Benin

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 25 August 2020

[reference to the provisions of the Budapest Convention]

Chapter I – Use of terms
Article 1 – "Computer system", "computer data", "service provider", "traffic data"

Chapter II – Measures to be taken at the national level
Section 1 – Substantive criminal law
Article 2 – Illegal access
Article 3 – Illegal interception
Article 4 – Data interference
Article 5 – System interference
Article 6 – Misuse of devices
Article 7 – Computer-related forgery
Article 8 – Computer-related fraud
Article 9 – Offences related to child pornography
Article 10 – Offences related to infringements of copyright and related rights
Article 11 – Attempt and aiding or abetting
Article 12 – Corporate liability
Article 13 – Sanctions and measures

Section 2 – Procedural law
Article 14 – Scope of procedural provisions
Article 15 – Conditions and safeguards
Article 16 – Expedited preservation of stored computer data
Article 17 – Expedited preservation and partial disclosure of traffic data
Article 18 – Production order
Article 19 – Search and seizure of stored computer data
Article 20 – Real-time collection of traffic data
Article 21 – Interception of content data

Section 3 – Jurisdiction
Article 22 – Jurisdiction

Chapter III – International co-operation
Article 24 – Extradition
Article 25 – General principles relating to mutual assistance
Article 26 – Spontaneous information
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements
Article 28 – Confidentiality and limitation on use
Article 29 – Expedited preservation of stored computer data
Article 30 – Expedited disclosure of preserved traffic data
Article 31 – Mutual assistance regarding accessing of stored computer data
Article 32 – Trans-border access to stored computer data with consent or where publicly available
Article 33 – Mutual assistance in the real-time collection of traffic data
Article 34 – Mutual assistance regarding the interception of content data
Article 35 – 24/7 Network

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

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

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

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	**Code du numérique (CdN) - Loi no 2017-20 du 20 avril 2018** **Article 1er** : Définitions Au sens du présent code, on entend par : (…) - Données informatiques : toute représentation de faits, d'informations, de concepts, de codes ou d'instructions lisibles par une machine, sous une forme qui se prête à un traitement informatique y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction ; (…) - Données relatives au trafic : toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent ; (…) - Fournisseur de services en ligne : personne physique ou morale qui assure, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par les destinataires de ces services. Il peut notamment s'agir de : • d'entités publiques ou privées qui offrent aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ; • d'entités traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs ; (…)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	- Système informatique : dispositif ou groupe de dispositifs interconnectés ou reliés, dont internet, qui, au moyen d'un programme, procède au traitement automatique des données ou à l'exécution d'autres fonctions. Un système informatique est un dispositif composé de matériels et de logiciels, conçus pour le traitement automatisé des données numériques. Il peut comprendre des moyens d'acquisition, de restitution et de stockage des données. Il peut être isolé ou connecté à d'autres dispositifs similaires au sein d'un réseau ; (…)
Chapter II – Measures to be taken at the national level	
Section 1 – Substantive criminal law	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**CdN** **Article 507 :** Accès et maintien illégal Quiconque accède ou se maintient intentionnellement et sans droit, dans l'ensemble ou partie d'un système informatique est puni d'un emprisonnement de un (01) à cinq (05) ans et d'une amende de cinq cent mille (500 000) francs CFA à un million (1 000 000) de francs CFA ou de l'une de ces peines seulement. Quiconque accède ou se maintient intentionnellement et sans droit, dans l'ensemble ou partie d'un système informatique, avec une intention frauduleuse est puni d'un emprisonnement de deux (02) ans à cinq (05) ans et d'une amende de cinq cent mille (500 000) francs CFA à deux millions (2 000 000) de francs CFA ou de l'une de ces peines seulement. Quiconque avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès légal à un système informatique, est puni d'un emprisonnement de deux (02) ans à cinq (05) ans et d'une amende de cinq cent mille (500 000) francs CFA à deux millions (2 000 000) de francs CFA ou de l'une de ces peines seulement. Lorsqu'il résulte des faits visés aux alinéas 1 à 3 soit la suppression, l'obtention ou la modification de données contenues dans le système informatique, soit une altération du fonctionnement de ce système informatique, les peines prévues dans ces alinéas seront doublées.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Lorsque les faits visés aux alinéas 1 à 3 sont commis en violation de mesures de sécurité, la peine est la réclusion criminelle à temps de dix (10) ans à vingt (20) ans et une amende de cinq millions (5 000 000) de francs CFA à cinq cent millions (500 000 000) de francs CFA. L'accès, pour une durée déterminée, à des systèmes informatiques est autorisé sans que le secret professionnel ou bancaire puisse être opposé conformément aux dispositions du code de procédure pénale.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**CdN** **Article 508** : Atteinte aux données informatiques Quiconque intercepte, divulgue, utilise, altère ou détourne intentionnellement et sans droit par des moyens techniques, des données informatiques lors de leur transmission non publique 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, est puni d'un emprisonnement de deux (02) ans à cinq (05) ans et d'une amende de cinq cent mille (500 000) francs CFA à deux millions (2 000 000) de francs CFA. Quiconque transfère sans autorisation des données d'un système informatique ou d'un moyen de stockage de données informatique est puni d'un emprisonnement de cinq (05) ans à dix (10) ans et d'une amende de cinq millions (5 000 000) à cent millions (100 000 000) de francs CFA. Si l'infraction visée à l'alinéa précédent est commise avec une intention frauduleuse, ou en rapport avec un système informatique connecté à un autre système informatique, ou en contournant les mesures de protection mises en place pour empêcher l'accès au contenu de la transmission non publique, les peines prévues à l'alinéa précédent sont doublées. Une personne ne commet pas une infraction au sens du présent article, si : 1- l'interception est réalisée conformément à un mandat de justice ; 2- la communication est envoyée par ou est destinée à une personne qui a consenti à l'interception ; 3- un fonctionnaire habilité estime qu'une interception est nécessaire en cas d'urgence, dans le but de prévenir un décès, une blessure ou un dommage à la santé physique ou mentale d'une personne, ou d'atténuer une blessure ou

