Cameroun

Législation sur la cybercriminalité

Équivalent national des dispositions de la Convention de Budapest

Version 28 Juin 2022

Table des matières

[référence aux dispositions de la Convention de Budapest]

Chapitre I – Terminologie

Article 1 - "Système informatique", "données informatiques", "fournisseur de services", "données relatives au trafic".

Chapitre II - Mesures à prendre au niveau national

Section 1 - Droit pénal matériel

Article 2 - Accès illégal

Article 3 - Interception illégale

Article 4 – Atteinte à l'intégrité des données

Article 5 - Atteinte à l'intégrité du système

Article 6 - Abus de dispositifs

Article 7 - Falsification informatique

Article 8 - Fraude informatique

Article 9 - Infractions se rapportant à la pornographie enfantine

Article 10 - Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

Article 11 - Tentative et complicité

Article 12 - Responsabilité des personnes morales

Article 13 - Sanctions et mesures

Section 2 - Droit procédural

Article 14 - Portée d'application des mesures du droit de procédure

Article 15 - Conditions et sauvegardes

Article 16 - Conservation rapide de données informatiques stockées

Article 17 - Conservation et divulgation rapides de données relatives au trafic

Article 18 - Injonction de produire

Article 19 - Perquisition et saisie de données informatiques stockées

Article 20 - Collecte en temps réel des données relatives au trafic

Article 21 - Interception de données relatives au contenu

Section 3 - Compétence

Article 22 - Compétence

Chapitre III - Coopération internationale

Article 24 - Extradition

Article 25 - Principes généraux relatifs à l'entraide

Article 26 - Information spontanée

Article 27 - Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

Article 28 - Confidentialité et restriction d'utilisation

Article 29 - Conservation rapide des données informatiques stockées

Article 30 - Divulgation rapide de données conservées

Article 31 - Enraide concernant l'accès aux données stockées

Article 32 - Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public

Article 33 - Entraide dans la collecte en temps réel de données relatives au trafic

Article 34 - Entraide en matière d'interception de données relatives au contenu

Article 35 - Réseau 24/7

www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

État :	
Signature de la Convention de Budapest :	N/A
Ratification/adhésion :	

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
Chapitre I - Terminologie	
Article 1 - "Système informatique", "données informatiques", "fournisseur de services", "données relatives au trafic" : Aux fins de la présente Convention : a l'expression «système informatique» désigne 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; b l'expression «données informatiques» désigne 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; c l'expression «fournisseur de services» désigne: i toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et ii toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs. d «données relatives au trafic» désigne 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 de service sous-jacent.	**Loi N° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun** **TITRE PREMIER DISPOSITIONS GENERALES** **Article 4**. Au sens de la présente loi et de ses textes d'application, les définitions ci-après, sont admises : (…) (41) **Données** : représentation de faits, d'informations ou de notions sous une forme susceptible d'être traitée par un équipement terminal, y compris un programme permettant à ce dernier d'exécuter une fonction ; (…) (43) **Données de trafic :** données ayant trait à une communication électronique 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 ; (…) (46) **Fournisseur des services de communications électroniques** : personne physique ou morale fournissant les prestations consistant entièrement ou principalement en la fourniture de communications électroniques ; (…) (72) **Système d'information** : dispositif isolé ou groupe de dispositifs interconnectés ou apparentés, assurant par lui-même ou par un ou plusieurs de ses éléments, conformément à un programme, un traitement automatisé de données ;

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
	D'autres définitions peuvent être trouvées dans d'autres textes tels que : Loi N° 2010/013 du 21 décembre 2010 et son amendement d'avril 2015, Directive No. 07/08-UEAC-133-CM-18 du 19 Décembre 19 2008 fixant le Cadre juridique de la protection des droits des utilisateurs de réseaux et de services de communications électroniques au sein de la CEMAC.
Chapitre II - Mesures à prendre au niveau national	
Section 1 - Droit pénal matériel	
Titre 1 - Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques	
Article 2 - Accès illégal Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.	**Loi N° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun** **TITRE III DE LA CYBERCRIMINALITE** **CHAPITRE II DES INFRACTIONS ET DES SANCTIONS** **Article 65.** (1) Est puni d'un emprisonnement de cinq (05) à dix (10) ans et d'une amende de 5.000.000 (cinq millions) à 10.000.000 (dix millions) F CFA ou de l'une de ces deux peines seulement, celui qui effectue, sans droit ni autorisation, l'interception par des moyens techniques, de données lors des transmissions ou non, à destination, en provenance ou à l'intérieur ou non d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal. (2) Est puni des peines prévues à l'alinéa 1 ci-dessus, tout accès non autorisé, à l'ensemble ou à une partie d'un réseau de communications électroniques ou d'un système d'information ou d'un équipement terminal. (3) Les peines prévues à l'alinéa 1 ci-dessus sont doublées, en cas d'accès illicite portant atteinte à l'intégrité, la confidentialité, la disponibilité du réseau de communications électroniques ou du système d'information. (4) Est puni des mêmes peines prévues à l'alinéa 1 ci-dessus, celui qui, sans droit, permet l'accès dans un réseau de communications électroniques ou dans un système d'information par défi intellectuel. **Article 69.**

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
	Est puni d'un emprisonnement de cinq (05) à dix (10) ans et d'une amende de 10.000.000 (dix millions) à 100.000.000 (cent millions) F CFA ou de l'une de ces deux peines seulement, celui qui accède sans droit, et en violation des mesures de sécurité, à l'ensemble ou à une partie d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal, afin d'obtenir des informations ou des données, en relation avec un système d'information connecté à un autre système d'information.
Article 3 - Interception illégale Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de 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. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.	**Loi N° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun** **TITRE III DE LA CYBERCRIMINALITE** **CHAPITRE II DES INFRACTIONS ET DES SANCTIONS** **Article 65.** (1) Est puni d'un emprisonnement de cinq (05) à dix (10) ans et d'une amende de 5.000.000 (cinq millions) à 10.000.000 (dix millions) F CFA ou de l'une de ces deux peines seulement, celui qui effectue, sans droit ni autorisation, l'interception par des moyens techniques, de données lors des transmissions ou non, à destination, en provenance ou à l'intérieur ou non d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal.
Article 4 - Atteinte à l'intégrité des données 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques. 2 Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.	**Loi N° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun** **TITRE III DE LA CYBERCRIMINALITE** **CHAPITRE II DES INFRACTIONS ET DES SANCTIONS** **Article 71.** Est puni d'un emprisonnement de deux (02) à cinq (05) ans et d'une amende de 1.000.000 (un million) à 25.000.000 (vingt-cinq millions) F CFA, celui qui introduit sans droit, des données dans un système d'information ou dans un réseau de communications électroniques en vue de supprimer ou de modifier les données qui en sont contenues. **Article 72.** Est puni des peines prévues par l'article 66 ci-dessus celui qui, de quelque manière que ce soit, sans droit, introduit, altère, efface, ou supprime, afin d'obtenir un

