Niger

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Version March 2020

Table of contents

[reference to the provisions of the Budapest Convention]

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

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

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	**Article 1 : Définitions** **« Cybercriminalité » :** l'ensemble des infractions pénales qui se commettent au moyen ou sur réseau de télécommunications ou un système d'information ; « **Preuve électronique** » : Tout écrit sous forme électronique, admis en preuve au même titre que l'écrit sur support papier et possédant la même force probante que celui-ci, sous réserve que puisse être dûment identifiée la personne de laquelle il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité et la pérennité ; **« Système informatique » :** tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs élément (s) assure (nt) en exécution d'un programme, un traitement automatisé de données. **« Communication électronique »** : toute transmission, toute émission ou toute réception de signes, de signaux, d'écrits, d'images, de sons, de données ou de renseignements de toute nature par câble en cuivre, fibres optiques, radioélectricité ou autres systèmes électromagnétiques. **« Données informatiques » :** toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction. **« Données relatives aux abonnés » :** toute information, contenue sous

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de service et qui se rapporte aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir : - le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ; - l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné ; - et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de service ; - toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de service. **« Données relatives au trafic »**: toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type du service sous-jacent. **« Fournisseur de service »**: toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs. **« Technologies de l'information et de la communication (TIC)»**: les technologies employées pour recueillir, stocker, utiliser et transmettre des informations ainsi que celles qui impliquent l'utilisation des ordinateurs ou de tout système de communication y compris de télécommunication. **« Pornographie enfantine »** : toute matière pornographique, quel que soit le support, notamment visuel ou sonore, représentant :

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	- un mineur se livrant à un comportement sexuellement explicite ; - une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite ; - des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite. **« Mineur »**: toute personne âgée de moins de 18 ans. Toutefois, les définitions des instruments juridiques nationaux, de la CEDEAO, de l'Union Africaine ou de l'Union Internationale des Télécommunications prévalent pour les termes non définis par la présente loi.
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.	**Article 3 : Accès illégal** Est puni d'une peine d'emprisonnement de un (1) à trois (3) ans et d'une amende de cinq cent mille (500 000) à un million (1 000 000) de francs CFA, quiconque accède, intentionnellement et sans droit, à tout ou partie d'un système informatique. Lorsqu'il en résulte soit la suppression, la modification ou l'altération des données informatiques contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement est de trois (3) à cinq (5) ans et l'amende de deux millions (2 000 000) à cinq millions (5 000 000) de francs CFA.
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	**Article 7 : Interception Illégale** Est puni d'une peine d'emprisonnement de deux (2) à cinq (5) ans et d'une amende d'un million (1 000 000) à cinq millions (5 000 000) de francs CFA,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	quiconque intercepte, intentionnellement et sans droit, par des moyens techniques, des données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques.
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.	**Article 8 : Atteinte à l'intégrité des données** Est puni d'une peine d'emprisonnement de deux (2) à cinq (5) ans et d'une amende de cinq millions (5 000 000) à vingt millions (20 000 000) de francs CFA, quiconque endommage, efface, détériore, altère, modifie ou supprime, intentionnellement et sans droit, des données informatiques.
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	
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	**Article 12 : Abus de dispositifs** Les peines applicables aux infractions prévues aux articles 3 à 8 de la présente loi sont encourues par, quiconque produit, vend, obtient pour utilisation, importe, diffuse ou met à disposition, intentionnellement et sans droit, sous quelque forme que ce soit : - un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une de ces infractions ; - un mot de passe, un code d'accès ou des données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, dans l'intention qu'ils soient utilisés afin de commettre l'une de ces infractions. Les mêmes peines s'appliquent à quiconque possède, intentionnellement et sans droit, un dispositif, un mot de passe, un code d'accès ou des données

