ou un domicile ou ses dépendances au sens des articles 479, 480 et 481 du Code pénal ou, au moyen d'un dispositif technique placé dans un local

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	utilisé à des fins professionnelles, un domicile ou ses dépendances ou un véhicule de l'image d'une ou de plusieurs personnes se trouvant dans ces lieux. (3) La captation de données informatiques consiste dans la mise en place d'un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement ou de transmission automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels. **Art. 88-2.** (L. 30 mai 2005) (L. du 27 juin 2018) (1) Les mesures visées à l'article 88-1 ne peuvent être décidées par le juge d'instruction qu'à titre exceptionnel et par décision spécialement motivée d'après les éléments de l'espèce et par référence aux conditions indiquées au paragraphe 2. (2) Elles sont subordonnées aux conditions : 1° que la poursuite pénale a pour objet, s'agissant de la surveillance et du contrôle des télécommunications ainsi que de la correspondance postale, en tout ou en partie, un fait d'une gravité particulière emportant une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à deux ans d'emprisonnement, et, s'agissant de la sonorisation et de la fixation d'images des lieux et véhicules visés à l'article 88-1, paragraphe 2, et de la captation de données informatiques, en tout ou en partie, un ou plusieurs des faits énumérés ci-après : a) crimes et délits contre la sûreté de l'État au sens des articles 101 à 123 du Code pénal ; b) actes de terrorisme et de financement de terrorisme au sens des articles 135-1 à 135-6, 135-9 et

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	135-11 à 135-16 du Code pénal ; 2° que des faits déterminés rendent la personne à surveiller suspecte, soit d'avoir commis l'infraction ou d'y avoir participé, soit de recevoir ou de transmettre des informations destinées à l'inculpé ou au suspect ou qui proviennent de lui ; 3°que les moyens ordinaires d'investigation s'avèrent inopérants en raison de la nature des faits et des circonstances spéciales de l'espèce. (3) La décision du juge d'instruction est écrite et contient, sous peine de nullité, les mentions suivantes : 1°la motivation spéciale d'après les éléments de l'espèce et par référence aux conditions indiquées au paragraphe 2 ; 2. 2° le nom ou, s'il n'est pas connu, une description aussi précise que possible de la ou des personnes visées par les mesures ordonnées ; 3. 3° la manière dont les mesures seront exécutées ; 4. 4° la période durant laquelle les mesures pourront être exécutées au regard des dispositions du paragraphe 4; 5. 5° le nom et la qualité de l'officier de police judiciaire qui procède à l'exécution de l'enquête. (4) Elles doivent être levées dès qu'elles ne sont plus nécessaires. Elles cessent de plein droit un mois à compter de la date de l'ordonnance. Elles peuvent toutefois être prorogées chaque fois pour un mois, sans que la durée totale puisse dépasser un an, par ordonnance motivée du juge d'instruction, approuvée par le président de la chambre du conseil de la cour d'appel qui statue dans les deux jours de la réception de l'ordonnance, le procureur général d'État entendu en ses conclusions. (5) Elles ne peuvent, à peine de nullité, être ordonnées à l'égard d'un inculpé après son premier interrogatoire par le juge d'instruction et celles ordonnées antérieurement cessent leurs effets de plein droit à cette date. (6) Ces mesures ne peuvent, à peine de nullité, être ordonnées à l'égard d'une personne liée par le secret professionnel au sens de l'article 458 du Code pénal, à

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	moins qu'elle ne soit elle-même suspecte d'avoir commis l'infraction ou d'y avoir participé. Les mesures ne peuvent, à peine de nullité, être ordonnée à l'égard d'un avocat ou d'un médecin sans que le bâtonnier ou le représentant du Collège médical, selon le cas, en soit averti. Ces mêmes personnes sont informées par le juge d'instruction des éléments des communications recueillis qu'il estime relever du secret professionnel et qui ne sont pas consignés au procès-verbal prévu par l'article 88-4, paragraphe 4. La mise en place du dispositif technique mentionné aux paragraphes 2 et 3 de l'article 88-1 ne peut, à peine de nullité, être réalisée dans les locaux utilisés à des fins professionnelles, le domicile ou ses dépendances au sens des articles 479, 480 et 481 du Code pénal ou le véhicule d'un avocat, d'un médecin, d'un journaliste professionnel ou d'un éditeur, ces deux derniers termes compris au sens défini par la loi modifiée du 8 juin 2004 sur la liberté d'expression dans les médias, ou concerner les systèmes automatisés de traitement de données se trouvant dans ces lieux. (7) Les mesures ne peuvent, à peine de nullité, pas avoir d'autre objet que l'information sur les infractions visées dans les décisions du juge d'instruction. Le fait qu'elles révèlent des infractions autres que celles visées dans ces décisions ne constitue pas une cause de nullité des procédures incidentes.
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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	
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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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