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
	bénéfice économique, les données électroniques, de manière à causer un préjudice patrimonial à autrui. **Article 86.** (2) Est également puni des mêmes peines prévues à l'alinéa 1 ci-dessus, quiconque provoque une perturbation grave ou une interruption d'un réseau de communications électroniques ou d'un système d'information dans l'intention de porter atteinte à l'intégrité des données. **Article 87.** Les auteurs de l'une des infractions prévues à l'article 86 ci-dessus encourent également les peines complémentaires suivantes : - la confiscation selon les modalités prévues par l'article 35 du Code Pénal, de tout objet ayant servi ou destiné à commettre l'infraction ou considéré comme en étant le produit, à l'exception des objets susceptibles de restitution ; - l'interdiction dans les conditions prévues par l'article 36 du Code Pénal, pour une durée de cinq (05) ans au moins, d'exercer une fonction publique ou une activité socioprofessionnelle, lorsque les faits ont été commis dans l'exercice ou à l'occasion de l'exercice des fonctions ; - la fermeture, dans les conditions prévues par l'article 34 du Code Pénal pour une durée de cinq (05) ans au moins, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ; - l'exclusion, pour une durée de cinq (05) ans au moins, des marchés publics.
Article 5 - Atteinte à l'intégrité du système Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.	**Loi N° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun** **TITRE III DE LA CYBERCRIMINALITE** **CHAPITRE II DES INFRACTIONS ET DES SANCTIONS** **Article 66.** (1) Est puni d'un emprisonnement de deux (02) à cinq (05) ans et d'une amende de 1.000.000 (un million) à 2.000.000 (deux millions) F CFA ou de l'une de ces deux peines seulement, celui qui entraîne la perturbation ou l'interruption du

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
	fonctionnement d'un réseau de communications électroniques ou d'un équipement terminal, en introduisant, transmettant, endommageant, effaçant, détériorant, modifiant, supprimant ou rendant inaccessibles les données. **Article 67.** Constitue une atteinte à l'intégrité d'un réseau de communications électroniques ou d'un système d'information et punie des peines prévues à l'article 66, alinéa 1 ci-dessus, le fait de provoquer une perturbation grave ou une interruption de fonctionnement d'un réseau de communications électroniques d'un équipement terminal par l'introduction, la transmission, la modification, la suppression, l'altération des données. **Article 68.** (1) Est puni d'un emprisonnement de cinq (05) à dix (10) ans et d'une amende de 10.000.000 (dix millions) à 50.000.000 (cinquante millions) F CFA ou de l'une de ces deux peines seulement, celui qui accède ou se maintient, frauduleusement, dans tout ou partie d'un réseau de communications électroniques ou d'un système d'information en transmettant, endommageant, provoquant une perturbation grave ou une interruption du fonctionnement dudit système ou dudit réseau. (2) Les peines prévues à l'alinéa 1 ci-dessus sont doublées s'il en est résulté, soit la suppression ou la modification des données contenues dans le système d'information, soit une altération de son fonctionnement.
Article 6 - Abus de dispositifs 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit: a la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition: i d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus;	**Loi N° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun** **TITRE III DE LA CYBERCRIMINALITE** **CHAPITRE II DES INFRACTIONS ET DES SANCTIONS** **Article 66.** (2) Sont passibles des mêmes peines prévues à l'alinéa 1 ci-dessus, les personnes qui font usage d'un logiciel trompeur ou indésirable en vue d'effectuer des opérations sur un équipement terminal d'un utilisateur sans en informer au préalable celui-ci de la nature exacte des opérations que ledit logiciel est susceptible d'endommager.

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
ii d'un mot de passe, d'un code d'accès ou de 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 ou l'autre des infractions visées par les articles 2 à 5; et b la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée. 2 Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique. 3 Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.	**Article 86.** (1) Est puni des peines prévues l'article 71 ci-dessus, celui qui importe, détient, offre, cède, vend ou met à disposition, sous quelle que forme que ce soit, un programme informatique, un mot de passe, un code d'accès ou toutes données informatiques similaires conçus et ou spécialement adaptés, pour permettre d'accéder, à tout ou partie d'un réseau de communications électroniques ou d'un système d'information.
Titre 2 - Infractions informatiques	
Article 7 - Falsification informatique Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de 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. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.	**Loi N° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun** **TITRE III DE LA CYBERCRIMINALITE** **CHAPITRE II DES INFRACTIONS ET DES SANCTIONS** **Article 71.** Est puni d'un emprisonnement de deux (02) à cinq (05) ans et d'une amende de 1.000.000 (un million) à 25.000.000 (vingt-cinq millions) F CFA, celui qui introduit sans droit, des données dans un système d'information ou dans un réseau de communications électroniques en vue de supprimer ou de modifier les données qui en sont contenues.

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
	Section 72. Est puni des peines prévues par l'article 66 ci-dessus celui qui, de quelque manière que ce soit, sans droit, introduit, altère, efface, ou supprime, afin d'obtenir un bénéfice économique, les données électroniques, de manière à causer un préjudice patrimonial à autrui. **Article 86.** (2) Est également puni des mêmes peines prévues à l'alinéa 1 ci-dessus, quiconque provoque une perturbation grave ou une interruption d'un réseau de communications électroniques ou d'un système d'information dans l'intention de porter atteinte à l'intégrité des données.
Article 8 - Fraude informatique Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui: a par toute introduction, altération, effacement ou suppression de données informatiques; b 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.	**Loi N° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun** **TITRE III DE LA CYBERCRIMINALITE** **CHAPITRE II DES INFRACTIONS ET DES SANCTIONS** **Action 73.** (1) Est puni d'un emprisonnement deux (02) à dix (10) ans et d'une amende de 25.000.000 (vingt-cinq millions) à 50.000.000 (cinquante millions) F CFA, ou de l'une de ces deux peines seulement, celui qui, par la voie d'un système d'information ou dans un réseau de communications contrefait, falsifie une carte de paiement, de crédit, ou de retrait ou fait usage ou tente de faire usage en connaissance de cause, d'une carte de paiement, de crédit ou de retrait contrefaite ou falsifiée.
Titre 3 - Infractions se rapportant au contenu	
Article 9 - Infractions se rapportant à la pornographie enfantine 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit: a la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique;	**Loi N° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun** **TITRE III DE LA CYBERCRIMINALITE** **CHAPITRE II DES INFRACTIONS ET DES SANCTIONS** **Article 76.**

