Algeria

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version [27.03.2020]

[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.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

State:	
Signature of the Budapest Convention:	No
Ratification/accession:	No

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	**Loi n°09-04 du 5 août 2009, article 2. Terminologie** Au sens de la présente loi, on entend par : a - Infractions liées aux technologies de l'information et de la communication : les infractions portant atteinte aux systèmes de traitement automatisé de données telles que définies par le code pénal ainsi que toute autre infraction commise ou dont la commission est facilitée par un système informatique ou un système de communication électronique. b - Système informatique : tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données. c - 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. d - Fournisseurs de services : 1 - toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique et/ou d'un système de télécommunication ; 2 - et toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs. e - Données relatives au trafic : toute donnée ayant trait à une communication passant par un système informatique, produite par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ainsi que le type de service. f - Communications électroniques : toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de renseignements de toute nature, par tout moyen électronique.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 394 bis (nouveau)** -Est puni d'une peine d'emprisonnement de trois (3) mois à un (1) an et d'une amende de cinquante mille (50.000) DA à cent mille (100.000) DA, quiconque accède ou se maintient, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données, ou tente de le faire. La peine est portée au double, lorsqu'il en est résulté soit la suppression soit la modification de données contenues dans le système. Lorsqu'il en est résulté une altération du fonctionnement de ce système, la peine est de six (6) mois à deux (2) ans d'emprisonnement et d'une amende de cinquante mille (50.000) DA à cent cinquante mille(150.000) DA **Loi n° 08-01 du 23 janvier 2008 complétant la loi n° 83-11 du 2 juillet 1983 relative aux assurances sociales :** **Article 4**. Les dispositions de la loi n° 83-11 du 2 juillet 1983, susvisée, sont complétées par un titre V bis intitulé "Dispositions pénales" comprenant les articles 93 quater, 93 quinquiès, 93 sixiès, 93 septiès et 93 octiès, rédigés comme suit : **Article 93 quater.** Sans préjudice des sanctions prévues par la législation en vigueur, est puni d'un emprisonnement de deux (2) ans à cinq (5) ans et d'une amende de 100.000 DA à 200.000 DA, quiconque remet ou se fait remettre aux fins d'un usage illégal la carte électronique de l'assuré social ou la clé électronique de la structure de soins ou la clé électronique du professionnel de la santé ».
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 303 bis (nouveau)** Est puni d'un emprisonnement de six (6) mois à trois (3) ans et d'une amende de cinquante mille (50.000) DA à trois cent mille (300.000) DA, quiconque, au moyen d'un procédé quelconque, porte volontairement atteinte à l'intimité de la vie privée d'autrui : 1 - en captant, enregistrant ou transmettant sans l'autorisation ou le consentement de leur auteur, des communications, des paroles prononcées à titre privé ou confidentiel. 2 - en prenant, enregistrant ou transmettant sans l'autorisation ou le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	La tentative du délit prévu par le présent article est punie des mêmes peines que l'infraction consommée. Le pardon de la victime met fin aux poursuites pénales. **Code pénal, article 303 bis 1 (nouveau)** Est punie des peines prévues à l'article précédent toute personne qui conserve, porte ou laisse porter à la connaissance du public ou d'un tiers ou utilise de quelque manière que ce soit, tout enregistrement, image ou document obtenu, à l'aide de l'un des actes prévus par l'article 303 bis de la présente loi. Si le délit prévu à l'alinéa précédent est commis par voie de presse, les dispositions particulières prévues par les lois y afférentes pour déterminer les personnes responsables sont applicables. La tentative du délit prévu par le présent article est punie des mêmes peines que l'infraction consommée. Le pardon de la victime met fin aux poursuites pénales.
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 394 bis (nouveau)** Est puni d'une peine d'emprisonnement de trois (3) mois à un (1) an et d'une amende de cinquante mille (50.000) DA à cent mille (100.000) DA, quiconque accède ou se maintient, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données, ou tente de le faire. La peine est portée au double, lorsqu'il en est résulté soit la suppression soit la modification de données contenues dans le système. Lorsqu'il en est résulté une altération du fonctionnement de ce système, la peine est de six (6) mois à deux (2) ans d'emprisonnement et d'une amende de cinquante mille (50.000) DA à cent cinquante mille(150.000) DA. Code pénal, article 394 ter (nouveau) Est puni d'un emprisonnement de six (6) mois à trois (3) ans et d'une amende de cinq cents mille (500.000) DA à deux millions (2.000.000) de DA, quiconque introduit frauduleusement des données dans un système de traitement automatisé ou supprime ou modifie frauduleusement les données qu'il contient. Loi n° 08-01 du 23 janvier 2008 complétant la loi n° 83-11 du 2 juillet 1983 relative aux assurances sociales :