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	informatiques similaires permettant d'accéder à tout ou partie d'un système informatique en vue de commettre l'une des infractions visées par les articles 3 à 8 de la présente loi. Les infractions prévues par le présent article ne sont pas établies lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition n'ont pas pour but de commettre une infraction prévue par les articles 3 à 8 de la présente loi, comme en cas d'essais autorisés ou de protection d'un système informatique.
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.	**Article 9 : Falsification informatique** Est puni d'une peine d'emprisonnement de cinq (5) à moins de dix (10) ans et d'une amende de cinq millions (5 000 000) à vingt millions (20 000 000) de francs CFA, quiconque introduit, altère, modifie, efface ou supprime, intentionnellement et sans droit, des données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**Article 11 : Fraude informatique** Est puni d'une peine d'emprisonnement de cinq (5) à moins de dix (10) ans et d'une amende de cinq millions (5 000 000) à vingt millions (20 000 000) de francs CFA, quiconque cause, intentionnellement et sans droit, un préjudice patrimonial à autrui par l'introduction, l'altération, la modification, l'effacement ou la suppression de données informatiques ou par toute forme d'atteinte au fonctionnement d'un système informatique, dans l'intention frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct	**Article 15 : Production, offre, diffusion de pornographie enfantine** Est puni d'une peine d'emprisonnement de cinq (5) à moins de dix (10) ans et d'une amende de cinq millions (5 000 000) à dix millions (10 000 000) de francs CFA, quiconque produit, offre ou diffuse, intentionnellement et sans droit, de la pornographie enfantine en vue de sa diffusion, offre ou met à disposition, diffuse ou transmet de la pornographie enfantine par le biais d'un système informatique. **Article 16 : Importation, exportation de la pornographie enfantine** Est puni d'une peine d'emprisonnement de cinq (5) à moins de dix (10) ans et d'une amende de cinq millions (5 000 000) à dix millions (10 000 000) de francs CFA, quiconque se fait procurer ou procure à autrui, importe, se fait importer ou exporte ou se fait exporter de la pornographie enfantine, intentionnellement et sans droit, par le biais d'un système informatique. **Article 17 : Détention ou possession de la pornographie enfantine** Est puni d'une peine d'emprisonnement de cinq (5) à moins de dix (10) ans et d'une amende de cinq millions (5 000 000) à dix millions (10 000 000) de francs CFA, quiconque, intentionnellement et sans droit, possède ou détient de la pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques. **Article 18 : Facilitation de l'accès des mineurs à des contenus**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	**pornographiques** Est puni d'une peine d'emprisonnement de cinq (5) à moins de dix (10) ans et d'une amende de cinq millions (5 000 000) à dix millions (10 000 000) de francs CFA, quiconque facilite, intentionnellement et sans droit, l'accès à des images, à des documents, au son ou à une représentation présentant un caractère de pédopornographie. **Article 19 : Consultation habituelle de sites de pornographie enfantine** Est puni d'une peine d'emprisonnement de cinq (5) à moins de dix (10) ans et d'une amende de cinq millions (5 000 000) à dix millions (10 000 000) de francs CFA, quiconque, intentionnellement et sans droit, consulte habituellement ou en contrepartie d'un paiement, un service de communication au public en ligne mettant à disposition des images ou vidéos pédopornographiques. **Article 20 : Sollicitations sexuelles d'un mineur de moins de quinze ans.** Est puni d'une peine d'emprisonnement d'un (1) à trois (3) ans et d'une amende de cinq cent mille (500 000) à un million (1 000 000) de francs CFA, toute personne majeure faisant des propositions sexuelles à un mineur de moins de quinze ans ou à une personne se présentant comme telle en utilisant un moyen de communication électronique. Lorsque les propositions ont été suivies d'une rencontre, les peines prévues à l'alinéa premier du présent article sont portées au double.
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.	**Article 21 : Reproduction, extraction, copiage de données informatiques** Est puni d'une peine d'emprisonnement de un (1) à cinq (5) ans et d'une amende de trois millions (3 000 000) à dix millions (10 000 000) de francs CFA, quiconque reproduit, extrait ou copie intentionnellement et sans droit des données informatiques appartenant à autrui.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	**Article 36 : Complicité** La complicité des infractions prévues par la présente loi est punissable dans les conditions prévues par le code pénal. **Article 37 : Tentative** La tentative de commettre l'une des infractions prévues par la présente loi est punissable comme le délit consommé.
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an	**Article 34 : Conditions de la responsabilité pénale des personnes morales** Toute personne morale, à l'exception de l'Etat, des collectivités locales et des établissements publics, est responsable des infractions prévues par la présente loi, lorsqu'elles sont commises pour son compte par toute personne physique qui, agissant soit individuellement, soit en tant que membre d'un organe de