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
b l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique; c la diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique; d le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique; e la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques. 2 Aux fins du paragraphe 1 ci-dessus, le terme «pornographie enfantine» comprend toute matière pornographique représentant de manière visuelle: a un mineur se livrant à un comportement sexuellement explicite; b une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite; c des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite. 3 Aux fins du paragraphe 2 ci-dessus, le terme «mineur» désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans. 4 Une Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, les paragraphes 1, alinéas d. et e, et 2, alinéas b. et c.	Est puni d'un emprisonnement de cinq (05) à dix (10) ans et d'une amende de 5.000.000 (cinq millions) à 10.000.000 (dix millions) F CFA ou de l'une de ces deux peines seulement, celui qui confectionne, transporte, diffuse, par voie de communications électroniques ou d'un système d'information, un message à caractère pornographique enfantine, ou de nature à porter gravement atteinte à la dignité d'un enfant. **Article 80.** (1) Est puni d'un emprisonnement de trois (03) à six (06) ans et d'une amende de 5.000.000 (cinq millions) à 10.000.000 (dix millions) F CFA ou de l'une de ces deux peines seulement, celui qui diffuse, fixe, enregistre ou transmet à titre onéreux ou gratuit l'image présentant les actes de pédophilie sur un mineur par voie de communications électroniques ou d'un système d'information. (2) Est puni des mêmes peines prévues à l'alinéa 1 ci-dessus, quiconque offre, rend disponible ou diffuse, importe ou exporte, par quelque moyen électronique que ce soit, une image ou une représentation à caractère pédophile. (3) Est puni d'un emprisonnement de un (01) à cinq (05) ans et d'une amende de 5.000.000 (cinq millions) à 10.000.000 (dix millions) F CFA ou de l'une de ces deux peines seulement, celui qui détient dans un réseau de communications électroniques ou dans un système d'informations, une image ou une représentation à caractère pédophile. (4) Les peines prévues à l'alinéa 3 ci-dessus sont doublées, lorsqu'il a été utilisé un réseau de communications électroniques pour la diffusion de l'image ou la représentation du mineur à destination du public. (5) Les dispositions du présent article sont également applicables aux images pornographiques mettant en scène les mineurs. **Article 81.** (1) Sont punis des peines prévues à l'article 82 ci-dessous, les faits ci-dessous, lorsqu'ils sont commis en utilisant un réseau de communications électroniques ou un système d'information : - l'offre, la production, la mise à disposition de pornographie enfantine en vue de sa diffusion ;

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
	- le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système d'information ; - le fait pour les personnes majeures de faire des propositions sexuelles à des mineurs de moins de quinze (15) ans ou une personne se présentant comme telle ; - la diffusion ou la transmission de pornographie enfantine par le biais d'un système d'information. (2) Est considéré comme pornographie enfantine, tout acte présentant de manière visuelle : - un mineur se livrant à un comportement sexuellement explicite ; - une personne qui apparaît comme mineur se livrant à un comportement sexuellement explicite ; - des images réalistes présentant un mineur se livrant à un comportement sexuellement explicite. **Article 82.** Est puni du double des peines prévues à l'article 79 de la présente loi celui qui commet ou tente de commettre par voie de communications électroniques un outrage à la pudeur sur un mineur de moins de quinze (15) ans.
Titre 4 - Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes	
Article 10 - Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle, définies par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.	**Loi No. 2000/011 du 19 décembre 2000 relative au droit d'auteur et aux droits voisins** **Titre VI Des infractions, des sanctions et des procédures** **80.** Est constitutive de contrefaçon : a) toute exploitation d'une œuvre littéraire ou artistique faite en violation de la présente loi, par représentation, reproduction, transformation ou distribution par quelque moyen que ce soit; b) toute reproduction, communication au public ou mise à la disposition du public par vente, échange, location d'une interprétation, d'un phonogramme, d'un vidéogramme, réalisées sans l'autorisation lorsqu'elle est exigée, de l'artiste interprète, du producteur de phonogramme ou de vidéogramme, ou de l'entreprise de communication audiovisuelle;

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la législation de ladite Partie, conformément aux obligations que cette dernière a souscrites en application de la Convention internationale pour la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion (Convention de Rome), de l'Accord relatif aux aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations et exécutions, et les phonogrammes, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique. 3 Une Partie peut, dans des circonstances bien délimitées, se réserver le droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 du présent article, à condition que d'autres recours efficaces soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cette Partie en application des instruments internationaux mentionnés aux paragraphes 1 et 2 du présent article.	c) toute atteinte au droit moral, par violation du droit de divulgation, du droit à la paternité ou du droit au respect d'une œuvre littéraire ou artistique; d) toute atteinte au droit à la paternité et au droit à l'intégrité de la prestation de l'artiste-interprète. **81.** Est assimilé à la contrefaçon : a) l'importation, l'exportation, la vente ou la mise en vente des objets contrefaisants; b) l'importation ou l'exportation de phonogrammes ou vidéogrammes réalisées sans autorisation lorsqu'elle est exigée, de l'artiste-interprète ou du producteur de phonogrammes ou de vidéogrammes; c) le fait de fabriquer sciemment ou d'importer en vue de la vente ou de la location, ou d'installer un équipement, matériel, dispositif ou instrument conçu en tout ou partie pour capter frauduleusement des programmes télédiffusés lorsque ces programmes sont réservés à un public déterminé qui y accède moyennant une rémunération versée à son opérateur ou à ses ayants droit ou ayants cause; d) la neutralisation frauduleuse des mesures techniques efficaces dont les titulaires de droits d'auteur et de droits voisins se servent pour la protection de leur production contre les actes non autorisés; e) le fait de laisser reproduire ou de représenter dans son établissement de façon irrégulière les productions protégées en vertu de la présente loi; f) le défaut de versement ou le retard injustifié de versement d'une rémunération prévue par la présente loi; g) le fait d'accomplir les actes suivants, en sachant ou, pour les sanctions civiles, en ayant de justes raisons de croire que cet acte va entraîner, permettre, faciliter ou dissimuler une atteinte à un droit prévu par la présente loi : — supprimer ou modifier sans y être habilité, toute information relative au régime des droits se présentant sous forme électronique; — distribuer, importer aux fins de distribution, communiquer au public sans y être habilité, des originaux ou des exemplaires d'œuvres, d'interprétations, de vidéogrammes, de phonogrammes, de programmes, en sachant que les informations relatives au régime des droits se présentant sous forme électronique ont été supprimées ou modifiées sans autorisation.