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Article 4 (article 93 quinquiès de la loi du 2 juillet 1983) - Sans préjudice des sanctions prévues par la législation en vigueur, est puni d'un emprisonnement de deux (2) ans à cinq (5) ans et d'une amende de 500.000 DA à 1.000.000 DA, quiconque effectue frauduleusement toute modification ou suppression totale ou partielle des données techniques et/ou administratives insérées dans la carte électronique de l'assuré social ou dans la clé électronique de la structure de soins ou dans la clé électronique du professionnel de la santé. [...]
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 394 bis (nouveau)** -Est puni d'une peine d'emprisonnement de trois (3) mois à un (1) an et d'une amende de cinquante mille (50.000) DA à cent mille (100.000) DA, quiconque accède ou se maintient, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données, ou tente de le faire. La peine est portée au double, lorsqu'il en est résulté soit la suppression soit la modification de données contenues dans le système. Lorsqu'il en est résulté une altération du fonctionnement de ce système, la peine est de six (6) mois à deux (2) ans d'emprisonnement et d'une amende de cinquante mille (50.000) DA à cent cinquante mille(150.000) DA.
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.	**Code pénal, article 394 quater (nouveau)** Est puni d'un emprisonnement de deux (2) mois à trois (3) ans et d'une amende de un million (1.000.000) de DA à cinq millions (5.000.000) de DA, quiconque volontairement et frauduleusement :1°) - conçoit, recherche, rassemble, met à disposition, diffuse ou commercialise des données qui sont stockées, traitées ou transmises par un système informatique, et par lesquelles les infractions prévues par la présente section peuvent être commises,2°) - détient, révèle, divulgue, ou fait un usage quelconque des données obtenues par l'une des infractions prévues par la présente section. **Loi n° 08-01 du 23 janvier 2008 complétant la loi n° 83-11 du 2 juillet 1983 relative aux assurances sociales :** **Article 4 (article 93 quinquiès de la loi du 2 juillet 1983)** - Est puni [...] [d'un emprisonnement de deux (2) ans à cinq (5) ans et d'une amende de 500.000 DA à 1.000.000 DA] quiconque élabore, modifie ou reproduit de manière illicite les logiciels permettant d'accéder ou d'utiliser les données contenues dans la carte électronique de l'assuré social ou dans la clé électronique de la structure de soins ou dans la clé électronique du professionnel de la santé.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	**Article 4 (article 93 sixiès de la loi du 2 juillet 1983)** -Sans préjudice des sanctions prévues par la législation en vigueur, est puni d'un emprisonnement de deux (2) ans à cinq (5) ans et d'une amende de 500.000 DA à 5.000.000 DA, quiconque reproduit, fabrique, détient ou met en circulation, de manière illicite, la carte électronique de l'assuré social ou la clé électronique de la structure de soins ou la clé électronique du professionnel de la santé ».
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**Code pénal - Chapitre 7 – Les faux (dispositions non spécifiques)** **Article 216 (modifié)** - Est punie de la réclusion à temps de dix (10) à vingt (20) ans et d'une amende de un million (1.000.000) de DA à deux millions (2.000.000) de DA, toute personne autre que celles désignées à l'article 215, qui commet un faux en écriture authentique ou publique: 1- soit par contrefaçon ou altération d'écriture ou de signature ; 2- soit par fabrication de conventions, dispositions, obligations ou décharges ou par leur insertion ultérieure dans ces actes ; 3- soit par addition, omission ou altération de clauses, de déclarations ou de faits que ces actes avaient pour objet de recevoir et de constater ; 4- soit par supposition ou substitution de personnes. **Article 219.** - Toute personne qui de l'une des manières prévues à l'article 216 commet ou tente de commettre un faux en écritures de commerce ou de banque est punie d'un emprisonnement d'un (1) à cinq (5) ans et d'une amende de cinq cents (500) à vingt mille (20.000) DA. Le coupable peut, en outre, être frappé de l'interdiction de l'un ou plusieurs des droits mentionnés à l'article 14 et d'une interdiction de séjour d'un (1) à cinq (5) ans au plus. La peine peut être portée au double du maximum prévu au premier alinéa lorsque le coupable de l'infraction est un banquier, un administrateur de société et, en général, une personne ayant fait appel au public en vue de l'émission d'actions, obligations, bons, parts ou titres quelconques, soit d'une société, soit

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	d'une entreprise commerciale ou industrielle. **Article 220**. - Toute personne qui de l'une des manières prévues à l'article 216, commet ou tente de commettre un faux en écritures privées est punie d'un emprisonnement d'un (1) à cinq (5) ans et d'une amende de cinq cents (500) à deux mille (2.000) DA. Le coupable peut, en outre, être frappé de l'interdiction de l'un ou plusieurs des droits mentionnés à l'article 14 et d'une interdiction de séjour d'un (1) an à cinq (5) ans au plus. **Article 221.** - Dans les cas visés à la présente section, celui qui fait usage ou tente de faire usage de la pièce qu'il savait fausse est puni des peines réprimant le faux, suivant les distinctions prévues aux articles 219 et 220.
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 - Chapitre 3, Section 2 - Escroquerie et émission de chèques sans provision et Section 3 - Abus de confiance** (dispositions non spécifiques) **Article 376.** - Quiconque de mauvaise foi détourne ou dissipe au préjudice des propriétaires, possesseurs ou détenteurs, des effets, deniers, marchandises, billets, quittances, ou tous autres écrits contenant ou opérant obligation ou décharge, qui ne lui ont été remis qu'à titre de louage, de dépôt, de mandat, de nantissement, de prêt à usage, ou pour un travail salarié ou non salarié, a la charge de les rendre ou représenter, ou d'en faire un usage ou un emploi déterminé, est coupable d'abus de confiance et puni d'un emprisonnement de trois (3) mois à trois (3) ans et d'une amende de cinq cents (500) à vingt mille (20.000) DA. Le coupable peut, en outre, être frappé pour un (1) an au moins et cinq (5) ans au plus de l'interdiction d'un ou plusieurs des droits mentionnés à l'article 14 et de l'interdiction de séjour. Le tout sans préjudice de ce qui est dit aux articles 158 et 159 relativement aux soustractions et enlèvement de derniers, effets, ou pièces dans les dépôts publics.
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	**Code pénal, article 333 bis** Est puni d'un emprisonnement de deux (2) mois à deux (2) ans et d'une amende de cinq cent (500) à deux mille (2000) DA quiconque aura fabriqué, détenu, importé ou fait importer en vue de faire commerce, distribution, location, affichage ou exposition, expose ou tente d'exposer aux regards du public, vendu ou tenté de vendre, distribué ou tenté de distribuer, tous

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	imprimés, écrits, dessins, affiches, gravures, peintures, photographies, clichés, matrices, ou reproductions, tous objets contraires à la décence. **Code pénal, article 333 bis 1 (nouveau)** Est puni d'un emprisonnement de cinq (5) ans à dix (10) ans et d'une amende de 500.000 DA à 1.000.000 DA quiconque, représente, par quelque moyen que ce soit, un mineur de moins de dix-huit (18) ans s'adonnant à des activités sexuelles explicites, réelles ou simulées, ou représente des organes sexuels d'un mineur, à des fins principalement sexuelles, ou fait la production, la distribution, la diffusion, la propagation, l'importation, l'exportation, l'offre, la vente ou la détention des matériels pornographiques mettant en scène des mineurs. En cas de condamnation, la juridiction prononce la confiscation des moyens qui ont servi à la commission de l'infraction ainsi que les biens obtenus de façon illicite, sous réserve des droits des tiers de bonne foi. **Code pénal, article 334. (modifié)** Est puni d'un emprisonnement de cinq (5) à dix (10) ans, tout attentat à la pudeur consommé ou tenté sans violence, sur la personne d'un mineur de 16 ans de l'un ou de l'autre sexe. Est puni de la réclusion à temps de cinq (5) à dix (10) ans, l'attentat à la pudeur commis par tout ascendant, sur la personne d'un mineur, même âgé de plus de 16 ans, mais non émancipé par le mariage.
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	**Ordonnance n°03-05 du 19 juillet 2003 relative aux droits d'auteur et aux droits voisins, chapitre II,** **Article 151** Est coupable du délit de contrefaçon quiconque : — divulgue illicitement une œuvre ou porte atteinte à l'intégrité d'une œuvre ou d'une prestation d'artiste interprète ou exécutant ; — reproduit une œuvre ou une prestation par quelque procédé que ce soit sous forme d'exemplaires contrefaits ; — importe ou exporte des exemplaires contrefaits d'une œuvre ou prestation ; — vend des exemplaires contrefaits d'une œuvre ou prestation ; — loue ou met en circulation des exemplaires contrefaits d'une œuvre ou