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	un dommage à la santé physique ou mentale d'une personne ; 4- une personne morale ou physique est légalement autorisée pour les besoins de la sécurité publique ou de la défense nationale ; ou 5- une personne morale ou physique est légalement autorisée en vertu des dispositions du code de procédure pénale.
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**CdN** **Article 510** : Atteinte à l'intégrité des données Quiconque, intentionnellement et sans droit, directement ou indirectement endommage, efface, détériore, altère ou supprime des données informatiques est puni d'un emprisonnement de six (06) mois à cinq (05) ans et d'une amende de cinq cent mille (500 000) francs CFA à deux millions (2 000 000) de francs CFA ou de l'une de ces peines seulement. Si l'infraction visée à l'alinéa 1er est commise avec une intention frauduleuse ou dans le but de nuire, la peine d'emprisonnement est de deux (02) ans à cinq (05) ans et d'une amende de cinq cent mille (500 000) francs à deux millions (2 000 000) de francs CFA ou l'une de ces peines seulement. La peine d'emprisonnement et l'amende sont applicables même si les conséquences sur le ou les systèmes informatiques visés aux alinéas précédents sont temporaires ou permanentes. + **Article 508,** *supra* (« altère »)
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	**CdN** **Article 509** : Atteinte à l'intégrité du système Quiconque qui, intentionnellement et sans droit, directement ou indirectement provoque, par tout moyen technologique, une interruption du fonctionnement normal d'un système informatique est puni d'un emprisonnement de deux (02) ans à cinq (05) ans et d'une amende de cinq millions (5 000 000) à cinq cent millions (500 000 000) de francs CFA ou de l'une de ces peines seulement. Quiconque, suite à la commission des faits visés à l'alinéa 1er, cause un dommage à des données dans le système informatique concerné ou dans tout autre système

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	informatique, est puni d'un emprisonnement de cinq (05) ans à dix (10) ans et d'une amende de cinq millions (5 000 000) à cinq cent millions (500 000 000) de francs CFA ou de l'une de ces peines seulement. Quiconque, suite à la commission des faits visés à l'alinéa 1er, provoque une perturbation grave ou empêche, totalement ou partiellement, le fonctionnement normal du système informatique concerné ou de tout autre système informatique, est condamné à la réclusion criminelle à temps de dix (10) ans à vingt (20) ans et à une amende de cinq millions (5 000 000) à cinq cent millions (500 000 000) de francs CFA ou de l'une de ces peines seulement. Lorsque la commission des faits visés à l'alinéa 1er touche une ou plusieurs infrastructures sensibles, au sens du présent code, la personne responsable est condamnée à la réclusion criminelle à temps de dix (10) ans à vingt (20) ans et à une amende de cinq millions (5 000 000) à cinq cent millions (500 000 000) de francs CFA ou de l'une de ces peines seulement. La peine d'emprisonnement et l'amende sont applicables même si les conséquences sur le ou les systèmes informatiques visés aux alinéas précédents sont temporaires ou permanentes.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.	**CdN** **Article 511** : Abus de dispositifs Quiconque, intentionnellement et sans droit, produit, vend, obtient en vue de son utilisation, importe, exporte, diffuse ou met à disposition sous une autre forme, un quelconque dispositif, y compris des données informatiques ou des programmes informatiques, principalement conçu ou adapté pour permettre la commission d'une ou plusieurs infractions visées au Titre I du présent Livre, est puni d'un emprisonnement de deux (02) ans à cinq (05) ans et d'une amende de cinq cent mille (500 000) francs CFA à deux millions (2 000 000) de francs CFA ou de l'une de ces peines seulement. Quiconque, intentionnellement et sans droit, possède au sens du présent code, dans l'intention de l'utiliser, un quelconque dispositif, y compris des données informatiques, principalement conçu ou adapté pour permettre la commission d'une ou plusieurs infractions visées au Titre I du présent Livre est puni d'un emprisonnement de six (06) mois à cinq (05) ans et d'une amende de cinq cent