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
	82. 1) Les infractions visées aux articles 80 et 81 sont punies d'un emprisonnement de cinq (5) ans à dix (10) ans et d'une amende de 500 000 à 10 000 000 de Francs CFA ou de l'une de ces deux peines seulement. 2) Les peines prévues au présent article sont doublées lorsque l'auteur de l'infraction est le cocontractant du titulaire du droit violé.
Titre 5 - Autres formes de responsabilité et de sanctions	
Article 11 - Tentative et complicité 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise. 2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9.1.a et c de la présente Convention. 3 Chaque Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2 du présent article.	
Article 12 - Responsabilité des personnes morales 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé: a sur un pouvoir de représentation de la personne morale; b sur une autorité pour prendre des décisions au nom de la personne morale; c sur une autorité pour exercer un contrôle au sein de la personne morale.	**Loi N° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun** **TITRE III DE LA CYBERCRIMINALITE** **CHAPITRE II DES INFRACTIONS ET DES SANCTIONS** **Article 64.** (1) Les personnes morales sont pénalement responsables des infractions commises, pour leur compte, par leurs organes dirigeants. (2) La responsabilité pénale des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits.

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
2 Outre les cas déjà prévus au paragraphe 1 du présent article, chaque Partie adopte les mesures qui se révèlent nécessaires pour s'assurer qu'une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission des infractions établies en application de la présence Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité. 3 Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative. 4 Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.	(3) Les peines encourues par les personnes morales sont des amendes de 5.000.000 (cinq millions) à 50.000.000 (cinquante millions) F CFA. (4) Nonobstant la peine prévue à l'alinéa 3 ci-dessus, l'une des peines accessoires suivantes peut également être prononcée à l'encontre des personnes morales : - la dissolution lorsqu'il s'agit d'un crime ou d'un délit puni en ce qui concerne les personnes physiques d'une peine d'emprisonnement supérieure ou égale à trois (03) ans et que la personne morale a été détournée de son objet pour servir de support à la commission des faits incriminés ; - l'interdiction, à titre définitif ou pour une durée de cinq ans au moins, d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ; - la fermeture temporaire pour une durée de cinq (05) ans au moins, dans les conditions prévues par l'article 34 du Code Pénal, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ; - l'exclusion des marchés publics à titre définitif ou pour une durée de cinq (05) ans au moins ; - l'interdiction, à titre définitif ou pour une durée de cinq (05) ans au moins, de faire appel public à l'épargne ; - l'interdiction, pour une durée de cinq (05) ans au moins, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ou d'utiliser des cartes de paiement ; - la confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit ; - la publication ou la diffusion de la décision prononcée soit par la presse écrite, soit par tout moyen de communication au public par voie électronique.
Article 13 - Sanctions et mesures 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les infractions pénales établies en application des articles 2 à 11 soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté. 2 Chaque Partie veille à ce que les personnes morales tenues pour responsables en application de l'article 12 fassent l'objet de sanctions ou de mesures pénales ou non pénales effectives, proportionnées et dissuasives, comprenant des sanctions pécuniaires.	**Loi N° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun** **TITRE III DE LA CYBERCRIMINALITE** **CHAPITRE II DES INFRACTIONS ET DES SANCTIONS** Les sanctions sont énoncées chaque article mentionné précédemment.

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
Section 2 - Droit procédural	
Article 14 - Portée d'application des mesures du droit de procédure 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques. 2 Sauf disposition contraire figurant à l'article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article: a aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention; b à toutes les autres infractions pénales commises au moyen d'un système informatique; et c à la collecte des preuves électroniques de toute infraction pénale. 3 a Chaque Partie peut se réserver le droit de n'appliquer les mesures mentionnées à l'article 20 qu'aux infractions ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles elle applique les mesures mentionnées à l'article 21. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée à l'article 20. b Lorsqu'une Partie, en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, n'est pas en mesure d'appliquer les mesures visées aux articles 20 et 21 aux communications transmises dans un système informatique d'un fournisseur de services: i qui est mis en œuvre pour le bénéfice d'un groupe d'utilisateurs fermé, et ii qui n'emploie pas les réseaux publics de télécommunication et qui n'est pas connecté à un autre système informatique, qu'il soit public ou privé, cette Partie peut réserver le droit de ne pas appliquer ces mesures à de telles communications. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée aux articles 20 et 21.	

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
Article 15 - Conditions et sauvegardes 1 Chaque Partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité. 2 Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question. 3 Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette section sur les droits, responsabilités et intérêts légitimes des tiers.	**Loi No. 96-06 du 18 Janvier 1996 portant révision de la Constitution du 02 juin 1972, modifiée et complétée par la loi No. 2008/001 du 14 avril 2008** **PREAMBULE** Le Peuple camerounais, Proclame que l'être humain, sans distinction de race, de religion, de sexe, de croyance, possède des droits inaliénables et sacrés ; Affirme son attachement aux libertés fondamentales inscrites dans la déclaration universelle des Droits de l'Homme, la charte des Nations-Unies, la charte africaine des droits de l'homme et des peuples et toutes les conventions internationales y relatives et dûment ratifiées, notamment aux principes suivants : - Tous les hommes sont égaux en droits et en devoirs. L'Etat assure à tous les citoyens les conditions nécessaires à leur développement ; - L'Etat assure la protection des minorités et préserve les droits des populations autochtones conformément à la loi ; - La liberté et la sécurité sont garanties à chaque individu dans le respect des droits d'autrui et de l'intérêt supérieur de l'Etat ; - Tout homme a le droit de se fixer en tout lieu et de se déplacer librement, sous réserve des prescriptions légales relatives à l'ordre, à la sécurité et à la tranquillité publics ; - Le domicile est inviolable. Nulle perquisition ne peut avoir lieu qu'en vertu de la loi ; - Le secret de toute correspondance est inviolable. Il ne peut y être porté atteinte qu'en vertu des décisions émanant de l'autorité judiciaire ; - Nul ne peut être contraint de faire ce que la loi n'ordonne pas ; - Nul ne peut être poursuivi, arrêté ou détenu que dans les cas et selon les formes déterminées par la loi ; **TITRE PREMIER De l'Etat et de la Souveraineté** **Article premier:** (2) La République du Cameroun est un Etat unitaire décentralisé. Elle 15s tune et indivisible, laïque, démocratique et sociale. Elle reconnaît et protège les valeurs traditionnelles conformes aux principes démocratiques, aux droits de l'homme et à la loi.