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	prestation. **Article 152** Est coupable du délit de contrefaçon, quiconque, en violation des droits protégés en vertu de la présente ordonnance, communique l'œuvre ou la prestation, par représentation ou exécution publique, radiodiffusion sonore ou audiovisuelle, câblodistribution ou tout autre moyen transmetteur de signes porteurs de sons ou d'images ou sons ou par tout système de traitement informatique. **Article 153** Le coupable du délit de contrefaçon d'une oeuvre ou d'une prestation, tel que prévu aux articles 151 et 152 ci-dessus est puni d'un emprisonnement de six (6) mois à trois (3) ans et d'une amende de cinq cent mille (500 000 DA) à un million (1.000. 000 DA) de dinars que la publication ait lieu en Algérie ou à l'étranger. **Article 154** Est coupable du délit prévu à l'article 151 de la présente ordonnance et encourt la peine prévue à l'article 153 ci-dessus quiconque concourt, par son action ou les moyens en sa possession, à porter atteinte aux droits d'auteur ou à tout titulaire de droits voisins. **Article 155** Est coupable du délit de contrefaçon et puni de la même peine prévue à l'article 153 ci-dessus, quiconque, en violation des droits reconnus, refuse délibérément de payer à l'auteur ou à tout autre titulaire de droits voisins la rémunération due au titre des droits prévus par la présente ordonnance. **Article 156** En cas de récidive, la peine prévue à l'article 153 de la présente ordonnance est portée au double. La juridiction compétente peut, en outre, prononcer la fermeture temporaire, pour une durée n'excédant pas six (6) mois, de l'établissement exploité par le contrefacteur ou son complice, ou le cas échéant, la fermeture définitive.
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	**Code pénal, article 394 noniès (nouveau)** La tentative des délits prévus à la présente section est punie des mêmes peines prévues pour le délit lui-même **Loi n° 08-01 du 23 janvier 2008 complétant la loi n° 83-11 du 2 juillet**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**1983 relative aux assurances sociales :** **Article 4 (article 93 quinquiès de la loi du 2 juillet 1983)** [...] Est punie de la même peine, la tentative des délits cités aux alinéas 1er et 2ème ci-dessus ». **Code pénal, articles 42-46** **Article 42 (modifié)** Sont considérés comme complices d'une infraction ceux qui, sans participation directe à cette infraction, ont, avec connaissance, aidé par tous moyens ou assisté l'auteur ou les auteurs de l'action dans les faits qui l'ont préparée ou facilitée, ou qui l'ont consommée. **Article 43** Est assimilé au complice celui qui, connaissant leur conduite criminelle, a habituellement fourni logement, lieu de retraite ou de réunions à un ou plusieurs malfaiteurs exerçant des brigandages ou des violences contre la sûreté de l'Etat, la paix publique, les personnes ou les propriétés. **Article 44** Le complice d'un crime ou d'un délit est punissable de la peine réprimant ce crime ou ce délit. Les circonstances personnelles d'où résultent aggravation, atténuation ou exemption de peine n'ont d'effet qu'à l'égard du seul participant auquel elles se rapportent. Les circonstances objectives, inhérentes à l'infraction, qui aggravent ou diminuent la peine de ceux qui ont participé à cette infraction, ont effet à leur charge ou en leur faveur, selon qu'ils en ont eu ou non connaissance. La complicité n'est jamais punissable en matière contraventionnelle. **Article 45** Celui qui a déterminé une personne, non punissable en raison d'une condition ou d'une qualité personnelle, à commettre une infraction, est passible des peines réprimant l'infraction. **Article 46** Lorsque l'infraction projetée n'aura pas été commise par le seul fait de l'abstention volontaire de celui qui devait la commettre, l'instigateur encourra néanmoins les peines prévues pour cette infraction.
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal	**Code pénal, article 51 bis (nouveau)** La personne morale, à l'exclusion de l'Etat, des collectivités locales et des personnes morales de droit public, est responsable pénalement, lorsque la loi le