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	mille (500 000) francs CFA à deux millions (2 000 000) de francs CFA ou de l'une de ces peines seulement. Est puni d'une peine d'emprisonnement de deux (02) ans à cinq (05) ans et d'une amende de cinq cent mille (500 000) francs CFA à deux millions (2 000 000) de francs CFA ou de l'une de ces peines seulement, tout officier ou fonctionnaire public, dépositaire ou agent de la force publique qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme un dispositif, y compris des données informatiques, principalement conçu ou adapté pour permettre la commission d'une ou plusieurs infractions visées au Titre I du présent Livre.
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**CdN** **Article 512** : Falsification informatique Quiconque commet un faux, en introduisant, intentionnellement et sans droit, dans un système informatique, en modifiant, altérant ou effaçant des données, qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation possible des données dans un système informatique, et ce dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si les données falsifiées étaient authentiques, est puni d'un emprisonnement de cinq (05) ans à dix (10) ans et d'une amende de cinq millions (5 000 000) à cinquante millions (50 000 000) de francs CFA ou de l'une de ces peines seulement. Quiconque cherchant à se procurer, pour lui-même ou pour autrui, avec une intention frauduleuse, un avantage économique illégal en introduisant dans un système informatique, en modifiant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation normale des données dans un système informatique, est puni d'un emprisonnement de cinq (05) ans à dix (10) ans et d'une amende de cinq millions (5 000 000) à cinquante millions (50 000 000) de francs CFA ou de l'une de ces peines seulement. Quiconque en connaissance de cause, décide de faire usage de données falsifiées, au sens des alinéas 1 et 2, sans en être l'auteur, est puni d'un emprisonnement

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	de cinq (05) ans à dix (10) ans et d'une amende de cinq millions (5 000 000) à cinquante millions (50 000 000) de francs CFA ou de l'une de ces peines seulement, comme s'il était l'auteur de la falsification informatique. La peine d'emprisonnement et l'amende sont applicables même si les conséquences sur le ou les systèmes informatiques visés aux alinéas précédents sont temporaires ou permanentes.
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**CdN** **Article 513** : Fraude informatique Quiconque, intentionnellement et sans droit, cause ou cherche à causer un préjudice patrimonial à autrui avec l'intention de procurer un avantage économique illégal à soi-même ou à une tierce partie, est puni d'un emprisonnement de cinq (05) ans à dix (10) ans et d'une amende de cinq millions (5 000 000) à cinquante millions (50 000 000) de francs CFA : 1- en introduisant dans un système informatique, en modifiant, altérant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique ; ou 2- en perturbant le fonctionnement normal d'un système informatique ou des données y contenues.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person;	**CdN** **Article 518** : Pédopornographie Quiconque aura par le biais d'un système informatique, intentionnellement et sans droit, exposé, produit pour lui-même ou pour autrui, vendu, offert, loué, distribué, transmis, diffusé, publié ou mis à la disposition des emblèmes, objets, films, photos, diapositives ou autres supports visuels qui représentent des positions ou des actes sexuels à caractère pornographique, impliquant ou présentant des mineurs ou les aura, en vue du commerce ou de la distribution, la diffusion, fabriqués, détenus, importés ou fait importer, remis à un agent de transport ou de distribution, est puni de la réclusion de deux (02) ans à sept (7) ans et d'une

