

Législation sur la cybercriminalité

Équivalent national des dispositions de la Convention de Budapest

Version 01/06/2020

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 - Divulgence rapide de données conservées

Article 31 - Entraide 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

Ce profil a été préparé par le Bureau du programme sur la cybercriminalité (C-PROC) du Conseil de l'Europe en vue de partager des informations sur la législation en matière de cybercriminalité et d'évaluer l'état actuel de la mise en œuvre de la Convention de Budapest sur la cybercriminalité dans les législations nationales. Il ne reflète pas nécessairement les positions officielles de l'Etat concerné ou du Conseil de l'Europe.

www.coe.int/cybercrime

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

État :	
Signature de la Convention de Budapest :	n/a
Ratification/adhésion :	n/a

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
Chapitre I - Terminologie	
<p>Article 1 - "Système informatique", "données informatiques", "fournisseur de services", "données relatives au trafic" :</p> <p>Aux fins de la présente Convention :</p> <p>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;</p> <p>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;</p> <p>c l'expression «fournisseur de services» désigne:</p> <p>i toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et</p> <p>ii toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.</p> <p>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.</p>	<p>LOI N° 2018 - 026 du 07/12/18 SUR LA CYBERSECURITE ET LA LUTTE CONTRE LA CYBERCRIMINALITE</p> <p>Art. 2 : Définitions</p> <p>48) 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;</p> <p>49) Données informatisées : toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique;</p> <p>54) Fournisseur des services de communications électroniques : personne physique ou morale fournissant les prestations consistant entièrement ou principalement en la fourniture de communications électroniques;</p> <p>85) Système informatique: tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données informatiques, ainsi que les données informatiques traitées, stockées, récupérées ou transmises par ce dispositif ou cet ensemble de dispositifs en vue du fonctionnement, de l'utilisation, de la protection ou de la maintenance de celui-ci.</p>

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
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	
<p>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.</p>	<p>LOI N° 2018 - 026 du 07/12/18 SUR LA CYBERSECURITE ET LA LUTTE CONTRE LA CYBERCRIMINALITE</p> <p>Art. 8 : Accès et maintien frauduleux à un système informatique</p> <p>Est punie d'une peine d'emprisonnement de six (6) mois à deux (2) ans et d'une amende de cinq millions (5 000 000) à vingt millions (20 000 000) de francs CFA ou de l'une de ces deux (2) peines, toute personne qui, sans droit, accède ou tente d'accéder, se maintient ou tente de se maintenir dans tout ou partie d'un système informatique.</p> <p>Les peines prévues à l'alinéa précédent sont portées au double lorsqu'il en est résulté une perturbation grave ou interruption de ce système informatique.</p> <p>Lorsque l'infraction au présent article est commise au préjudice de l'Etat togolais, les peines encourues sont portées à cinq (5) ans d'emprisonnement et à une amende de quinze millions (15 000 000) à soixante millions (60 000 000) de francs CFA.</p>
<p>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.</p>	<p>LOI N° 2018 - 026 du 07/12/18 SUR LA CYBERSECURITE ET LA LUTTE CONTRE LA CYBERCRIMINALITE</p> <p>Art. 9 : Entrave au fonctionnement d'un système informatique</p> <p>Est punie d'une peine d'emprisonnement de trois (3) à cinq (5) ans et d'une amende de vingt-cinq millions (25 000 000) à cent millions (100 000 000) de francs CFA, toute personne qui, avec ou sans droit détruit, entrave, fausse, perturbe, interrompt le fonctionnement d'un système informatique.</p>