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	prévoit, des infractions commises, pour son compte, par ses organes ou représentants légaux. La responsabilité pénale de la personne morale n'exclut pas celle de la personne physique auteur ou complice des mêmes faits. **Code pénal, article 394 sixiès (nouveau)** La personne morale qui a commis une infraction prévue par la présente section est punie d'une amende qui équivaut à cinq (5) fois le maximum de l'amende prévue pour la personne physique **Loi n° 08-01 du 23 janvier 2008 complétant la loi n° 83-11 du 2 juillet 1983 relative aux assurances sociales :** **Article 4 (article 93 septiès de la loi du 2 juillet 1983)** - Toute personne morale qui a commis l'un des délits prévus par les articles 93 quinquiès et 93 sixiès ci-dessus est passible d'une amende égale à cinq (5) fois le montant maximal de l'amende prévue pour la personne physique ».
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.	**Article 394 septiès (nouveau)** Quiconque participe à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par la présente section est puni des peines prévues pour l'infraction elle-même. **Code pénal, article 394 octiès (nouveau)** Sans préjudice des droits des tiers de bonne foi, il sera procédé à la confiscation des instruments, programmes et moyens utilisés dans la commission de l'infraction ainsi qu'à la fermeture des sites, objet de l'une des infractions prévues à la présente section, et des locaux et lieux d'exploitation dans le cas où le propriétaire en est informé. **Code pénal, article 18 bis (modifié)** Les peines encourues par la personne morale en matière criminelle et délictuelle sont : 1- L'amende dont le taux est d'une (1) à cinq (5) fois le maximum de l'amende prévue pour les personnes physiques, par la loi qui réprime l'infraction. 2 - Une ou plusieurs des peines complémentaires suivantes : - la dissolution de la personne morale ; - la fermeture de l'établissement ou de l'une de ses annexes pour une durée qui ne peut excéder cinq (5) ans ; - l'exclusion des marchés publics pour une durée qui ne peut excéder cinq (5)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	ans ; - l'interdiction, à titre définitif ou pour une durée qui ne peut excéder cinq (5) ans, d'exercer directement ou indirectement, une ou plusieurs activités professionnelles ou sociales ; - la confiscation de la chose qui a servi à commettre l'infraction ou de la chose qui en est le produit ; - l'affichage et la diffusion du jugement de condamnation ; - le placement, pour une durée qui ne peut excéder cinq (5) ans, sous surveillance judiciaire pour l'exercice de l'activité conduisant à l'infraction ou à l'occasion de laquelle cette infraction a été commise. **Article 4 (article 93 octiès de la loi du 2 juillet 1983)** — . Sans préjudice des droits des tiers de bonne foi, il est procédé à la confiscation des appareils et des moyens utilisés, ainsi qu'à la fermeture des locaux et des lieux d'exploitation objet des délits cités aux articles 93 quinquiès et 93 sixiès ci-dessus dans le cas où le propriétaire en est informé
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.	De nombreuses garanties ont été mises en œuvre, même si des faiblesses peuvent encore être constatées. Outre une définition plus nette, indiquée ci-dessus, des principes directeurs de l'enquête et du procès pénal, trois textes principaux ont réaffirmé certains droits fondamentaux en en précisant l'étendue : • La loi organique n° 12-05 du 12 janvier 2012 relative à l'information, ayant pour objet de fixer les principes et les règles de l'exercice du droit à l'information et à la liberté de la presse. • La loi n° 17-07 du 27 mars 2017 modifiant et complétant l'ordonnance n° 66-155 du 8 juin 1966 portant Code de procédure pénale. Cette loi réaffirme les principes de légalité, du procès équitable et du respect de la dignité et droits humains, précise en conséquence des principes de procédure pénale, apporte des précisions sur l'action publique, les missions de la police judiciaire et les contrôles dont elle fait l'objet, la mise en liberté des prévenus, le jugement des manquements des officiers de police judiciaire dans l'exercice de leurs fonctions, les compétences et composition des juridictions de première et de deuxième instance en matière de jugement des crimes et autres infractions connexes, la procédure devant ces juridictions. • La loi organique n° 17-06 du 27 mars 2017 modifiant la loi organique n° 05-11 du 17 juillet 2005 relative à l'organisation judiciaire, principalement aux

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	fins de clarifier l'existence d'un double degré de juridiction (suite à l'avis n° 01/A.L.O/CC/17 du 16 mars 2017 relatif au contrôle de conformité de la loi organique modifiant la loi organique n° 05-11 du 17 juillet 2005 relative à l'organisation judiciaire à la Constitution). Par ailleurs, la Constitution révisée en mars 2016 garantit expressément différents droits et libertés incluant les suivants : • L'égalité devant la loi « *sans distinction de race, de sexe, d'opinion ou de toute autre condition ou circonstance personnelle ou sociale* » (article 32). • Les « *libertés fondamentales et les droits de l'Homme et du Citoyen* » (article 38). • La liberté de conscience et la liberté d'opinion, l'exercice du culte étant garanti dans le respect de la loi (article 39). • La liberté d'investissement et de commerce (article 43). • La liberté de création intellectuelle, artistique et scientifique, incluant les droits d'auteurs, les libertés académiques et la liberté de recherche scientifique (article 44). • Le droit à l'enseignement (article 65) et à la culture (article 45). • La vie privée et l'honneur du citoyen, incluant « *le secret de la correspondance et de la communication privées, sous toutes leur formes* », étant précisé qu' « *aucune atteinte à ces droits n'est tolérée sans une réquisition motivée de l'autorité judiciaire* », la loi punissant « *toute violation de cette disposition* » (article 46). • La protection des personnes physiques dans le traitement des données à caractère personnel, qui est « u*n droit fondamental* » (article 46). • L'inviolabilité du domicile, la perquisition ne pouvant « *intervenir que sur ordre écrit émanant de l'autorité judiciaire compétente* » (article 47). • Les libertés d'expression, d'association et de réunion (article 48). • La « l*iberté de la presse écrite, audiovisuelle et sur les réseaux d'information* », qui ne peut être « r*estreinte par aucune forme de censure préalable* ». La « *diffusion des informations, des idées, des images et des opinions en toute liberté est garantie dans le cadre de la loi et du respect des constantes et des valeurs religieuses, morales et culturelles de la Nation* », mais le « *délit de presse ne peut être sanctionné par une peine privative de liberté* » (article 50).

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	• La présomption d'innocence et le droit à un procès équitable (article 56). • La légalité des délits et des peines (article 58). • La liberté physique (article 59), la Constitution déterminant les limites de la garde à vue et les droits fondamentaux du gardé à vue (article 60). • Le droit à réparation de l'Etat en cas d'erreur judiciaire (article 61). • Le droit des enfants, protégés par « *la famille, la société et l'Etat* », la violence contre les enfants étant réprimée par la loi (article 72). • Le droit à la défense (article 169) et à la protection de l'avocat contre toute forme de pression (article 170). Enfin, comme dans le cadre de la Constitution précédente, le pouvoir législatif légifère en matière de droits fondamentaux et le pouvoir judiciaire est garant de la sauvegarde de ces droits. La Constitution de 2016 renforce par ailleurs les droits du Parlement, notamment de l'opposition parlementaire qui jouit notamment d'une « *participation effective* » aux travaux législatifs et au contrôle de l'action gouvernementale et du droit de saisir le Conseil constitutionnel conformément à la Constitution (article 114). La Constitution de 2016 renforce également l'indépendance du pouvoir judiciaire, notamment en affirmant l'inamovibilité des juges du siège dans les conditions fixées par le statut de la magistrature (article 166). Toutefois, le Conseil supérieur de la magistrature (qui décide de la nomination et du déroulement de la carrière des magistrats - article 174) reste présidé par le Président de la République (article 173). En revanche, il convient de noter que l'ordonnance n° 15-02 du 23 juillet 2015 modifiant et complétant le code pénal prive de double degré de juridiction les jugements correctionnels et contraventionnels n'ayant pas prononcé de peine d'emprisonnement et, pour les délits, ayant prononcé une peine d'amende n'excédant pas certains montants (nouvel article 416 du code de procédure pénale, p. 36 de la loi[1]). Par ailleurs, si les pouvoirs et les limites des services d'enquête sont encadrés,