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
	Elle assure l'égalité de tous les citoyens devant la loi. **Loi N° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun** **TITRE PREMIER DISPOSITIONS GENERALES** **Article 1.** La présente loi régit le cadre de sécurité des réseaux de communications électroniques et des systèmes d'information, définit et réprime les infractions liées à l'utilisation des technologies de l'information et de la communication au Cameroun. A ce titre, elle vise notamment à : - instaurer la confiance dans les réseaux de communications électroniques et les systèmes d'information ; - fixer le régime juridique de la preuve numérique, des activités de sécurité, de cryptographie et de certification électronique ; - protéger les droits fondamentaux des personnes physiques, notamment le droit à la dignité humaine, à l'honneur et au respect de la vie privée, ainsi que les intérêts légitimes des personnes morales. **CHAPITRE IX DE LA PROTECTION DES RESEAUX DE COMMUNICATIONS ELECTRONIQUES, DES SYSTEMES D'INFORMATION ET DE LA VIE PRIVEE DES PERSONNES** **SECTION IV DE LA PROTECTION DE LA VIE PRIVEE DES PERSONNES** **Article 41.** Toute personne a droit au respect de sa vie privée. Les juges peuvent prendre les mesures conservatoires, notamment le séquestre et la saisie pour empêcher ou faire cesser une atteinte à la vie privée.
Article 16 - Conservation rapide de données informatiques stockées 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, 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.	

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
2 Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite. 3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne. 4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.	
Article 17 - Conservation et divulgation rapides de données relatives au trafic 1 Afin d'assurer la conservation des données relatives au trafic, en application de l'article 16, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires: a pour veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication; et b pour assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par la Partie des fournisseurs de services et de la voie par laquelle la communication a été transmise. 2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.	
Article 18 - Injonction de produire 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner: a à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui	

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
sont stockées dans un système informatique ou un support de stockage informatique; et b à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services. 2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15. 3 Aux fins du présent article, l'expression «données relatives aux abonnés» désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir: a le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service; b l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services; c toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.	
Article 19 - Perquisition et saisie de données informatiques stockées Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire: a à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées; et b à un support du stockage informatique permettant de stocker des données informatiques sur son territoire. 2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de	**Loi N° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun** **TITRE III DE LA CYBERCRIMINALITE** **CHAPITRE I DES DISPOSITIONS DU DROIT PROCESSUEL** **Article 53.** (1) Les perquisitions en matière de cybercriminalité sont susceptibles de porter sur des données qui peuvent être des supports physiques ou des copies réalisées en présence des personnes qui assistent à la perquisition. (2) Lorsqu'une copie des données saisies a été faite, celle-ci peut être détruite sur instruction du Procureur de la République pour des raisons de sécurité.

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système. 3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes: a saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage informatique; b réaliser et conserver une copie de ces données informatiques; c préserver l'intégrité des données informatiques stockées pertinentes; d rendre inaccessibles ou enlever ces données informatiques du système informatique consulté. 4 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à 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 visées par les paragraphes 1 et 2. 5 Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et 15.	(3) Sur accord du Procureur de la République, seuls seront gardés sous scellé par l'Officier de Police Judiciaire, les objets, documents et données utilisées à la manifestation de la vérité. (4) Les personnes présentes lors de la perquisition peuvent être réquisitionnées de fournir les renseignements sur les objets, documents et données saisis. **Article 54.** Les perquisitions et les saisies sont effectuées conformément aux dispositions du Code de Procédure Pénale en tenant compte du dépérissement des preuves. **Article 55.** (1) Lorsqu'il apparaît que les données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait l'objet d'opérations de transformation empêchant d'accéder en clair ou sont de nature à compromettre les informations qu'elles contiennent, le Procureur de la République, le Juge d'Instruction ou la juridiction de jugement peuvent réquisitionner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair desdites données. (2) Lorsqu'un moyen de cryptographie a été utilisé, les autorités judiciaires peuvent exiger la convention secrète de déchiffrement du cryptogramme. **TITRE II DE LA CYBERSECURITE** **CHAPITRE IX DE LA PROTECTION DES RESEAUX DE COMMUNICATIONS ELECTRONIQUES, DES SYSTEMES D'INFORMATION ET DE LA VIE PRIVEE DES PERSONNES** **SECTION I DE LA PROTECTION DES RESEAUX DE COMMUNICATIONS ELECTRONIQUES** **Article 25.** (1) Les opérateurs de réseaux et les fournisseurs de services de communications électroniques ont l'obligation de conserver les données de connexion et de trafic pendant une période de dix (10) ans. (2) Les opérateurs de réseaux et les fournisseurs de services de communications électroniques installent des mécanismes de surveillance de trafic des données de

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
	leurs réseaux. Ces données peuvent être accessibles lors des investigations judiciaires. (3) La responsabilité des opérateurs de réseaux et celles des fournisseurs de services de communications électroniques est engagée si l'utilisation des données prévue à l'alinéa 2 ci-dessus porte atteinte aux libertés individuelles des usagers.
Article 20 - Collecte en temps réel des données relatives au trafic 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes: a à collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, et b à obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes: i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou iii à 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 son territoire au moyen d'un système informatique. 2 Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire. 3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet. 4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.	

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
Article 21 - Interception de données relatives au contenu 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes en ce qui concerne un éventail d'infractions graves à définir en droit interne : a à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, et b à obliger un fournisseur de services, dans le cadre de ses capacités techniques: i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou ii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique. 2 Lorsqu'une Partie, en raison des principes établis dans son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au contenu de communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire. 3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet. 4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.	**Loi N° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun** **TITRE II CYBERSÉCURITÉ** **CHAPITRE IX DE LA PROTECTION DES RESEAUX DE COMMUNICATIONS ELECTRONIQUES, DES SYSTEMES D'INFORMATION ET DE LA VIE PRIVEE DES PERSONNES** **SECTION V DE L'INTERCEPTION DES COMMUNICATIONS ELECTRONIQUES** **Article 49.** Nonobstant les dispositions du Code de Procédure Pénale, en cas de crimes ou délits prévus dans la présente loi, l'Officier de Police Judiciaire peut intercepter, enregistrer ou transcrire toute communication électronique. **Article 50**. Si les opérateurs de réseaux de communications électroniques ou les fournisseurs de services de communications électroniques procèdent au codage, à la compression ou au chiffrement des données transmises, les interceptions correspondantes sont fournies en clair aux services qui les ont requis. **Article 51.** Les personnels des opérateurs des réseaux de communications électroniques ou des fournisseurs de services de communications électroniques sont astreints au secret professionnel quant aux réquisitions reçues.
Section 3 - Compétence	
Article 22 - Compétence	**Loi N° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun**