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	amende de vingt millions (20 000 000) à cent millions (100 000 000) de francs CFA. Quiconque acquiert, détient ou aura possédé au sens du présent code, intentionnellement et sans droit, de la pornographie enfantine au sens du présent code dans un système informatique ou un moyen de stockage de données informatique, est puni d'un emprisonnement de six (06) mois à cinq (05) ans et d'une amende de cinquante millions (50 000 000) à cinq cent millions (500 000 000) de francs CFA ou de l'une de ces peines seulement. Quiconque consulte habituellement ou en contrepartie d'un paiement un service de communication au public en ligne mettant à disposition de la pornographie enfantine au sens du présent code, par quelque moyen que ce soit est puni de dix (10) ans d'emprisonnement et de vingt cinq millions (25 000 000) de francs CFA d'amende. Les dispositions du présent article sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur et dont l'objectif est de faire passer la personne comme un mineur et ce même s'il est établi que cette personne était âgée de dix-huit (18) ans au jour de la fixation ou de l'enregistrement de son image. La confiscation peut être appliquée à l'égard des infractions visées aux alinéas 1 et 2, même lorsque la propriété des choses sur lesquelles portent l'infraction n'appartiennent pas au condamné. La responsabilité pénale de l'auteur n'est pas en cause lorsque l'acte est commis dans un objectif de répression de la pédopornographie. Une interdiction, telle que prévue par le code pénal, peut être prononcée par les tribunaux à titre de peine complémentaire. Une interdiction à titre provisoire ou définitive de fréquenter certains endroits, établissements à qui l'on confie la garde des mineurs ou d'exercer certaines activités à même de mettre le condamné en rapport avec des mineurs, peut être prononcée par les tribunaux. Cette interdiction est prolongée en cas de récidive. Sans avoir égard à la qualité de la personne physique ou morale de l'exploitant, propriétaire, locataire ou gérant, le tribunal peut ordonner la fermeture de l'établissement dans lequel les infractions ont été commises, pour une durée de un (01) mois à trois (03) ans.
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights	**CdN**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	**Article 529** : Dispositions existantes Les dispositions du présent chapitre viennent compléter les dispositions de la loi n° 2005-30 du 10 avril 2006 relative à la protection des droits d'auteurs et des droits voisins en République du Bénin. **Article 530** : Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes A l'article 2 de la loi n° 2005-30 du 10 avril 2006 relative à la protection des droits d'auteurs et des droits voisins en République du Bénin, sont apportées les modifications suivantes : « L'auteur de toute œuvre originale de l'esprit, littéraire ou artistique, quels qu'en soient le genre, la forme d'expression, le mérite ou la destination, jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle, exclusif à tous et opposable à tous ». A l'article 8 de la loi n° 2005-30 du 10 avril 2006 relative à la protection des droits d'auteurs et des droits voisins en République du Bénin, sont apportées les modifications suivantes : « Constituent les œuvres de l'esprit protégées par la présente loi : - (…) - les logiciels, y compris le matériel de conception préparatoire ; - (…) ». SECTION I DE L'ATTEINTE AUX DROITS DE PROPRIETE INTELLECTUELLE **Article 531** : Sanctions Sont punis d'une peine d'emprisonnement de trois (03) mois à deux (02) ans et d'une amende de cinq cent mille (500 000) francs CFA à dix millions (10 000 000) de FCFA, les atteintes à la propriété intellectuelle commises au moyen d'un ou sur un réseau de communication électronique ou un système informatique. **Article 532** : Œuvres de l'esprit Constitue une atteinte à la propriété intellectuelle, le fait, sans autorisation de l'auteur ou de ses ayants droit de reproduire, représenter ou de mettre à la disposition du public une œuvre de l'esprit protégée par le droit d'auteur ou un droit voisin au moyen d'un ou sur un réseau de communication électronique ou un système informatique. **Article 533** : Contrefaçon de marque, nom commercial, appellation d'origine, indication géographique Constitue une atteinte à la propriété intellectuelle, le fait sans autorisation de l'auteur ou de ses ayants droit, de reproduire, d'utiliser, de vendre, de dénigrer, de dénaturer une marque, un nom commercial, une appellation d'origine ou une indication géographique appartenant à un tiers au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Article 534 : Contrefaçon de dessins et modèles Constitue une atteinte à la propriété intellectuelle, le fait, sans autorisation de l'auteur ou de ses ayants droit de reproduire, de représenter ou de mettre à la disposition du public, un dessin ou un modèle protégé par le droit d'auteur ou un droit voisin au moyen d'un ou sur un réseau de communication électronique ou un système informatique. **Article 535** : Atteinte aux droits de propriété des brevets Constitue une atteinte à la propriété intellectuelle le fait, en toute connaissance de cause, sans droit, de vendre ou de mettre à disposition du public par reproduction ou par représentation, un bien ou un produit protégé par un brevet d'invention au moyen d'un ou sur un réseau de communication électronique ou un système informatique. **Article 536** : Atteinte aux schémas de configuration de circuits intégrés Constitue une atteinte à la propriété intellectuelle, le fait, en toute connaissance de cause, sans droit, de vendre ou de mettre à disposition du public par reproduction ou par représentation un schéma de configuration de circuits intégrés au moyen d'un ou sur un réseau de communication électronique ou un système informatique. **Article 537** : Atteinte à une mesure technique efficace Est puni de sept cent mille (700 000) francs CFA d'amende, le fait de porter atteinte sciemment, à des fins autres que la recherche, à une mesure technique efficace afin d'altérer la protection d'une œuvre par un décodage, un décryptage ou toute autre intervention personnelle destinée à contourner, neutraliser ou supprimer un mécanisme de protection ou de contrôle, lorsque cette atteinte est réalisée par d'autres moyens que l'utilisation d'une application technologique, d'un dispositif ou d'un composant existant. Est puni de six (6) mois d'emprisonnement et de cinq cent mille (500 000) francs CFA d'amende, le fait de procurer ou proposer sciemment à autrui, directement ou indirectement, des moyens conçus ou spécialement adaptés pour porter atteinte à une mesure technique efficace, par l'un des procédés suivants : 1- en fabriquant ou en important une application technologique, un dispositif ou un composant, à des fins autres que la recherche ; 2- en détenant en vue de la vente, du prêt ou de la location, en offrant à ces mêmes fins ou en mettant à disposition du public sous quelque forme que ce soit, une application technologique, un dispositif ou un composant ; 3- en fournissant un service à cette fin ; 4- en incitant à l'usage ou en commandant, concevant, organisant, reproduisant, distribuant ou diffusant une publicité en faveur de l'un des