[1] Maître Mohamed Brahimi, *Les jugements non susceptibles d'appel en matière pénale*, 31 octobre 2017, http://brahimi-avocat.e-monsite.com/blog/les-jugements-non-susceptibles-d-appel-en-matiere-penale.html#Od3P0FLKUOz1HJTA.99.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	ils peuvent encore sembler disproportionnés à certains égards. Notamment : • En matière d'interception de correspondances selon le Code de procédure pénale (voir ci-dessous, en lien avec l'article 21 de la Convention de Budapest), l'autorisation doit « *comporter tous les éléments permettant d'identifier les liaisons à intercepter, les lieux d'habitation ou autres visés et l'infraction qui motive le recours à ces mesures ainsi que la durée de celles-ci* » et est donnée pour 4 mois renouvelables « *selon les nécessités de l'enquête ou de l'information dans les mêmes conditions de forme et de durée* » (article 65 bis 7) par le procureur de la République ou (en cas d'information judiciaire) par le juge d'instruction (article 65 bis 5 : des garanties existent donc mais la supervision d'un magistrat indépendant fait défaut). Ces opérations ne doivent pas porter préjudice au secret professionnel, mais « *la révélation des infractions autres que celles mentionnées dans l'autorisation du magistrat ne constitue pas une cause de nullité des procédures incidentes* » (article 65 bis 6, une telle possibilité semblant excéder le principe de stricte nécessité de l'ingérence). Les articles 65 bis 9 et 10 prévoient des garanties en termes de transparence de l'interception (transcription dans un procès-verbal des opérations d'interception et de mise en place des dispositifs y nécessaires, mentionnant les dates et heures de début et de fin ; description des conversations « *utiles à la manifestation de la vérité* »), mais la durée de conservation de ces éléments de même que la manière dont ils sont protégés des accès et utilisations illégitimes ne semblent pas réglementés. • Aux termes de la loi n°09-04 du 5 août 2004, les opérations de surveillance électronique peuvent être mises en place « *pour les besoins des enquêtes et des informations judiciaires lorsqu'il est difficile d'aboutir à des résultats intéressant les recherches en cours sans recourir à la surveillance électronique* » (article 4 c), permettant un champ d'application extrêmement large sans le limiter à des infractions graves. Ces mesures sont autorisées par l'autorité judiciaire mais la seule autre garantie entourant la perquisition et la saisie est l'impossibilité d'utiliser les données obtenues « *à des fins autres que les enquêtes et les informations judiciaires* » (article 9), ce qui permet malgré tout des utilisations assez larges. Enfin, les dispositions de droit pénal matériel ne prévoient pas toutes l'impératif

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	d'une commission intentionnelle et sans droit (exemple de l'infraction de pornographie enfantine).
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Article 12 - Obligations des fournisseurs d'accès à internet** Outre les obligations prévues par l'article 11 ci-dessus, les fournisseurs d'accès à internet sont tenus : a) d'intervenir, sans délai, pour retirer les contenus dont ils autorisent l'accès en cas d'infraction aux lois, les stocker ou les rendre inaccessibles dès qu'ils en ont pris connaissance directement ou indirectement ; b) de mettre en place des dispositifs techniques permettant de limiter l'accessibilité aux distributeurs contenant des informations contraires à l'ordre public ou aux bonnes mœurs et en informer les abonnés. **Code pénal, article 394 bis 8 (créé par la loi n° 16-02 du 19 juin 2016)** Sans préjudice des sanctions administratives prévues par la législation et la réglementation en vigueur, est puni d'un emprisonnement d'un an à trois (3) ans et d'une amende de 2.000.000 DA à 10.000.000 DA, ou de l'une de ces deux peines seulement, le fournisseur d'accès à internet au sens de l'article 2 de la loi n° 09-04 du 14 Chaâbane 1430 correspondant au 5 août 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication, qui malgré sa mise en demeure par l'organe national prévu par la loi suscitée ou l'intervention d'une décision de justice l'obligeant à le faire : a) n'intervient pas, sans délai, pour retirer, stocker ou rendre inaccessibles les données dont il autorise l'accès, lorsque leur contenu constitue une infraction à la législation pénale, b) ne met pas en place des dispositifs techniques permettant de retirer, stocker ou rendre inaccessibles les données contenant les infractions prévues au paragraphe a) du présent article ».
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,	**Loi n° 09- 04 du 5 août 2009** **CHAPITRE IV Obligations des fournisseurs de services** **Article 10 - Assistance aux autorités** Dans le cadre de l'application des dispositions de la présente loi, les fournisseurs de services sont tenus de [...] mettre à [la] [...] disposition [des autorités chargées des enquêtes judiciaires] les données qu'ils sont tenus de conserver en vertu de l'article 11 ci-dessous. Sous peine des sanctions prévues en matière de violation du secret de l'enquête