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux articles 2 à 11 de la présente Convention, lorsque l'infraction est commise: a sur son territoire; ou b à bord d'un navire battant pavillon de cette Partie; ou c à bord d'un aéronef immatriculé selon les lois de cette Partie; ou d par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat. 2 Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou des conditions spécifiques, les règles de compétence définies aux paragraphes 1.b à 1.d du présent article ou dans une partie quelconque de ces paragraphes. 3 Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, paragraphe 1, de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition. 4 La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne. 5 Lorsque plusieurs Parties revendiquent une compétence à l'égard d'une infraction présumée visée dans la présente Convention, les Parties concernées se concertent, lorsque cela est opportun, afin de déterminer la mieux à même d'exercer les poursuites.	**TITRE III DE LA CYBERCRIMINALITE** **CHAPITRE I DES DISPOSITIONS DU DROIT PROCESSUEL** **Article 57.** (1) Les autorités judiciaires camerounaises peuvent donner commission rogatoire tant nationale qu'internationale, à toute personne morale ou physique pour rechercher les éléments constitutifs des infractions de cybercriminalité, dont au moins l'un des éléments constitutifs a été commis sur le territoire camerounais ou dont l'un des auteurs ou complices se trouve dans ledit territoire. (2) Sous réserve des règles de réciprocité entre le Cameroun et les pays étrangers liés par un accord de coopération judiciaire, les commissions rogatoires sont exécutées conformément aux dispositions du Code de Procédure Pénale.
Chapitre III - Coopération internationale	
Article 24 - Extradition 1 a Le présent article s'applique à l'extradition entre les Parties pour les infractions pénales définies conformément aux articles 2 à 11 de la présente Convention, à condition qu'elles soient punissables dans la législation des deux Parties concernées par une peine privative de liberté pour une période maximale d'au moins un an, ou par une peine plus sévère.	Les dispositions relatives à l'extradition peuvent être trouvées dans le **Code de procédure pénale** (Arts. 635-675).

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
b Lorsqu'il est exigé une peine minimale différente, sur la base d'un traité d'extradition tel qu'applicable entre deux ou plusieurs parties, y compris la Convention européenne d'extradition (STE n° 24), ou d'un arrangement reposant sur des législations uniformes ou réciproques, la peine minimale prévue par ce traité ou cet arrangement s'applique. 2 Les infractions pénales décrites au paragraphe 1 du présent article sont considérées comme incluses en tant qu'infractions pouvant donner lieu à extradition dans tout traité d'extradition existant entre ou parmi les Parties. Les Parties s'engagent à inclure de telles infractions comme infractions pouvant donner lieu à extradition dans tout traité d'extradition pouvant être conclu entre ou parmi elles. 3 Lorsqu'une Partie conditionne l'extradition à l'existence d'un traité et reçoit une demande d'extradition d'une autre Partie avec laquelle elle n'a pas conclu de traité d'extradition, elle peut considérer la présente Convention comme fondement juridique pour l'extradition au regard de toute infraction pénale mentionnée au paragraphe 1 du présent article. 4 Les Parties qui ne conditionnent pas l'extradition à l'existence d'un traité reconnaissent les infractions pénales mentionnées au paragraphe 1 du présent article comme des infractions pouvant donner lieu entre elles à l'extradition. 5 L'extradition est soumise aux conditions prévues par le droit interne de la Partie requise ou par les traités d'extradition en vigueur, y compris les motifs pour lesquels la Partie requise peut refuser l'extradition. 6 Si l'extradition pour une infraction pénale mentionnée au paragraphe 1 du présent article est refusée uniquement sur la base de la nationalité de la personne recherchée ou parce que la Partie requise s'estime compétente pour cette infraction, la Partie requise soumet l'affaire, à la demande de la Partie requérante, à ses autorités compétentes aux fins de poursuites, et rendra compte, en temps utile, de l'issue de l'affaire à la Partie requérante. Les autorités en question prendront leur décision et mèneront l'enquête et la procédure de la même manière que pour toute autre infraction de nature comparable, conformément à la législation de cette Partie. 7 a Chaque Partie communique au Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, le nom et l'adresse de chaque autorité responsable de l'envoi ou de la réception d'une demande d'extradition ou d'arrestation provisoire, en l'absence de traité.	

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
b Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités ainsi désignées par les Parties. Chaque Partie doit veiller en permanence à l'exactitude des données figurant dans le registre.	
Article 25 - Principes généraux relatifs à l'entraide 1 Les Parties s'accordent l'entraide la plus large possible 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. 2 Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 27 à 35. 3 Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les 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. L'Etat requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication. 4 Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale. 5 Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne 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 la Partie requérante.	**Loi N° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun** **TITRE III DE LA CYBERCRIMINALITE** **CHAPITRE I DES DISPOSITIONS DU DROIT PROCESSUEL** **Article 59.** (1) Lorsque les nécessités de l'enquête ou de l'instruction le justifient, l'audition ou l'interrogatoire d'une personne et/ou la confrontation entre plusieurs personnes, peuvent être effectuées en plusieurs points du territoire national se trouvant reliés par des moyens de communications électroniques garantissant la confidentialité de la transmission. Il est dressé, dans chacun des lieux, un Procès-verbal des opérations qui y ont été effectuées. Ces opérations peuvent faire l'objet d'enregistrement audiovisuel et/ou sonore. (2) Lorsque les circonstances l'exigent, l'interprétation peut être faite au cours d'une audition, d'un interrogatoire ou d'une confrontation par des moyens de communications électroniques. (3) Les dispositions du 24manant article sont également applicables pour l'exécution simultanée, sur un point du territoire national et sur un point situé à l'extérieur, des demandes d'entraide 24manant des autorités judiciaires étrangères ou des actes d'entraide réalisés à l'étranger sur demande des autorités judiciaires camerounaises. (4) Les modalités d'application du présent article sont définies par voie réglementaire.
Article 26 - Information spontanée 1 Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes	