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	procédés visés aux points 1 à 3 au moyen d'un ou sur un réseau de communication électronique ou un système informatique. Ces dispositions ne sont pas applicables aux actes réalisés à des fins de sécurité informatique. **Article 538** : Suppression d'un élément d'information sur le régime des droits pour porter atteinte au droit d'auteur Est puni de sept cent mille (700 000) francs CFA d'amende, le fait de supprimer ou de modifier, sciemment et à des fins autres que la recherche, tout élément d'information sur le régime des droits, par une intervention personnelle ne nécessitant pas l'usage d'une application technologique, d'un dispositif ou d'un composant existant, conçus ou spécialement adaptés à cette fin, dans le but de porter atteinte à un droit d'auteur, de dissimuler ou de faciliter une telle atteinte. Est puni de six (6) mois d'emprisonnement et de cinq cent mille (500 000) francs CFA d'amende, le fait de procurer ou proposer sciemment à autrui, directement ou indirectement, des moyens conçus ou spécialement adaptés pour supprimer ou modifier, même partiellement, un élément d'information sur le régime des droits, dans le but de porter atteinte à un droit d'auteur, de dissimuler ou de faciliter une telle atteinte, par l'un des procédés suivants : 1- en fabriquant ou en important une application technologique, un dispositif ou un composant, à des fins autres que la recherche ; 2- en détenant en vue de la vente, du prêt ou de la location, en offrant à ces mêmes fins ou en mettant à disposition du public sous quelque forme que ce soit une application technologique, un dispositif ou un composant ; 3- en fournissant un service à cette fin ; 4- en incitant à l'usage ou en commandant, concevant, organisant, reproduisant, distribuant ou diffusant une publicité en faveur de l'un des procédés visés aux points 1 à 3 au moyen d'un ou sur un réseau de communication électronique ou un système informatique. Est puni de six (6) mois d'emprisonnement et de cinq cent mille (500 000) francs CFA d'amende, le fait sciemment, d'importer, de distribuer, de mettre à disposition du public sous quelque forme que ce soit ou de communiquer au public, directement ou indirectement, une œuvre dont un élément d'information sur le régime des droits a été supprimé ou modifié dans le but de porter atteinte à un droit d'auteur, de dissimuler ou de faciliter une telle atteinte. Ces dispositions ne sont pas applicables aux actes réalisés à des fins de recherche ou de sécurité informatique. **Article 539** : Altération Est puni de sept cent mille (700 000) francs CFA d'amende, le fait de porter atteinte sciemment, à des fins autres que la recherche, à une mesure technique

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	efficace afin d'altérer la protection d'une interprétation, d'un phonogramme, d'un vidéogramme ou d'un programme par un décodage, un décryptage ou toute autre intervention personnelle destinée à contourner, neutraliser ou supprimer un mécanisme de protection ou de contrôle, lorsque cette atteinte est réalisée par d'autres moyens que l'utilisation d'une application technologique, d'un dispositif ou d'un composant existant mentionné au chapitre II du présent Livre. Est puni de six (6) mois d'emprisonnement et de cinq cent mille (500 000) francs CFA d'amende, le fait de procurer ou proposer sciemment à autrui, directement ou indirectement, des moyens conçus ou spécialement adaptés pour porter atteinte à une mesure technique efficace, par l'un des procédés suivants : 1- en fabriquant ou en important une application technologique, un dispositif ou un composant, à des fins autres que la recherche ; 2- en détenant en vue de la vente, du prêt ou de la location, en offrant à ces mêmes fins ou en mettant à disposition du public sous quelque forme que ce soit une application technologique, un dispositif ou un composant ; 3- en fournissant un service à cette fin ; 4- en incitant à l'usage ou en commandant, concevant, organisant, reproduisant, distribuant ou diffusant une publicité en faveur de l'un des procédés visés aux points 1 à 3. Ces dispositions ne sont pas applicables aux actes réalisés à des fins de sécurité informatique. SECTION II DES MOYENS D'ECHANGE ILLICITE ET TELECHARGEMENT SUR INTERNET **Article 540** : Personnes facilitant sur les réseaux, les échanges illicites d'éléments protégés Est puni de trois (3) ans d'emprisonnement et de trois millions (3 000 000) de francs CFA d'amende, le fait : 1- d'éditer, de mettre à la disposition du public ou de communiquer au public, sciemment et sous quelque forme que ce soit, un logiciel manifestement destiné à la mise à disposition du public non autorisée d'œuvres ou d'objets protégés ; 2- d'inciter sciemment, y compris à travers une annonce publicitaire, à l'usage d'un logiciel mentionné au point 1, au moyen d'un ou sur un réseau de communication électronique ou un système informatique. **Article 541** : Atteinte aux droits d'auteur par un service de communication au public en ligne En présence d'une atteinte à un droit d'auteur ou à un droit voisin occasionnée par le contenu d'un service de communication au public en ligne, le tribunal de

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	première instance, peut ordonner à la demande des titulaires de droits sur les œuvres et objets protégés, de leurs ayants droit, toutes mesures propres à prévenir ou à faire cesser une telle atteinte à un droit d'auteur ou un droit voisin, à l'encontre de toute personne susceptible de contribuer à y remédier. **Article 542** : Obligation de l'abonné internet de veiller à ce que son accès internet ne fasse pas l'objet d'une utilisation type téléchargement illicite La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits lorsqu'elle est requise. Le manquement de la personne titulaire de l'accès à l'obligation définie au premier alinéa n'a pas pour effet d'engager la responsabilité pénale de l'intéressé, sous réserve des articles 544 et 545 ci-dessous. **Article 543** : En cas de téléchargement illicite : réponse graduée En cas d'infraction définie à l'article 542 ci-dessus, l'organe national en charge du droit d'auteur et des droits voisins peut envoyer à l'abonné, sous son timbre et pour son compte, par la voie électronique et par l'intermédiaire de la personne dont l'activité est d'offrir un accès à des services de communication au public en ligne ayant conclu un contrat avec l'abonné, une recommandation lui rappelant les dispositions de l'article ci-dessous, lui enjoignant de respecter l'obligation qu'elles définissent et l'avertissant des sanctions encourues. Cette recommandation contient également une information de l'abonné sur l'offre légale de contenus culturels en ligne, sur l'existence de moyens de sécurisation permettant de prévenir les manquements à l'obligation définie à l'article ci-dessus ainsi que sur les dangers pour le renouvellement de la création artistique et pour l'économie du secteur culturel des pratiques ne respectant pas le droit d'auteur et les droits voisins. En cas de renouvellement, dans un délai de six (6) mois à compter de l'envoi de la recommandation visée au 1er alinéa, de faits susceptibles de constituer un manquement à l'obligation définie à l'article ci-dessus, le Bureau béninois du droit d'auteur peut adresser une nouvelle recommandation comportant les mêmes informations que la précédente par la voie électronique dans les conditions prévues au 1er alinéa. Elle doit assortir cette recommandation d'une lettre remise contre signature ou de tout autre moyen propre à établir la preuve de la date de présentation de cette recommandation. Les recommandations adressées sur le fondement du présent article mentionnent la date et l'heure auxquelles les faits susceptibles de constituer un manquement à l'obligation définie à l'article ci-dessus ont été constatés. En revanche, elles ne