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	ladite personne morale, exerce un pouvoir de direction en son sein. Le pouvoir de direction visé à l'alinéa premier du présent article est exercé sur les bases suivantes : • un pouvoir de représentation de la personne morale ; • une autorité pour prendre des décisions au nom de la personne morale ; • une autorité pour exercer un contrôle au sein de la personne morale. La responsabilité des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits. Toute personne morale est également tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, a rendu possible la commission des infractions visées par la présente loi pour le compte de ladite personne morale par une personne physique agissant sous son autorité.
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 35 : Sanctions contre les personnes morales** Les peines encourues par les personnes morales sont : 1) l'amende dont le taux maximum est égal au quintuple de celui prévu pour les personnes physiques par la loi qui réprime l'infraction ; 2) la dissolution, lorsque la personne morale a été créée pour commettre les faits incriminés ; 3) la dissolution, lorsque la personne morale a été détournée de son objet pour commettre les faits incriminés et si l'infraction retenue expose son auteur, personne physique, à une peine d'emprisonnement supérieure à cinq (5) ans ; 4) l'interdiction à titre définitif ou pour une durée de cinq (5) ans au plus, d'exercer directement ou indirectement une ou plusieurs activité (s) professionnelle (s) ou sociale (s) ; 5) la fermeture définitive ou pour une durée de cinq (5) ans au plus d'un ou de plusieurs établissement (s) de l'entreprise ayant servi à commettre les faits incriminés ; 6) l'exclusion des marchés publics à titre définitif ou pour une durée n'excédant pas cinq (5) ans ; 7) l'interdiction à titre définitif ou pour une durée de cinq (5) ans au plus de faire appel public à l'épargne ; 8) l'interdiction pour une durée de cinq (5) ans au plus d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	du tiré ou ceux qui sont certifiés ou d'utiliser des cartes de paiement ; 9) la confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit ; 10) l'affichage de la décision prononcée et la diffusion de celle-ci soit par la presse écrite, soit par tout moyen de communication au public par voie électronique. **Article 22 : Escroquerie portant sur des données informatiques** **Article 23 : Abus de confiance portant sur les données informatiques** **Article 24 : Recel portant sur des données informatiques** **Article 25 : Extorsion portant sur des données informatiques** **Article 26 : Chantage portant sur des données informatiques** **Article 27 : Escroquerie par un moyen de communication électronique** **Article 28 : Chantage par un moyen de communication électronique** **Article 29 : Diffamation par un moyen de communication électronique** **Article 30 : Injure par un moyen de communication électronique** **Article 31 : Diffusion de données de nature à troubler l'ordre public ou à porter atteinte à la dignité humaine** **Article 32 : Propos à caractère raciste, régionaliste, ethnique, religieux ou xénophobe** **Article 33 : Peines complémentaires**
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 38 : Champ d'application** Les procédures prévues dans le présent titre s'appliquent **:** - aux infractions pénales prévues par la présente loi ; - à toutes autres infractions pénales commises au moyen d'un système informatique ; - à la collecte des preuves électroniques de toute infraction pénale

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Article 39 : Conservation rapide de données informatiques stockées** Si les nécessités de l'enquête ou de l'information l'exigent, l'officier de police judiciaire ou le juge d'instruction peut ordonner à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification. La personne visée à l'alinéa premier du présent article est tenue de conserver et de protéger l'intégrité des données pendant une durée maximale de 90 jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Le gardien des données ou une autre personne chargée de conserver celles-ci est tenu de garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue. Toute violation du secret est punie des peines applicables au délit de violation du secret professionnel prévu par le code pénal.
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	**Article 40 : Conservation et divulgation rapides de données relatives au trafic** Si les nécessités de l'enquête ou de l'information l'exigent, l'officier de police judiciaire ou le juge d'instruction peut ordonner à une personne de conserver des données relatives au trafic se trouvant en sa possession ou sous son contrôle, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	La mesure prévue par l'alinéa premier du présent article peut être ordonnée lorsqu'un seul ou plusieurs fournisseur (s) de service a, (ont), participé à la transmission de cette communication. La personne assurant le contrôle des données doit assurer la divulgation rapide à l'autorité compétente ou à une personne désignée par cette autorité d'une quantité de données relatives au trafic suffisante pour permettre l'identification des fournisseurs de service et de la voie par laquelle la communication a été transmise.
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	**Article 41 : Injonction de produire** Si les nécessités de l'enquête ou de l'information l'exigent, l'officier de police judiciaire ou le juge d'instruction peut ordonner à : - une personne présente sur son ressort de communiquer les données informatiques spécifiées, en la possession ou sous le contrôle de cette personne, et stockées dans un système informatique ou un support de stockage informatique ; - un fournisseur de services offrant des prestations sur le territoire national, de communiquer les données en sa possession ou sous son contrôle relatif aux abonnés et concernant de tels services
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	**Article 42 : Perquisition de données informatiques stockées** Lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données informatisées sur le territoire