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre. 2 Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières.	
Article 27 - Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables 1 En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions des paragraphes 2 à 9 du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du reste de cet article. 2 a Chaque Partie désigne une ou plusieurs autorités centrales chargées d'envoyer les demandes d'entraide ou d'y répondre, de les exécuter ou de les transmettre aux autorités compétentes pour leur exécution; b Les autorités centrales communiquent directement les unes avec les autres; c Chaque Partie, au moment de la signature ou du dépôt de ses instruments de ratification, d'acceptation, d'approbation ou d'adhésion, communique au Secrétaire Général du Conseil de l'Europe les noms et adresses des autorités désignées en application du présent paragraphe; d Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités centrales désignées par les Parties. Chaque Partie veille en permanence à l'exactitude des données figurant dans le registre. 3 Les demandes d'entraide sous le présent article sont exécutées conformément à la procédure spécifiée par la Partie requérante, sauf lorsqu'elle est incompatible avec la législation de la Partie requise. 4 Outre les conditions ou les motifs de refus prévus à l'article 25, paragraphe 4, l'entraide peut être refusée par la Partie requise:	**Loi N° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun** **TITRE IV DE LA COOPERATION ET DE L'ENTRAIDE JUDICIAIRE INTERNATIONALES** **CHAPITRE II DE L'ENTRAIDE JUDICIAIRE INTERNATIONALE** **Article 91.** (1) A moins qu'une convention internationale à laquelle le Cameroun est partie n'en dispose autrement, les demandes d'entraide émanant des autorités judiciaires camerounaises et destinées aux autorités judiciaires étrangères sont transmises par l'intermédiaire du Ministère chargé des Relations Extérieures. Les pièces d'exécution sont renvoyées aux autorités de l'Etat requérant par la même voie. (2) Les demandes d'entraide émanant des autorités judiciaires étrangères et destinées aux autorités judiciaires camerounaises doivent être présentées par la voie diplomatique par le Gouvernement étranger intéressé. Les pièces d'exécution sont renvoyées aux autorités de l'Etat requérant par la même voie. (3) En cas d'urgence, les demandes d'entraide demandées par les autorités camerounaises ou étrangères peuvent être transmises directement aux autorités de l'Etat requis pour leur exécution. Le renvoi des pièces d'exécution aux autorités compétentes de l'Etat requérant est effectué selon les mêmes modalités. (4) Sous réserve des conventions internationales, les demandes d'entraide émanant des autorités judiciaires étrangères et destinées aux autorités judiciaires

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou b si la Partie requise estime 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. 5 La Partie requise peut surseoir à l'exécution de la demande si cela risquerait de porter préjudice à des enquêtes ou procédures conduites par ses autorités 6 Avant de refuser ou de différer sa coopération, la Partie requise examine, après avoir le cas échéant consulté la Partie requérante, s'il peut être fait droit à la demande partiellement, ou sous réserve des conditions qu'elle juge nécessaires. 7 La Partie requise informe rapidement la Partie requérante de la suite qu'elle entend donner à la demande d'entraide. Elle doit motiver son éventuel refus d'y faire droit ou l'éventuel ajournement de la demande. La Partie requise informe également la Partie requérante de tout motif rendant l'exécution de l'entraide impossible ou étant susceptible de la retarder de manière significative. 8 La Partie requérante peut demander que la Partie requise garde confidentiels le fait et l'objet de toute demande formulée au titre du présent chapitre, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si la Partie requise ne peut faire droit à cette demande de confidentialité, elle doit en informer rapidement la Partie requérante, qui devra alors déterminer si la demande doit néanmoins être exécutée. 9 a En cas d'urgence, les autorités judiciaires de la Partie requérante peuvent adresser directement à leurs homologues de la Partie requise les demandes d'entraide ou les communications s'y rapportant. Dans un tel cas, copie est adressée simultanément aux autorités centrales de la Partie requise par le biais de l'autorité centrale de la Partie requérante. b Toute demande ou communication formulée au titre du présent paragraphe peut l'être par l'intermédiaire de l'Organisation internationale de police criminelle (Interpol). c Lorsqu'une demande a été formulée en application de l'alinéa a. du présent article et lorsque l'autorité n'est pas compétente pour la traiter,	camerounaises doivent faire l'objet d'un avis de la part du gouvernement étranger intéressé. Cet avis est transmis aux autorités judiciaires compétentes par voie diplomatique. (5) En cas d'urgence, les demandes d'entraide émanant des autorités judiciaires étrangères sont transmises au Procureur de la République ou au Juge d'Instruction territorialement compétent. (6) Si le Procureur de la République reçoit directement d'une autorité étrangère, une demande d'entraide qui ne peut être exécutée que par le Juge d'Instruction, il la transmet pour exécution à ce dernier ou saisit le Procureur Général dans le cas prévu à l'article 94 de la présente loi. (7) Avant de procéder à l'exécution d'une demande d'entraide dont il a été directement saisi, le Juge d'Instruction la communique immédiatement pour avis au Procureur de la République. **Article 92.** (1) Les demandes d'entraide émanant des autorités judiciaires étrangères sont exécutées par le Procureur de la République ou par les officiers ou agents de Police Judiciaire requis à cette fin par ce magistrat. (2) Elles sont exécutées par le Juge d'Instruction ou par des officiers de Police Judiciaire agissant sur commission rogatoire de ce magistrat lorsqu'elles nécessitent certains actes de procédure qui ne peuvent être ordonnés ou exécutés qu'au cours d'une instruction préparatoire. **Article 93** (1) Les demandes d'entraide émanant des autorités judiciaires étrangères sont exécutées selon les règles de procédure prévues par le Code de Procédure Pénale. (2) Toutefois, si la demande d'entraide le précise, elle est exécutée selon les règles de procédure expressément indiquées par les autorités compétentes de l'Etat requérant, sans que ces règles ne réduisent les droits des parties ou les garanties procédurales prévues par le Code de Procédure Pénale.

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
elle la transmet à l'autorité nationale compétente et en informe directement la Partie requérante. d Les demandes ou communications effectuées en application du présent paragraphe qui ne supposent pas de mesure de coercition peuvent être directement transmises par les autorités compétentes de la Partie requérante aux autorités compétentes de la Partie requise. e Chaque Partie peut informer le Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, que, pour des raisons d'efficacité, les demandes faites sous ce paragraphe devront être adressées à son autorité centrale.	(3) Lorsque la demande d'entraide ne peut être exécutée conformément aux exigences de l'Etat requérant, les autorités compétentes camerounaises en informent sans délai les autorités de l'Etat requérant et indiquent dans quelles conditions la demande pourrait être exécutée. (4) Les autorités camerounaises compétentes et celles de l'Etat requérant peuvent ultérieurement s'accorder sur la suite à réserver à la demande, le cas échéant, en la subordonnant au respect desdites conditions. (5) L'irrégularité de la transmission de la demande d'entraide ne peut constituer une cause de nullité des actes accomplis en exécution de cette demande. **Article 94.** (1) Si l'exécution d'une demande d'entraide émanant d'une autorité judiciaire étrangère est de nature à porter atteinte à l'ordre public ou aux intérêts essentiels de la Nation, le Procureur de la République saisi ou avisé de cette demande, la transmet au Procureur Général qui en saisit le Ministre chargé de la Justice et donne, le cas échéant, avis de cette transmission au Procureur de la République. (2) S'il est saisi, le Ministre chargé de la Justice informe l'autorité requérante, le cas échéant, de ce qu'il ne peut être donné suite, totalement ou partiellement, à sa demande. Cette information est notifiée à l'autorité judiciaire concernée et fait obstacle à l'exécution de la demande d'entraide ou au retour des pièces d'exécution.
Article 28 - Confidentialité et restriction d'utilisation 1 En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du présent article. 2 La Partie requise peut subordonner la communication d'informations ou de matériels en réponse à une demande: a à la condition que ceux-ci restent confidentiels lorsque la demande d'entraide ne pourrait être respectée en l'absence de cette condition; ou	