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
<p>Article 4 - Atteinte à l'intégrité des données</p> <p>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.</p> <p>2 Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.</p>	<p>LOI N° 2018 - 026 du 07/12/18 SUR LA CYBERSECURITE ET LA LUTTE CONTRE LA CYBERCRIMINALITE</p> <p>Art. 10 : Atteinte aux données informatisées</p> <p>Est punie d'une peine d'emprisonnement de trois (3) à cinq (5) ans et d'une amende de vingt-cinq millions (25 000 000) à cent millions (100 000 000) de francs CFA, toute personne qui, avec ou sans droit :</p> <ol style="list-style-type: none"> 1) introduit, supprime ou modifie les données informatiques d'un système informatique ; 2) détruit, détériore, altère, rend inaccessibles ou endommage ces données ; 3) soustrait ces données pour son usage personnel ou pour les céder à un tiers, à titre onéreux ou gratuit ; 4) détruit, entrave, fausse, perturbe, interrompt le fonctionnement d'un système informatique. <p>Est punie des mêmes peines, toute personne qui intercepte frauduleusement par des moyens techniques des données informatisées lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système informatique.</p> <p>Lorsque l'infraction définie au présent article est commise au préjudice de l'Etat togolais, son auteur est puni d'une peine de vingt (20) à trente (30) ans de réclusion criminelle et d'une amende de cinquante millions (50 000 000) à cent cinquante millions (150 000 000) de francs CFA</p>
<p>Article 5 - Atteinte à l'intégrité du système</p> <p>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.</p>	
<p>Article 6 - Abus de dispositifs</p> <p>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:</p> <p>a la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition:</p>	<p>LOI N° 2018 - 026 du 07/12/18 SUR LA CYBERSECURITE ET LA LUTTE CONTRE LA CYBERCRIMINALITE</p> <p>Art. 34 : Disposition d'un équipement pour commettre des infractions</p> <p>La production, la commercialisation, la fourniture ou la maintenance d'outils, d'équipements, de programmes informatiques, de dispositifs, de données, de</p>

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
<p>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;</p> <p>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</p> <p>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.</p> <p>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.</p> <p>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.</p>	<p>mots de passe, codes d'accès ou données informatisées similaires, conçus ou destinés à commettre les délits et les crimes visés au présent chapitre, lorsqu'on ne peut méconnaître l'usage délictueux ou criminel qui peut en être fait par nature ou par destination, est punie d'une peine d'emprisonnement d'un (1) à cinq (5) an(s) et d'une amende de cinq millions (5 000 000) à cinquante millions (50 000.000) de francs CFA.</p> <p>Lorsque l'infraction définie au présent article a été commise au préjudice de l'Etat togolais, les peines encourues sont portées à dix (10) ans de réclusion criminelle et à une amende de deux cent millions (200 000 000) de francs CFA.</p>
Titre 2 - Infractions informatiques	

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
<p>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.</p>	
<p>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:</p> <p>a par toute introduction, altération, effacement ou suppression de données informatiques;</p> <p>b par toute forme d'atteinte au fonctionnement d'un système informatique,</p> <p>dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.</p>	<p>LOI N° 2018 - 026 du 07/12/18 SUR LA CYBERSECURITE ET LA LUTTE CONTRE LA CYBERCRIMINALITE</p> <p>Art. 19 : Vol d'information ou de données</p> <p>La soustraction frauduleuse d'information ou de données au préjudice d'autrui est assimilée au vol et est punie conformément aux peines prévues par le code pénal.</p> <p>Art. 20 : Circonstances aggravantes</p> <p>Le fait d'utiliser les technologies de l'information et de la communication ou d'agir en bande organisée en vue de commettre des infractions de droit commun comme le vol, l'escroquerie, le recel, l'abus de confiance, constitue une circonstance aggravante de ces infractions au sens de la présente loi.</p> <p>Lorsque les infractions visées au premier alinéa du présent article ont été commises par le biais d'un système informatique, les peines prévues dans le code pénal ou autre texte législatif en vigueur pour les sanctionner peuvent être portées au double.</p> <p>Lorsque les infractions ont été commises par le biais d'un système informatique, il ne peut être prononcé le sursis à l'exécution</p>
Titre 3 - Infractions se rapportant au contenu	
<p>Article 9 - Infractions se rapportant à la pornographie infantile 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit</p>	<p>LOI N° 2018 - 026 du 07/12/18 SUR LA CYBERSECURITE ET LA LUTTE CONTRE LA CYBERCRIMINALITE</p>

CONVENTION DE BUDAPEST**LÉGISLATION NATIONALE**

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;
- 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.