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	et de l'instruction, les fournisseurs de services sont tenus de garder la confidentialité des opérations qu'ils effectuent sur réquisition des enquêteurs et les informations qui s'y rapportent. **Article 11 - Conservation des données relatives au trafic** Selon la nature et les types de services, les fournisseurs de services s'engagent à conserver : a) les données permettant l'identification des utilisateurs du service ; b) les données relatives aux équipements terminaux des communications utilisées ; c) les caractéristiques techniques ainsi que la date, le temps et la durée de chaque communication ; d) les données relatives aux services complémentaires requis ou utilisés et leurs fournisseurs ; e) les données permettant d'identifier le ou les destinataires de la communication ainsi que les adresses des sites visités. Pour les activités de téléphonie, l'opérateur conserve les données citées au paragraphe (a) du présent article et celles permettant d'identifier et de localiser l'origine de la communication. La durée de conservation des données citées au présent article est fixée à une (1) année à compter du jour de l'enregistrement. Sans préjudice des sanctions administratives découlant du non-respect des obligations prévues par le présent article, la responsabilité pénale des personnes physiques et morales est engagée lorsque cela a eu pour conséquence d'entraver le bon déroulement des enquêtes judiciaires. La peine encourue par la personne physique est l'emprisonnement de six (6) mois à cinq (5) ans et l'amende de 50.000 DA à 500.000 DA. La personne morale encourt la peine d'amende suivant les modalités prévues par le code pénal. Les modalités d'application des alinéas 1, 2 et 3 du présent article sont, en tant que de besoin, précisées par voie réglementaire.
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	**Loi n° 09- 04 du 5 août 2009** **CHAPITRE IV Obligations des fournisseurs de services** **Article 10 - Assistance aux autorités** Dans le cadre de l'application des dispositions de la présente loi, les fournisseurs de services sont tenus de prêter leur assistance aux autorités chargées des enquêtes judiciaires pour la collecte ou l'enregistrement, en temps réel, des données relatives au contenu des communications et de mettre à leur

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	disposition les données qu'ils sont tenus de conserver en vertu de l'article 11 ci-dessous. Sous peine des sanctions prévues en matière de violation du secret de l'enquête et de l'instruction, les fournisseurs de services sont tenus de garder la confidentialité des opérations qu'ils effectuent sur réquisition des enquêteurs et les informations qui s'y rapportent.
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:	**Loi n° 09- 04 du 5 août 2009** **CHAPITRE III - Règles de procédure** **Article 5 - Perquisition des systèmes informatiques** Les autorités judiciaires compétentes ainsi que les officiers de police judiciaire, agissant dans le cadre du code de procédure pénale et dans les cas prévus par l'article 4 ci-dessus, peuvent, aux fins de perquisition, accéder, y compris à distance : a) à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ; b) à un système de stockage informatique. Lorsque, dans le cas prévu par le paragraphe (a) du présent article, l'autorité effectuant la perquisition a des raisons de croire que les données recherchées sont stockées dans un autre système informatique et que ces données sont accessibles à partir du système initial, elle peut étendre, rapidement, la perquisition au système en question ou à une partie de celui-ci après information préalable de l'autorité judiciaire compétente. S'il est préalablement avéré que les données recherchées, accessibles au moyen du premier système, sont stockées dans un autre système informatique situé en dehors du territoire national, leur obtention se fait avec le concours des autorités étrangères compétentes conformément aux accords internationaux

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	pertinents et suivant le principe de la réciprocité. Les autorités en charge de la perquisition sont habilitées à réquisitionner toute personne connaissant le fonctionnement du système informatique en question ou les mesures appliquées pour protéger les données informatiques qu'il contient, afin de les assister et leur fournir toutes les informations nécessaires à l'accomplissement de leur mission. **Article 6 - Saisie de données informatiques** Lorsque l'autorité effectuant la perquisition découvre, dans un système informatique, des données stockées qui sont utiles à la recherche des infractions ou leurs auteurs, et que la saisie de l'intégralité du système n'est pas nécessaire, les données en question de même que celles qui sont nécessaires à leur compréhension, sont copiées sur des supports de stockage informatique pouvant être saisis et placés sous scellés dans les conditions prévues par le code de procédure pénale. L'autorité effectuant la perquisition et la saisie doit, en tout état de cause, veiller à l'intégrité des données du système informatique en question. Toutefois, elle peut employer les moyens techniques requis pour mettre en forme ou reconstituer ces données en vue de les rendre exploitables pour les besoins de l'enquête, à la condition que cette reconstitution ou mise en forme des données n'en altère pas le contenu. **Article 7 - Saisie par l'interdiction d'accès aux données** Si, pour des raisons techniques, l'autorité effectuant la perquisition se trouve dans l'impossibilité de procéder à la saisie conformément à l'article 6 ci-dessus, elle doit utiliser les techniques adéquates pour empêcher l'accès aux données contenues dans le système informatique ou aux copies de ces données qui sont à la disposition des personnes autorisées à utiliser ce système. **Article 8 - Données saisies au contenu incriminé** L'autorité ayant procédé à la perquisition peut ordonner les mesures nécessaires pour rendre inaccessible les données dont le contenu constitue une infraction, notamment en désignant toute personne qualifiée pour employer les moyens techniques appropriés à cet effet. **Article 9 - Limites à l'utilisation des données collectées** Sous peine de sanctions édictées par la législation en vigueur, les données obtenues au moyen des opérations de surveillance prévues à la présente loi ne peuvent être utilisées à des fins autres que les enquêtes et les informations judiciaires.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Loi n° 09- 04 du 5 août 2009** **CHAPITRE IV Obligations des fournisseurs de services** **Article 10 - Assistance aux autorités** Dans le cadre de l'application des dispositions de la présente loi, les fournisseurs de services sont tenus de prêter leur assistance aux autorités chargées des enquêtes judiciaires pour la collecte ou l'enregistrement, en temps réel, des données relatives au contenu des communications et de mettre à leur disposition les données qu'ils sont tenus de conserver en vertu de l'article 11 ci-dessous. Sous peine des sanctions prévues en matière de violation du secret de l'enquête et de l'instruction, les fournisseurs de services sont tenus de garder la confidentialité des opérations qu'ils effectuent sur réquisition des enquêteurs et les informations qui s'y rapportent. **Article 11 - Conservation des données relatives au trafic** Selon la nature et les types de services, les fournisseurs de services s'engagent à conserver : a) les données permettant l'identification des utilisateurs du service ; b) les données relatives aux équipements terminaux des communications utilisées ; c) les caractéristiques techniques ainsi que la date, le temps et la durée de chaque communication ; d) les données relatives aux services complémentaires requis ou utilisés et leurs fournisseurs ; e) les données permettant d'identifier le ou les destinataires de la communication ainsi que les adresses des sites visités. Pour les activités de téléphonie, l'opérateur conserve les données citées au paragraphe (a) du présent article et celles permettant d'identifier et de localiser l'origine de la communication. La durée de conservation des données citées au présent article est fixée à une (1) année à compter du jour de l'enregistrement. Sans préjudice des sanctions administratives découlant du non-respect des obligations prévues par le présent article, la responsabilité pénale des personnes physiques et morales est engagée lorsque cela a eu pour conséquence d'entraver le bon déroulement des enquêtes judiciaires. La peine encourue par la personne physique est l'emprisonnement de six (6) mois à cinq (5) ans et l'amende de 50.000 DA à 500.000 DA.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	La personne morale encourt la peine d'amende suivant les modalités prévues par le code pénal. Les modalités d'application des alinéas 1, 2 et 3 du présent article sont, en tant que de besoin, précisées par voie réglementaire.
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, articles 65 bis 5 à 65 bis 10 insérés par la loi n° 06-22 du 20 décembre 2006.** **Article 65 bis 5** Si les nécessités de l'enquête de flagrance ou de l'enquête préliminaire relative aux infractions en matière de trafic de drogue, de crime transnational organisé, d'atteinte aux systèmes de traitements automatisés de données, de blanchiment d'argent, de terrorisme et d'infractions relatives à la législation des changes ainsi qu'aux infractions de corruption l'exigent, le procureur de la République compétent peut, autoriser : — l'interception de correspondances émises par la voie des télécommunications ; — 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 de paroles prononcées par une ou plusieurs personnes à titre privé ou confidentiel dans des lieux privés ou publics, ou de l'image d'une ou de plusieurs personnes se trouvant dans un lieu privé. L'autorisation permet, pour la mise en place du dispositif technique, l'introduction dans tout lieu d'habitation ou autre, y compris hors des heures prévues à l'article 47 de la présente loi, à l'insu ou sans le consentement des personnes titulaires d'un droit sur ces biens. Les opérations ainsi autorisées doivent s'effectuer sous le contrôle direct du procureur de la République compétent. Dans le cas où une information judiciaire est ouverte, cette autorisation est donnée par le juge d'instruction. Les opérations ainsi autorisées se déroulent sous son contrôle direct. **Article 65 bis 6** Les opérations visées à l'article 65 bis 5 ci-dessus s'effectuent sans porter préjudice au secret professionnel prévu à l'article 45 de la présente loi. La révélation des infractions autres que celles mentionnées dans l'autorisation du magistrat ne constitue pas une cause de nullité des procédures incidentes". **Article 65 bis 7** Les autorisations prévues à l'article 65 bis 5 ci-dessus doivent comporter tous les éléments permettant d'identifier les liaisons à intercepter, les lieux