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
b à la condition qu'ils ne soient pas utilisés aux fins d'enquêtes ou de procédures autres que celles indiquées dans la demande. 3 Si la Partie requérante ne peut satisfaire à l'une des conditions énoncées au paragraphe 2, elle en informe rapidement la Partie requise, qui détermine alors si l'information doit néanmoins être fournie. Si la Partie requérante accepte cette condition, elle sera liée par celle-ci. 4 Toute Partie qui fournit des informations ou du matériel soumis à l'une des conditions énoncées au paragraphe 2 peut exiger de l'autre Partie qu'elle lui communique des précisions, en relation avec cette condition, quant à l'usage fait de ces informations ou de ce matériel.	
Article 29 - Conservation rapide de données informatiques stockées 1 Une Partie peut demander à une autre Partie d'ordonner ou d'imposer d'une autre façon la conservation rapide de données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, et au sujet desquelles la Partie requérante a l'intention de 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 desdites données. 2 Une demande de conservation faite en application du paragraphe 1 doit préciser: a l'autorité qui demande la conservation; b l'infraction faisant l'objet de l'enquête ou de procédures pénales et un bref exposé des faits qui s'y rattachent; c les données informatiques stockées à conserver et la nature de leur lien avec l'infraction; d toutes les informations disponibles permettant d'identifier le gardien des données informatiques stockées ou l'emplacement du système informatique; e la nécessité de la mesure de conservation; et f le fait que la Partie 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. 3 Après avoir reçu la demande d'une autre Partie, la Partie requise doit prendre toutes les mesures appropriées afin de procéder sans délai à la conservation des données spécifiées, conformément à son droit interne. Pour	

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
pouvoir répondre à une telle demande, la double incrimination n'est pas requise comme condition préalable à la conservation. 4 Une Partie qui exige la double incrimination comme condition pour répondre à une demande d'entraide visant la perquisition ou l'accès similaire, la saisie ou l'obtention par un moyen similaire ou la divulgation des données stockées peut, pour des infractions autres que celles établies conformément aux articles 2 à 11 de la présente Convention, se réserver le droit de refuser la demande de conservation au titre du présent article dans le cas où elle a des raisons de penser que, au moment de la divulgation, la condition de double incrimination ne pourra pas être remplie. 5 En outre, une demande de conservation peut être refusée uniquement: a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou b si la Partie requise 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. 6 Lorsque la Partie requise estime que la conservation simple ne suffira pas à garantir la disponibilité future des données, ou compromettra la confidentialité de l'enquête de la Partie requérante, ou nuira d'une autre façon à celle-ci, elle en informe rapidement la Partie requérante, qui décide alors s'il convient néanmoins d'exécuter la demande. 7 Toute conservation effectuée en réponse à une demande visée au paragraphe 1 sera valable pour une période d'au moins soixante jours afin de permettre à la Partie requérante 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 - Divulgation rapide de données conservées 1 Lorsque, en exécutant une demande de conservation de données relatives au trafic concernant une communication spécifique formulée en application de l'article 29, la Partie requise découvre qu'un fournisseur de services dans un autre Etat a participé à la transmission de cette communication, la Partie requise divulgue rapidement à la Partie requérante une quantité suffisante de données concernant le trafic, aux fins d'identifier	

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
ce fournisseur de services et la voie par laquelle la communication a été transmise. 2 La divulgation de données relatives au trafic en application du paragraphe 1 peut être refusée seulement: a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou b 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 – Entraide concernant l'accès aux données stockées 1 Une Partie peut demander à une autre Partie de perquisitionner ou d'accéder de façon similaire, de saisir ou d'obtenir de façon similaire, de divulguer des données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, y compris les données conservées conformément à l'article 29. 2 La Partie requise satisfait à la demande en appliquant les instruments internationaux, les arrangements et les législations mentionnés à l'article 23, et en se conformant aux dispositions pertinentes du présent chapitre. 3 La demande doit être satisfaite aussi rapidement que possible dans les cas suivants: a il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification; ou b les instruments, arrangements et législations visés au paragraphe 2 prévoient une coopération rapide.	
Article 32 - Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public Une Partie peut, sans l'autorisation d'une autre Partie : a accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou b accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.	

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
Article 33 - Entraide dans la collecte en temps réel de données relatives au trafic 1 Les Parties s'accordent l'entraide dans la collecte en temps réel de données relatives au trafic, associées à des communications spécifiées sur leur territoire, transmises au moyen d'un système informatique. Sous réserve des dispositions du paragraphe 2, cette entraide est régie par les conditions et les procédures prévues en droit interne. 2 Chaque Partie 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 - Entraide en matière d'interception de données relatives au contenu Les Parties s'accordent l'entraide, dans la mesure permise par leurs traités et lois internes applicables, pour la collecte ou l'enregistrement en temps réel de données relatives au contenu de communications spécifiques transmises au moyen d'un système informatique.	
Article 35 - Réseau 24/7 Chaque Partie désigne un point de contact 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 englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes: a apport de conseils techniques; b conservation des données, conformément aux articles 29 et 30; c recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects. 2 a Le point de contact d'une Partie aura les moyens de correspondre avec le point de contact d'une autre Partie selon une procédure accélérée. b Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette Partie responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités, selon une procédure accélérée. 3 Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.	
Article 42 - Réserves	

Retour à la table des matières

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, tout Etat peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la ou les réserves prévues à l'article 4, paragraphe 2, à l'article 6, paragraphe 3, à l'article 9, paragraphe 4, à l'article 10, paragraphe 3, à l'article 11, paragraphe 3, à l'article 14, paragraphe 3, à l'article 22, paragraphe 2, à l'article 29, paragraphe 4, et à l'article 41, paragraphe 1. Aucune autre réserve ne peut être faite.	

Retour à la table des matières