Art.11: Production d'une image ou d'une représentation à caractère pornographique infantile

Est punie d'une peine de cinq (5) à dix (10) ans de réclusion criminelle et d'une amende de dix millions (10 000 000) à vingt-cinq (25 000 000) de francs CFA ou de l'une de ces deux (2) peines, toute personne qui produit ou enregistre, offre, met à disposition, diffuse, transmet une image ou une représentation présentant un caractère de pornographie mettant en scène un ou plusieurs enfants âgés de moins de quinze (15) ans par le biais d'un système informatique ou par tout autre procédé technique quelconque.

Art.12: Importation ou exportation d'une image ou d'une représentation à caractère pornographique infantile

Est punie de cinq (5) à dix (10) ans de réclusion criminelle et d'une amende de vingt cinq millions (25 000 000) à cinquante millions (50 000 000) de francs CFA ou de l'une de ces deux (2) peines, toute personne qui se procure ou procure à autrui, importe ou fait importer, exporte ou fait exporter une image ou une représentation présentant un caractère pornographique mettant en scène un ou plusieurs enfants âgés de moins de quinze (15) ans par le biais d'un système informatique ou par tout autre procédé technique quelconque.

Art.13 Possession d'une image ou d'une représentation à caractère pornographique infantile

Est punie d'une peine d'emprisonnement de six (6) mois à trois (3) ans et d'une amende d'un million (1 000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux (2) peines, toute personne qui sciemment, possède des images ou représentations présentant un caractère pornographique mettant en scène un ou plusieurs enfants âgés de moins de quinze (15) ans dans un système informatique ou dans un moyen quelconque de stockage de données informatisées.

Art.14 : Facilitation d'accès à des images, des documents, du son ou une représentation présentant un caractère de pornographie à un mineur

Toute personne qui sciemment, facilite l'accès à des images, des documents, du

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
	son ou une représentation présentant un caractère de pornographie à un mineur, est punie de d'un (1) à trois (3) ans d'emprisonnement et d'une amende d'un million (1 000 000) à quinze millions (15 000 000) de francs CFA ou de l'une de ces deux (2) peines.
Titre 4 - Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes	
<p>Article 10 - Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes</p> <p>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.</p> <p>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.</p> <p>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</p>	

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
internationales incombant à cette Partie en application des instruments internationaux mentionnés aux paragraphes 1 et 2 du présent article.	
Titre 5 - Autres formes de responsabilité et de sanctions	
<p>Article 11 - Tentative et complicité</p> <p>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.</p> <p>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.</p> <p>3 Chaque Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2 du présent article.</p>	
<p>Article 12 - Responsabilité des personnes morales</p> <p>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:</p> <p>a sur un pouvoir de représentation de la personne morale;</p> <p>b sur une autorité pour prendre des décisions au nom de la personne morale;</p> <p>c sur une autorité pour exercer un contrôle au sein de la personne morale.</p> <p>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</p>	<p>LOI N° 2018 - 026 du 07/12/18 SUR LA CYBERSECURITE ET LA LUTTE CONTRE LA CYBERCRIMINALITE</p> <p>Art. 36 : Responsabilité des personnes morales</p> <p>Les personnes morales, autres que l'Etat, les collectivités décentralisées et les établissements publics, sont pénalement responsables des infractions prévues par la présente loi, commises pour leur compte par leurs organes ou représentants.</p> <p>La responsabilité des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits.</p> <p>Les peines encourues par les personnes morales sont :</p> <p>1) l'amende qui peut être portée au quintuple de celle encourue par les personnes physiques ou à trois cent millions (300 000 000) de francs CFA si aucune amende n'est prévue ;</p> <p>2) la dissolution, lorsque la personne morale a été créée ou détournée de son objet pour commettre les faits incriminés ;</p> <p>3) l'interdiction à titre définitif ou temporaire d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ;</p> <p>4) la fermeture définitive ou temporaire d'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;</p>