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	d'habitation ou autres visés et l'infraction qui motive le recours à ces mesures ainsi que la durée de celles-ci. Ces autorisations sont données par écrit pour une durée maximale de quatre (4) mois, renouvelable selon les nécessités de l'enquête ou de l'information dans les mêmes conditions de forme et de durée. **Article 65 bis 8** Le procureur de la République ou l'officier de police judiciaire par lui autorisé, le juge d'instruction ou l'officier de police judiciaire par lui commis, peuvent requérir tout agent qualifié d'un service, d'une unité ou d'un organisme public ou privé chargé des télécommunications, en vue de la prise en charge des aspects techniques des opérations mentionnées à l'article 65 bis 5 ci-dessus. **Article 65 bis 9** L'officier de police judiciaire autorisé ou commis par le magistrat compétent dresse un procès-verbal de chacune des opérations d'interception et d'enregistrement des correspondances, ainsi que de celles concernant la mise en place du dispositif technique et des opérations de captation, de fixation et d'enregistrement sonore ou audio-visuel. Le procès-verbal mentionne la date et l'heure auxquelles ces opérations ont commencé et celles auxquelles elles ont pris fin. **Article 65 bis 10** L'officier de police judiciaire autorisé ou commis décrit ou transcrit dans un procès-verbal, qui est versé au dossier, les correspondances, les images ou les conversations enregistrées, qui sont utiles à la manifestation de la vérité. Les conversations en langue étrangère sont transcrites et traduites, le cas échéant, avec l'assistance d'un interprète requis à cette fin. **Loi n° 09- 04 du 5 août 2009** **Article 3 - Champ d'application** Conformément aux règles prévues par le code de procédure pénale et par la présente loi et sous réserve des dispositions légales garantissant le secret des correspondances et des communications, il peut être procédé, pour des impératifs de protection de l'ordre public ou pour les besoins des enquêtes ou des informations judiciaires en cours, à la mise en place de dispositifs techniques pour effectuer des opérations de surveillance des communications électroniques, de collecte et d'enregistrement en temps réel de leur contenu ainsi qu'à des perquisitions et des saisies dans un système informatique.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	CHAPITRE II Surveillance des communications électroniques **Article 4 - Cas autorisant le recours à la surveillance électronique** Les opérations de surveillance prévues par l'article 3 ci-dessus peuvent être effectuées dans les cas suivants : a) pour prévenir les infractions qualifiées d'actes terroristes ou subversifs et les infractions contre la sûreté de l'Etat. b) lorsqu' il existe des informations sur une atteinte probable à un système informatique représentant une menace pour l'ordre public, la défense nationale, les institutions de l'Etat ou l'économie nationale ; c) pour les besoins des enquêtes et des informations judiciaires lorsqu'il est difficile d'aboutir à des résultats intéressant les recherches en cours sans recourir à la surveillance électronique ; d) dans le cadre de l'exécution des demandes d'entraide judiciaire internationale. Les opérations de surveillance ci-dessus mentionnées ne peuvent être effectuées que sur autorisation écrite de l'autorité judiciaire compétente. Lorsqu'il s'agit du cas prévu au paragraphe (a) du présent article, l'autorisation est délivrée aux officiers de police judiciaire relevant de l'organe visé à l'article 13 ci-après, par le procureur général près la Cour d'Alger, pour une durée de six (6) mois renouvelable, sur la base d'un rapport indiquant la nature du procédé technique utilisé et les objectifs qu'il vise. Sous peine des sanctions prévues par le code pénal en matière d'atteinte à la vie privée d'autrui, les dispositifs techniques mis en place aux fins désignées au paragraphe du présent article doivent être orientés, exclusivement, vers la collecte et l'enregistrement de données en rapport avec la prévention et la lutte contre les actes terroristes et les atteintes à la sûreté de l'Etat. **CHAPITRE IV Obligations des fournisseurs de services** **Article 10 - Assistance aux autorités** Dans le cadre de l'application des dispositions de la présente loi, les fournisseurs de services sont tenus de prêter leur assistance aux autorités chargées des enquêtes judiciaires pour la collecte ou l'enregistrement, en temps réel, des données relatives au contenu des communications et de mettre à leur disposition les données qu'ils sont tenus de conserver en vertu de l'article 11 ci-dessous. Sous peine des sanctions prévues en matière de violation du secret de l'enquête et de l'instruction, les fournisseurs de services sont tenus de garder la confidentialité des opérations qu'ils effectuent sur réquisition des enquêteurs et les informations qui s'y rapportent.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	**Code pénal, Article 3** La loi pénale s'applique à toutes les infractions commises sur le territoire de la République. Elle s'applique également aux infractions commises à l'étranger lorsqu'elles relèvent de la compétence des juridictions répressives algériennes en vertu des dispositions du code de procédure pénale. **Loi n° 09- 04 du 5 août 2009** **CHAPITRE VI La coopération et l'entraide judiciaire internationales** **Article 15 - Compétence judiciaire** Outre les règles de compétence prévues par le code de procédure pénale, les juridictions algériennes sont compétentes pour connaître des infractions liées aux technologies de l'information et de la communication commises en dehors du territoire national, lorsque leur auteur est un étranger et qu'elles ont pour cible les institutions de l'Etat algérien, la défense nationale ou les intérêts stratégiques de l'économie nationale.
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	**Articles 614 à 713 du Code de procédure pénale.** (s'appliquant sauf dispositions contraires résultat de traités ou de Conventions diplomatiques).