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	national sont utiles à la manifestation de la vérité, le juge d'instruction ou l'officier de police judiciaire peut perquisitionner ou accéder d'une façon similaire à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées et à un support du stockage informatique permettant de stocker des données informatiques sur son ressort. Lorsqu'au cours des opérations de perquisition, les autorités visées à l'alinéa premier du présent article ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur le territoire national, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, elles peuvent étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système. S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par le juge d'instruction ou par l'officier de police judicaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur. **Article 43 : Saisie de données informatiques stockées** Lorsque le juge d'instruction découvre dans un système informatique des données stockées qui sont utiles pour la manifestation de la vérité, mais que la saisie du support ne paraît pas souhaitable, ces données, de même que celles qui sont nécessaires pour les comprendre, sont copiées sur des supports de stockage informatique pouvant être saisis et placés sous scellés. Le juge d'instruction ou l'officier de police judiciaire peut ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures prévues à l'alinéa premier du présent article. Si les données qui sont liées à l'infraction, soit qu'elles en constituent l'objet, soit qu'elles en sont le produit, sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, le juge d'instruction ou l'officier de police judiciaire ordonne les mesures conservatoires nécessaires, notamment en désignant toute personne qualifiée avec pour mission d'utiliser tous les moyens techniques appropriés pour rendre