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
<p>application de la présence Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité.</p> <p>3 Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative.</p> <p>4 Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.</p>	<p>5) l'exclusion des marchés publics à titre définitif ou temporaire ;</p> <p>6) l'interdiction à titre définitif ou temporaire de faire appel public à l'épargne ;</p> <p>7) l'interdiction temporaire 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 ;</p> <p>8) la confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit ;</p> <p>9) l'affichage de la décision prononcée ou la diffusion de celle-ci soit par la presse écrite soit par tout moyen de communication au public par voie électronique.</p>
<p>Article 13 - Sanctions et mesures</p> <p>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.</p> <p>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.</p>	
<p>Section 2 - Droit procédural</p>	
<p>Article 14 - Portée d'application des mesures du droit de procédure</p> <p>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.</p> <p>2 Sauf disposition contraire figurant à l'article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article:</p> <p>a aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention;</p> <p>b à toutes les autres infractions pénales commises au moyen d'un système informatique; et</p> <p>c à la collecte des preuves électroniques de toute infraction pénale.</p> <p>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</p>	<p>LOI N° 2018 - 026 du 07/12/18 SUR LA CYBERSECURITE ET LA LUTTE CONTRE LA CYBERCRIMINALITE</p> <p>Art. 40 Prescription en matière d'infractions commises par le biais de réseaux informatiques</p> <p>Les crimes, délits et contraventions, lorsqu'ils sont commis par le biais de réseaux informatiques se prescrivent dans les délais de droit commun à compter de la cessation de l'activité délictueuse en ligne.</p> <p>Art. 41 : Preuve électronique en matière pénale</p> <p>L'écrit électronique en matière pénale est admis comme mode de preuve au même titre que l'écrit sur support papier à condition que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.</p>

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> 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, <p>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.</p>	
<p>Article 15 - Conditions et sauvegardes</p> <p>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.</p> <p>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.</p> <p>3 Dans la mesure où cela est conforme à l'intérêt public, en particulier</p>	

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
<p>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.</p>	
<p>Article 16 - Conservation rapide de données informatiques stockées</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.</p>	
<p>Article 17 - Conservation et divulgation rapides de données relatives au trafic</p> <p>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:</p> <p>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</p> <p>b pour assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité</p>	

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
<p>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.</p> <p>2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.</p>	
<p>Article 18 - Injonction de produire</p> <p>1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner:</p> <p>a à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique; et</p> <p>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.</p> <p>2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.</p> <p>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:</p> <p>a le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service;</p> <p>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;</p> <p>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.</p>	
<p>Article 19 - Perquisition et saisie de données informatiques stockées</p> <p>Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à</p>	<p>LOI N° 2018 - 026 du 07/12/18 SUR LA CYBERSECURITE ET LA LUTTE CONTRE LA CYBERCRIMINALITE</p>

CONVENTION DE BUDAPEST**LÉGISLATION NATIONALE**

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 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.

Art. 42 : Perquisition ou accès à un système informatique

Lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données informatisées sur le territoire togolais, sont utiles à la manifestation de la vérité, l'officier de police judiciaire peut opérer une perquisition, sous le contrôle du procureur de la République, ou accéder à un système informatique ou à une partie de celui-ci ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.

S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par l'officier de police judiciaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur.

Art. 43 : Placement sous scellé de supports électroniques

Lorsque l'officier de police judiciaire 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.

L'officier de police judiciaire désigne, sous le contrôle du procureur de la République, toute personne qualifiée pour utiliser les moyens techniques appropriés afin d'empêcher l'accès aux données visées à l'article 42 de la présente loi dans le système informatique ou aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique et de garantir leur intégrité.

Si les données qui sont liées à l'infraction, soit qu'elles en constituent l'objet, soit qu'elles en ont été 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, l'officier de police judiciaire ordonne, sous le contrôle du procureur de la République, les mesures conservatoires nécessaires, notamment en désignant toute personne qualifiée avec pour mission d'utiliser tous les moyens techniques

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
<p>5 Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et 15.</p>	<p>appropriés pour rendre ces données inaccessibles.</p> <p>Lorsque la mesure prévue à l’alinéa 2 du présent article n’est pas possible, pour des raisons techniques ou en raison du volume des données, l’officier de police judiciaire, sous le contrôle du procureur de la République, 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.</p> <p>L’Officier de police judiciaire, sous le contrôle du procureur de la République, 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.</p>
<p>Article 20 - Collecte en temps réel des données relatives au trafic</p> <p>1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habilitier ses autorités compétentes:</p> <p>a à collecter ou enregistrer par l’application de moyens techniques existant sur son territoire, et</p> <p>b à obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes:</p> <p>i à collecter ou à enregistrer par l’application de moyens techniques existant sur son territoire, ou</p> <p>iii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,</p> <p>en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d’un système informatique.</p> <p>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.</p> <p>3 Chaque Partie adopte les mesures législatives et autres qui se révèlent</p>	