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 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	**Loi n° 09- 04 du 5 août 2009** **Article 15** Dans le cadre des investigations ou des informations judiciaires menées pour la constatation des infractions comprises dans le champ d'application de la présente loi et la recherche de leurs auteurs, les autorités compétentes peuvent recourir à l'entraide judiciaire internationale pour recueillir des preuves sous forme électronique. En cas d'urgence, et sous réserve des conventions internationales et du principe de réciprocité, les demandes d'entraide judiciaire visées à l'alinéa précédent sont recevables si elles sont formulées par des moyens rapides de communication, tels que la télécopie ou le courrier électronique pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification. **Article 17 - Echange d'informations et les mesures conservatoires** Les demandes d'entraide tendant à l'échange d'informations ou à prendre toute mesure conservatoire sont satisfaites conformément aux conventions internationales pertinentes, aux accords bilatéraux et en application du principe de réciprocité. **Article 18 - Restrictions aux demandes d'entraide internationale** L'exécution de la demande d'entraide est refusée si elle est de nature à porter atteinte à la souveraineté nationale ou à l'ordre public. La satisfaction des demandes d'entraide peut être subordonnée à la condition de conserver la confidentialité des informations communiquées ou à la condition de ne pas les utiliser à des fins autres que celles indiquées dans la demande.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	**Loi n° 09- 04 du 5 août 2009** **Article 15** [...] En cas d'urgence, et sous réserve des conventions internationales et du principe de réciprocité, les demandes d'entraide judiciaire visées à l'alinéa précédent sont recevables si elles sont formulées par des moyens rapides de communication, tels que la télécopie ou le courrier électronique pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification. **Article 17 - Echange d'informations et les mesures conservatoires** Les demandes d'entraide tendant à l'échange d'informations ou à prendre toute mesure conservatoire sont satisfaites conformément aux conventions internationales pertinentes, aux accords bilatéraux et en application du principe de réciprocité.
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	**Loi n° 09- 04 du 5 août 2009** **Article 15** Dans le cadre des investigations ou des informations judiciaires menées pour la constatation des infractions comprises dans le champ d'application de la présente loi et la recherche de leurs auteurs, les autorités compétentes peuvent recourir à l'entraide judiciaire internationale pour recueillir des preuves sous forme électronique. En cas d'urgence, et sous réserve des conventions internationales et du principe de réciprocité, les demandes d'entraide judiciaire visées à l'alinéa précédent sont recevables si elles sont formulées par des moyens rapides de communication, tels que la télécopie ou le courrier électronique pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification. **Article 18 - Restrictions aux demandes d'entraide internationale** L'exécution de la demande d'entraide est refusée si elle est de nature à porter atteinte à la souveraineté nationale ou à l'ordre public. La satisfaction des demandes d'entraide peut être subordonnée à la condition de conserver la confidentialité des informations communiquées ou à la condition de ne pas les utiliser à des fins autres que celles indiquées dans la demande.

Back to the Table of Contents

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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 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.	**Loi n° 09- 04 du 5 août 2009** **Article 18 - Restrictions aux demandes d'entraide internationale** L'exécution de la demande d'entraide est refusée si elle est de nature à porter atteinte à la souveraineté nationale ou à l'ordre public. La satisfaction des demandes d'entraide peut être subordonnée à la condition de conserver la confidentialité des informations communiquées ou à la condition de ne pas les utiliser à des fins autres que celles indiquées dans la demande.
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	**Loi n° 09- 04 du 5 août 2009** **CHAPITRE II Surveillance des communications électroniques** **Article 4 - Cas autorisant le recours à la surveillance électronique** Les opérations de surveillance prévues par l'article 3 ci-dessus peuvent être effectuées dans les cas suivants : [...] d) dans le cadre de l'exécution des demandes d'entraide judiciaire internationale. [...]
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	**Loi n° 09- 04 du 5 août 2009** **CHAPITRE V Organe national de prévention et de lutte contre les infractions liées aux technologies de l'information et de la**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**communication** **Article 13 - Création de l'organe** Il est créé un organe national de prévention et de lutte contre la criminalité liée aux technologies de l'information et de la communication. La composition, l'organisation et les modalités de fonctionnement de l'organe sont fixées par voie réglementaire. **Article 14 - Missions de l'organe** L'organe visé à l'article 13 ci-dessus est chargé notamment de : a) la dynamisation et la coordination des opérations de prévention et de lutte contre la criminalité liée aux technologies de l'information et de la communication ; b) l'assistance des autorités judiciaires et des services de police judiciaire en matière de lutte contre la criminalité liée aux technologies de l'information et de la communication, y compris à travers la collecte de l'information et les expertises judiciaires ; c) l'échange d'informations avec ses interfaces à l'étranger aux fins de réunir toutes données utiles à la localisation et à l'identification des auteurs des infractions liées aux technologies de l'information et de la communication.
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