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	ces données inaccessibles. Lorsque la mesure prévue à l'alinéa premier du présent article n'est pas possible, pour des raisons techniques ou en raison du volume des données, le juge d'instruction utilise les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité. Le juge d'instruction ou l'officier de police judiciaire informe le responsable du système informatique de la recherche effectuée dans le système informatique et lui communique une copie des données qui ont été copiées, rendues inaccessibles ou retirées.
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	**Article 44 : Collecte en temps réel des données relatives au trafic** Lorsque les nécessités de l'enquête ou de l'information l'exigent, l'officier de police judiciaire ou le juge d'instruction peut collecter ou enregistrer par l'utilisation de moyens techniques existants ou obliger un fournisseur de services, dans la limite des capacités techniques existantes à : - collecter ou enregistrer par l'utilisation de moyens techniques existants sur le territoire national ; - prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur le territoire national au moyen d'un système informatique. Le fournisseur de services visé à l'alinéa premier du présent article est tenu de garder secret le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Article 45 : Interception de données relatives au contenu** En matière criminelle ou lorsque la peine encourue est égale ou supérieure à deux (2) ans d'emprisonnement en matière correctionnelle, le juge d'instruction peut, si les nécessités de l'information l'exigent, notamment à la demande d'un officier de police judiciaire, prescrire la collecte, l'interception, l'enregistrement et la transcription de données relatives au contenu de communications spécifiques relevant de son ressort, transmises au moyen d'un système informatique. Ces opérations sont effectuées sous son autorité et son contrôle. La décision d'interception est écrite. Elle n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours. La décision d'interception prise en application de l'alinéa premier du présent article comporte tous les éléments d'identification de la liaison à intercepter, l'infraction qui motive le recours à l'interception ainsi que la durée de celle-ci. Cette décision d'interception est prise pour une durée maximale de trois (3) mois. Elle ne peut être renouvelée qu'une fois dans les mêmes conditions de forme et de durée à condition que la demande de renouvellement soit transmise au plus tard quarante-huit (48) heures avant l'échéance de la première décision d'interception. Le juge d'instruction ou l'officier de police judiciaire par lui commis peut requérir tout agent qualifié d'un service ou organisme public en charge des communications électroniques ou tout agent qualifié d'un exploitant de réseau ou fournisseur de services, dans le cadre de ses capacités techniques existantes, en vue de procéder à l'installation d'un dispositif d'interception. Le juge d'instruction ou l'officier de police judiciaire commis par lui dresse procès-verbal de chacune des opérations d'interception et d'enregistrement. Ce procès-verbal mentionne la date et l'heure auxquelles l'opération a commencé et celles auxquelles elle s'est terminée.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Les enregistrements sont placés sous scellés fermés et accessibles par le juge d'instruction, l'officier de police judiciaire ou toute personne habilitée par le juge d'instruction. Le juge d'instruction ou l'officier de police judiciaire commis par lui transcrit la correspondance utile à la manifestation de la vérité. Il en est dressé procès-verbal. Cette transcription est versée au dossier. Les correspondances dans une langue autre que la langue officielle sont transcrites en français avec l'assistance d'un interprète requis à cette fin. A peine de nullité, ne peuvent être transcrites les correspondances entre l'inculpé et son conseil lorsqu'elles relèvent de l'exercice des droits de la défense. Les enregistrements sont détruits, à la diligence du procureur de la République ou du procureur général, à l'expiration du délai de prescription de l'action publique. Il est dressé procès-verbal de l'opération de destruction. Le fournisseur de services visé au cinquième alinéa du présent article est tenu de garder secret le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet. **Article 46 :** Les correspondances dépendant du bureau ou du domicile d'un parlementaire ne peuvent être interceptées sans que le Bureau de l'Assemblée nationale en soit informé par le juge d'instruction. **Article 47 ;** Les correspondances dépendant du cabinet d'un avocat ou de son domicile ne peuvent être interceptées sans que le bâtonnier de l'ordre des avocats en soit informé par le juge d'instruction. **Article 48 :** Les correspondances dépendant du cabinet d'un magistrat ou d'un juge ou de leurs domiciles ne peuvent être interceptées sans que le président de la cour d'appel ou le procureur général près la cour dont relève la juridiction à laquelle il appartient en soit informé par le juge d'instruction. **Article 49 :** Les correspondances dépendant du cabinet du président d'une

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	cour d'appel, ou du procureur général près une cour d'appel, ou celle d'un magistrat ou d'un juge d'une haute juridiction ou d'un magistrat exerçant dans l'administration, ne peuvent être interceptées sans que le Ministre chargé de la Justice en soit informé par le juge d'instruction. **Article 50 :** Les correspondances dépendant du cabinet d'un membre du gouvernement ou de son domicile ne peuvent être interceptées sans que le Premier Ministre en soit informé par le juge d'instruction. **Article 51 :** Les correspondances dépendant du Cabinet du Premier Ministre ou de son domicile ne peuvent être interceptées sans que le Président de la République en soit informé par le juge d'instruction. **Article 52 :** Les formalités prévues par les articles 45 à 51 ci-dessus sont prescrites à peine de nullité. Les personnalités avisées sont liées par le secret de l'instruction. **Article 53 :** Si les nécessités de l'enquête de flagrance ou de l'enquête préliminaire relative à l'une des infractions prévues par la présente loi l'exigent, le président du tribunal de grande instance ou le juge par lui délégué peut, à la requête du procureur de la République, autoriser l'interception, l'enregistrement et la transcription de correspondances émises par la voie des communications électroniques selon les modalités prévues par le présent article, pour une durée maximale de trois mois, renouvelable une fois dans les mêmes conditions de forme et de durée à condition que la demande de renouvellement soit transmise au plus tard quarante-huit heures (48) avant l'échéance de la première décision d'interception. La requête du procureur et l'ordonnance du président sont frappées du sceau de la confidentialité.