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	divulguent pas le contenu des œuvres ou objets protégés concernés par ce manquement. Elles indiquent les coordonnées téléphoniques, postales et électroniques où leur destinataire peut adresser, s'il le souhaite, des observations au Bureau de droit d'auteur et droit voisin et obtenir, s'il en formule la demande expresse, des précisions sur le contenu des œuvres ou objets protégés concernés par le manquement qui lui est reproché. **Article 544** : Sanctions du téléchargement illicite Lorsque l'infraction définie à l'article 542 est commise au moyen d'un service de communication au public en ligne, les personnes coupables des infractions de contrefaçons peuvent en outre être condamnées à la peine complémentaire d'une amende de un million (1 000 000) de francs CFA. Lorsque ce service est acheté selon des offres commerciales composites incluant d'autres types de services, tels que services de téléphonie ou de télévision, les décisions d'amende ne s'appliquent pas à ces services. La prononciation de l'amende n'affecte pas, par elle-même, le versement du prix de l'abonnement au fournisseur du service. **Article 545** : Négligence caractérisée La peine complémentaire définie à l'article précédent peut être prononcée selon les mêmes modalités, en cas de négligence caractérisée définie ci-dessous, à l'encontre du titulaire de l'accès à un service de communication au public en ligne auquel le Bureau béninois du droit d'auteur et droits voisins a préalablement adressé, par voie d'une lettre remise contre signature ou de tout autre moyen propre à établir la preuve de la date de présentation, une recommandation l'invitant à mettre en œuvre un moyen de sécurisation de son accès à internet. La négligence caractérisée s'apprécie sur la base des faits commis au plus tard un (1) an après la présentation de la recommandation mentionnée à l'alinéa précédent. Dans ce cas, l'amende maximale est de cinq cent mille (500 000) francs CFA. **Article 546** : Définition de la négligence caractérisée Constitue une négligence caractérisée le fait, sans motif légitime, pour la personne titulaire d'un accès à des services de communication au public en ligne : 1- soit de ne pas avoir mis en place un moyen de sécurisation de cet accès ; 2- soit d'avoir manqué de diligence dans la mise en œuvre de ce moyen. Les dispositions de l'alinéa 1er ne sont applicables que lorsque se trouvent réunies les deux conditions suivantes : - lorsque le titulaire de l'accès s'est vu recommander par le Bureau béninois du droit d'auteur et des droits voisins de mettre en œuvre un moyen de sécurisation de son accès permettant de prévenir le renouvellement d'une utilisation de celui-ci à des fins de

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	reproduction, de représentation ou de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits ; - dans l'année suivant la présentation de cette recommandation, cet accès est à nouveau utilisé aux fins mentionnées au point 1 du présent alinéa.
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	**CdN** **Article 580** : Tentative Le fait de tenter de commettre l'une des infractions visées au Titre I du présent Livre, est puni des mêmes peines. **Article 581** : Complice Le fait d'inciter à commettre l'une des infractions visées au Titre I du présent Livre, d'y participer ou de s'en rendre complice est puni des mêmes peines
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.	**CdN** **Article 494** : Responsabilité des personnes morales Les personnes morales autres que l'Etat, les collectivités locales et les établissements publics sont responsables des infractions prévues par les dispositions du présent Livre 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 : 1- sur un pouvoir de représentation de la personne morale ; 2- sur une autorité pour prendre des décisions au nom de la personne morale ; 3- sur une autorité pour exercer un contrôle au sein de la personne morale. Outre les cas déjà prévus à l'alinéa précédent, une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée à l'alinéa précédent a rendu possible l'Autorité des infractions prévues par les dispositions du présent Livre pour le