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
<p>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.</p> <p>4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.</p>	
<p>Article 21 - Interception de données relatives au contenu</p> <p>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 :</p> <p>a à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, et</p> <p>b à obliger un fournisseur de services, dans le cadre de ses capacités techniques:</p> <p>i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>4 Les pouvoirs et procédures mentionnés dans le présent article doivent</p>	<p>LOI N° 2018 - 026 du 07/12/18 SUR LA CYBERSECURITE ET LA LUTTE CONTRE LA CYBERCRIMINALITE</p> <p>Art. 44 : Interception des données informatisées</p> <p>Lorsque les nécessités de l'information l'exigent, l'Officier de police judiciaire, sous le contrôle du procureur de la République, peut utiliser les moyens techniques appropriés pour collecter ou enregistrer en temps réel, les données relatives au contenu de communications spécifiques, transmises au moyen d'un système informatique ou obliger un fournisseur de services, dans le cadre de ses capacités techniques à collecter ou à enregistrer, en application de moyens techniques existants, ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer lesdites données informatisées.</p> <p>Le fournisseur d'accès est tenu de garder le secret.</p> <p>Toute violation du secret est punie des peines applicables au délit de violation du secret professionnel.</p>

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
être soumis aux articles 14 et 15.	
Section 3 - Compétence	
<p>Article 22 - Compétence</p> <p>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:</p> <ul style="list-style-type: none"> 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. <p>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.</p> <p>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.</p> <p>4 La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne.</p> <p>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.</p>	

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.

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.

CONVENTION DE BUDAPEST**LÉGISLATION NATIONALE**

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.

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

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
<p>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.</p>	
<p>Article 26 - Information spontanée</p> <p>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 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.</p> <p>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.</p>	
<p>Article 27 - Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables</p> <p>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.</p> <p>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;</p> <p>b Les autorités centrales communiquent directement les unes avec les autres;</p>	

CONVENTION DE BUDAPEST**LÉGISLATION NATIONALE**

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:

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

CONVENTION DE BUDAPEST**LÉGISLATION NATIONALE**

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, 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.

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

b à la condition qu'ils ne soient pas utilisés aux fins d'enquêtes ou de procédures autres que celles indiquées dans la demande.

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
<p>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.</p> <p>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.</p>	
<p>Article 29 - Conservation rapide de données informatiques stockées</p> <p>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.</p> <p>2 Une demande de conservation faite en application du paragraphe 1 doit préciser:</p> <ul style="list-style-type: none"> 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. <p>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 pouvoir répondre à une telle demande, la double incrimination n'est pas requise comme condition préalable à la conservation.</p> <p>4 Une Partie qui exige la double incrimination comme condition pour</p>	

CONVENTION DE BUDAPEST**LÉGISLATION NATIONALE**

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 ce fournisseur de services et la voie par laquelle la communication a été transmise.

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
<p>2 La divulgation de données relatives au trafic en application du paragraphe 1 peut être refusée seulement:</p> <p>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</p> <p>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.</p>	
<p>Article 31 – Entraide concernant l'accès aux données stockées</p> <p>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.</p> <p>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.</p> <p>3 La demande doit être satisfaite aussi rapidement que possible dans les cas suivants:</p> <p>a il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification; ou</p> <p>b les instruments, arrangements et législations visés au paragraphe 2 prévoient une coopération rapide.</p>	
<p>Article 32 - Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public</p> <p>Une Partie peut, sans l'autorisation d'une autre Partie :</p> <p>a accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou</p> <p>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.</p>	
<p>Article 33 - Entraide dans la collecte en temps réel de données relatives au trafic</p>	

CONVENTION DE BUDAPEST	LÉGISLATION NATIONALE
<p>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.</p> <p>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.</p>	
<p>Article 34 - Entraide en matière d'interception de données relatives au contenu</p> <p>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.</p>	
<p>Article 35 - Réseau 24/7</p> <p>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:</p> <ul style="list-style-type: none"> 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. <p>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.</p> <p>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.</p> <p>3 Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.</p>	
<p>Article 42 - Réserves</p>	

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.