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.	**Article 68 : Autorité compétente** L'autorité compétente désignée aux fins de l'application de la présente loi est le Ministre chargé de la Justice. A ce titre, il a l'obligation de faire en sorte que le point de contact dispose d'un personnel suffisamment formé et équipé en vue de faciliter le fonctionnement du point de contact 24/7 établi par la Convention du Conseil de l'Europe sur la cybercriminalité et les autres conventions pertinentes.
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.	**Article 57 : Principes généraux relatifs à la coopération internationale** L'autorité compétente coopère avec les autres Etats, conformément aux dispositions du présent titre, en application des instruments internationaux en vigueur sur la coopération internationale en matière pénale auxquels le Niger est partie, dans la mesure la plus large possible, aux fins

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep	d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et données informatiques ou pour recueillir les preuves, sous forme électronique, d'une infraction pénale. **Article 58 : Extradition** Le présent article s'applique à l'extradition pour les infractions pénales définies aux articles de la présente loi, à condition qu'elles soient punissables dans la législation interne et dans la législation de l'Etat requérant d'une peine privative de liberté pour une période maximale d'au moins un (1) an, ou par une peine plus sévère. Lorsqu'il est exigé une peine minimale différente, sur la base d'un instrument international applicable entre le Niger et l'Etat requérant, la peine minimale prévue par cet instrument s'applique. L'extradition est soumise aux conditions prévues par le droit interne ou par les traités d'extradition en vigueur, y compris les motifs pour lesquels l'autorité compétente peut refuser l'extradition. Si l'extradition pour une infraction pénale mentionnée au premier paragraphe du présent article est refusée uniquement sur la base de la nationalité de la personne recherchée ou parce que l'autorité habilitée s'estime compétente pour cette infraction, elle soumet l'affaire à la demande de l'Etat requérant, à ses autorités compétentes aux fins de poursuite, et rend compte, en temps utile, de l'issue de l'affaire à l'Etat requérant. Les autorités en question prennent leur décision et mènent l'enquête et la procédure de la même manière que pour toute autre infraction de nature comparable, conformément à la législation du Niger.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	**Article 59 : Principes généraux relatifs á l'entraide** L'autorité compétente accorde l'entraide la plus large possible aux autres Etats aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale. L'autorité compétente peut, en cas d'urgence, formuler une demande d'entraide ou des communications s'y rapportant 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, y compris, si nécessaire, le cryptage, avec confirmation officielle ultérieure si l'Etat requis l'exige. Si le Niger fait l'objet d'une telle demande, l'autorité compétente accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication. Lorsque le Niger reçoit une demande d'entraide, celle-ci est soumise, sauf disposition contraire expressément prévue dans les articles du présent chapitre, aux conditions fixées par le droit national ou par les traités d'entraide applicables, y compris les motifs sur la base desquels l'Etat requis peut refuser la coopération. L'Etat requis ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 3 à 31 au seul motif que la demande porte sur une infraction qu'il considère comme de nature fiscale. La condition de double incrimination, à laquelle est subordonnée toute demande d'entraide, est considérée comme satisfaite dès lors que le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale dans le droit nigérien, que ce dernier classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de l'Etat requérant.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	**Article 60 : Information spontanée** L'autorité compétente peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à un autre Etat des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider l'Etat destinataire à engager ou mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente loi, ou lorsque ces informations pourraient aboutir à une demande de coopération. Avant de communiquer de telles informations, le Niger peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions.
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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). 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the	**Article 61 : Conservation rapide de données informatiques stockées** L'autorité compétente peut se voir ordonner ou imposer d'une autre façon par un autre Etat partie la conservation rapide de données stockées au moyen d'un système informatique se trouvant sur le territoire du Niger, et au sujet desquelles l'Etat requérant a l'intention de soumettre une demande d'entraide