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	compte de ladite personne morale par une personne physique agissant sous son autorité. La responsabilité des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits. Les peines encourues par les personnes morales, pour les infractions visées au Titre I du présent Livre, sont les suivantes : 1- une amende dont le montant maximum est égal au quintuple de celui prévu pour les personnes physiques par la loi qui réprime l'infraction ; 2- la dissolution, lorsque la personne morale a été créée ou, 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 à cinq (05) ans, détournée de son objet pour commettre les faits incriminés ; 3- l'interdiction définitive ou pour une durée de cinq (05) ans au plus d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ; 4- la fermeture définitive ou pour une durée de cinq (05) ans au plus d'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ; 5- l'exclusion définitive des marchés publics ou pour une durée de cinq (05) ans au plus ; 6- l'interdiction définitive ou pour une durée de cinq (05) ans au plus de faire appel public à l'épargne ; 7- l'interdiction pour une durée de cinq (05) ans au plus 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 ; 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 ; Toute personne morale condamnée à l'une des peines ci-dessus énumérées a l'obligation d'afficher la décision prononcée ou de la diffuser par la presse écrite soit par tout moyen de communication au public par voie électronique.
Article 13 – Sanctions and measures 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	**CdN** **Article 492** : Champ d'application Les pouvoirs et procédures prévus dans le présent Titre aux fins d'enquêtes ou de procédures pénales spécifiques s'appliquent : 1. aux infractions pénales établies conformément au Titre I du présent Livre ; 2. à toutes les autres infractions pénales commises sur et au moyen d'un système informatique ; 3. à la collecte des preuves électroniques de toute infraction pénale. **Article 577** : Mode de preuve électronique L'écrit sous forme électronique, en application du Livre II, est, pour les besoins de l'application du présent Livre, admis en preuve au même titre que l'écrit sur support papier et possède la même force probante que celui-ci, sous réserve que puisse être dûment identifié la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité et la pérennité.
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are	**CdN**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	**Article 493** : Garantie des droits fondamentaux et des libertés La mise en œuvre et l'application des pouvoirs et procédures prévus au présent Titre sont soumises aux conditions et sauvegardes prévues par le droit interne de la République du Bénin, 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 du Pacte international relatif aux droits civils et politiques des Nations-Unies et de la Charte africaine des droits de l'homme et des peuples ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.	**Article 495** : Obligation de conservation de données Les fournisseurs de services en ligne détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont ils sont prestataires. Ils fournissent aux personnes qui éditent un service de communication au public en ligne des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues à l'article 501. Les magistrats et les fonctionnaires chargés de la mise en œuvre de l'exercice de l'action publique, les autorités administratives mentionnées à l'article 595 du présent code pourraient requérir auprès des fournisseurs de services en ligne, conformément à la loi, la conservation et la protection de l'intégrité ainsi que la communication des données mentionnées au premier alinéa. Les dispositions prévues au Livre V du présent code sont applicables au traitement de ces données. **Article 591** : Injonction de conserver et de protéger l'intégrité des données informatiques Il est inséré dans le code de procédure pénale, un article 78 bis rédigé comme suit :

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	« En matière criminelle et en matière correctionnelle, lorsque les nécessités de l'information l'exigent, l'officier de police judiciaire ou le juge d'instruction peut, par le biais d'une notification écrite et : • lorsqu'il y a des raisons de croire que les données informatiques stockées dans un système informatique sont particulièrement susceptibles de perte ou de modification ; et • que ces données informatiques sont utiles à la manifestation de la vérité, ordonner à une personne, fournisseur de services en ligne visé à l'article 495 du présent code ou opérateur ou fournisseur de services de communication au public en ligne visés à l'article 34 du présent code, de conserver et de protéger l'intégrité des données informatiques stockées spécifiées dans la notification et qui se trouvent en sa possession ou sous son contrôle, pendant une durée de quatre vingt dix (90) jours maximum afin de permettre aux autorités désignées dans la notification écrite d'obtenir la divulgation des données et pour la bonne démarche des investigations judiciaires. La durée exacte doit être indiquée dans la notification écrite et est renouvelable jusqu'à atteindre deux (02) ans maximum. Le gardien des données ou une autre personne chargée de conserver et de protéger ces mêmes données est tenu de garder le secret de la mise en œuvre des procédures prises dans le cadre de l'alinéa 1er. Toute violation du secret est punie par les dispositions prévues par le code pénal relatives au secret professionnel. L'alinéa 2 ne s'appliquera pas lorsque l'obligation au secret a été levée par l'officier de police judiciaire ou le juge d'instruction, auteur de la notification écrite ».
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.	**CdN** **Article 592** : Conservation et divulgation rapide de données relatives au trafic Il est inséré dans le code de procédure pénale, un article 78 ter rédigé comme suit : « En matière criminelle et en matière correctionnelle, lorsque les nécessités de l'information l'exigent, un officier de police judiciaire ou un juge d'instruction peut, lorsqu'il y a des raisons de croire que les données stockées dans un système informatique sont particulièrement susceptibles de perte ou de modification et que ces données sont utiles à la manifestation de la vérité, par le biais d'une notification écrite, exiger d'une personne contrôlant le système informatique, fournisseur de services en ligne visé à l'article 495 du présent code ou opérateur