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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	en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation desdites données. Une demande de conservation faite en application du paragraphe précédent doit préciser : - l'autorité qui demande la conservation ; - l'infraction faisant l'objet de l'enquête ou de procédures pénales et un bref exposé des faits qui s'y rattachent ; - les données informatiques stockées à conserver et la nature de leur lien avec l'infraction ; - toutes les informations disponibles permettant d'identifier le gardien des données informatiques stockées ou l'emplacement du système informatique ; - la nécessité de la mesure de conservation ; - le fait que l'Etat requérant entend soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données informatiques stockées. Après avoir reçu la demande d'un autre Etat, l'autorité compétente doit prendre toutes les mesures appropriées afin de procéder sans délai à la conservation des données spécifiées, conformément au droit interne. Pour pouvoir répondre à une telle demande, la double incrimination n'est pas requise comme condition préalable à la conservation. Une demande de conservation peut être refusée uniquement : - si l'autorité compétente a des raisons de penser que, au moment de la divulgation, la condition de double incrimination ne pourra pas être remplie ; - si la demande porte sur une infraction que l'Etat requis considère comme étant de nature politique ou liée à une infraction de nature politique ; - si l'Etat requis estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à d'autres intérêts essentiels.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	Lorsque l'autorité compétente estime que la conservation simple ne suffira pas à garantir la disponibilité future des données, ou compromettra la confidentialité de l'enquête de l'Etat requérant, ou nuira d'une autre façon à celle-ci, elle en informe rapidement cet Etat. Toute conservation effectuée en réponse à une demande visée au présent article est valable pour une durée de soixante (60) jours afin de permettre à l'Etat requérant de soumettre une demande en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données. Après la réception d'une telle demande, les données doivent continuer à être conservées en attendant l'adoption d'une décision concernant la demande.
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 62 : Divulgation rapide de données conservées** Lorsque, en exécutant une demande de conservation de données relatives au trafic concernant une communication spécifique formulée en application de l'article précédent, l'autorité compétente découvre qu'un fournisseur de services dans un autre Etat a participé à la transmission de cette communication, l'autorité compétente divulgue rapidement à cet Etat une quantité suffisante de données concernant le trafic, aux fins d'identifier ce fournisseur de services et la voie par laquelle la communication a été transmise. La divulgation de données relatives au trafic en application du paragraphe précédent peut être refusée seulement : - si la demande porte sur une infraction que l'autorité compétente considère comme étant de nature politique ou liée à une infraction de nature politique ; - si elle considère que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.
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	**Article 63 : Entraide concernant l'accès aux données stockées** L'autorité compétente peut se voir requise par un autre Etat de perquisitionner ou d'accéder de façon similaire, de divulguer des données stockées au moyen d'un système informatique se trouvant sur son territoire, y compris les données conservées conformément aux articles 39 et 40 de la présente loi. L'autorité compétente satisfait à la demande en appliquant les instruments

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	internationaux en vigueur et en se conformant aux dispositions pertinentes du présent titre. La demande doit être satisfaite aussi rapidement que possible dans les cas où : - il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification ; - les instruments internationaux en vigueur prévoient une coopération rapide.
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 64 : Accès transfrontalier à des données stockées** L'autorité compétente peut accéder à des données informatiques stockées accessibles au public, quelle que soit la localisation géographique de ces données et sans l'autorisation de l'Etat sur le territoire duquel se trouvent ces données. L'autorité compétente peut recevoir ou accéder, au moyen d'un système informatique situé sur son territoire, à des données informatiques situées sur le territoire d'un autre Etat dès lors qu'elle obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.
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 65 : Entraide dans la collecte en temps réel de données relatives au trafic** L'autorité compétente accorde aux autres Etats l'entraide dans la collecte en temps réel de données relatives au trafic, associées à des communications spécifiées sur son territoire, transmises au moyen d'un système informatique. Sous réserve des dispositions du paragraphe suivant, cette entraide est régie par les conditions et les procédures prévues en droit interne. L'autorité compétente accorde cette entraide au moins à l'égard des infractions pénales pour lesquelles la collecte en temps réel de données concernant le trafic serait disponible dans une affaire analogue au niveau interne.
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	**Article 66 : Entraide en matière d'interception de données relatives au contenu** Dans la mesure permise par les traités et son droit interne applicables, l'autorité compétente accorde aux autres Etats l'entraide pour la collecte ou l'enregistrement en temps réel de données relatives au contenu de communications spécifiques transmises au moyen d'un système informatique.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	**Article 67 : Point de contact 24/7** Pour les infractions relevant de la présente loi, la Direction de la police judiciaire constitue, en attendant la mise en place d'une structure spécialement dédiée, le point de contact central joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Cette assistance doit englober la facilitation, si le droit le permet, et l'application directe des mesures suivantes : - apport de conseils techniques; - conservation des données, conformément aux articles 61 et 62 ci-dessus; - recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects. Le point de contact, dit 24/7, doit être doté des moyens de correspondre avec le point de contact d'un autre Etat selon une procédure accélérée.
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