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	ou fournisseur de services de communication au public en ligne visés à l'article 34 du présent code, qu'elle divulgue ou conserve suffisamment de données de trafic associées à une communication électronique spécifique, afin d'identifier : • le ou les fournisseurs de services ; et/ou • la voie par laquelle la communication en question a été transmise. Si la notification écrite requiert la conservation rapide, les principes de délais de l'article 35 de la présente loi s'appliquent. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie par les dispositions prévues par le code pénal relatives au secret professionnel. L'alinéa 3 ne s'applique pas lorsque l'obligation au secret a été levée par l'officier de police judiciaire ou le juge d'instruction, auteur de la notification écrite ».
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;	**CdN** **Article 586** : Injonction de produire Il est inséré dans le code de procédure pénale, un article 54 bis rédigé comme suit : « Le procureur de la République, son substitut ou le juge d'instruction peut ordonner, par le biais d'une injonction de produire, à toute personne, tout établissement ou organisme privé ou public ou toute administration publique présentes sur le territoire de la République du Bénin ou fournissant des prestations de service en République du Bénin, susceptibles de détenir des documents intéressant l'enquête criminelle y compris ceux issus d'un système informatique ou un support de stockage informatique, de lui remettre ces documents, notamment sous forme numérique ou sous une version imprimée, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel. Lorsque les réquisitions concernent des personnes mentionnées à l'article 102, la remise des documents ne peut intervenir qu'avec leur accord. Le procureur de la République, son substitut ou le juge d'instruction peut ordonner, par le biais d'une injonction de produire, à un fournisseur de services présent sur le territoire de la République du Bénin offrant des prestations sur le territoire de la République du Bénin, de communiquer les données informatiques en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	Le procureur de la République, son substitut ou le juge d'instruction peut ordonner, par le biais d'une injonction de produire, à une personne présente sur le territoire de la République du Bénin ayant accès à un système informatique particulier et qui traite des données informatiques spécifiques provenant de ce système de les donner à une personne spécifique. A l'exception des personnes mentionnées à l'article 102, le fait de s'abstenir de répondre dans les meilleurs délais à cette réquisition est puni d'une amende maximale de dix millions (10 000 000) de francs CFA. »
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied	**CdN** **Article 587** : Données stockées dans un système informatique Lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données informatisées sur le territoire béninois, sont utiles à la manifestation de la vérité, le juge d'instruction peut opérer une perquisition ou accéder à un système informatique ou à une partie de celui-ci ou dans un autre système informatique ou un support et aux données présentes dans ces derniers dès lors que ces données sont accessibles à partir du système initial ou disponible pour le système initial. S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponible pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par le juge d'instruction, par voie de commission rogatoire internationale. **Article 588** : Requête Les officiers de police judiciaire peuvent, par tout moyen, requérir toute personne susceptible d'avoir connaissance des mesures appliquées pour protéger les données auxquelles il est permis d'accéder dans le cadre de la perquisition de leur remettre les informations permettant d'accéder aux données mentionnées. Le fait de s'abstenir de répondre dans les meilleurs délais à cette réquisition est puni d'une amende de deux cent mille (200 000) francs CFA. **Article 589** : Conditions de perquisition

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	Les perquisitions prévues à l'article 587 ne peuvent avoir lieu qu'avec le consentement exprès de la personne chez qui l'opération a lieu. Cependant, si l'enquête est relative à un crime ou un délit puni de plus de cinq (5) ans de peine d'emprisonnement ou si la recherche de biens le justifie, le juge d'instruction peut, sur autorisation écrite, décider que la perquisition et la saisie seront effectuées sans l'assentiment de la personne. **Article 590** : Copie des données Lorsque le juge d'instruction découvre dans un système informatique des données stockées qui sont utiles pour la manifestation de la vérité, mais que la saisie du support ne paraît pas souhaitable, ces données, de même que celles qui sont nécessaires pour les comprendre, sont copiées sur des supports de stockage informatique pouvant être saisis et placés sous scellés, elles peuvent être de plus rendues inaccessibles ou retirées du système informatique en question sous ordre du juge.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.	**CdN** **Article 593** : Collecte en temps réel des données relatives au trafic Il est inséré dans le code de procédure pénale, un article 108 bis rédigé comme suit : « En matière criminelle et en matière correctionnelle, lorsque les nécessités de l'information l'exigent, le juge d'instruction ou l'officier de police judiciaire commis par lui peut utiliser les moyens techniques appropriés pour collecter ou enregistrer en temps réel, sur le territoire de la République du Bénin, les données relatives au trafic de communications spécifiques, transmises au moyen d'un système informatique ou le juge d'instruction ou l'officier de police judiciaire commis par lui peut requérir tout agent qualifié d'un service, organisme placé sous l'autorité ou la tutelle du ministre chargé des communications électroniques ou tout agent qualifié d'un opérateur, en vue de procéder à l'installation d'un dispositif, dans le cadre de ses capacités techniques à collecter ou à enregistrer, transcrire en application de moyens techniques existant, ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer lesdites données informatisées.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie par les dispositions prévues par le code pénal relatives au secret professionnel. L'alinéa 2 ne s'appliquera pas lorsque l'obligation au secret a été levée par l'officier de police judiciaire ou le juge d'instruction, auteur de la notification écrite ou lorsque l'auteur ou le destinataire de la communication donne son consentement express ».
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**CdN** **Article 594** : Interception et accès aux données par les autorités judiciaires A l'article 108, alinéa 1 er du code de procédure pénale, sont apportées les modifications suivantes : « En matière criminelle et en matière correctionnelle, si la peine encourue est au moins égale à deux (02) ans d'emprisonnement, le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspondances conformément aux dispositions de l'article 12 du présent code, y compris des données relatives au contenu, émises par voie de communications électroniques. » A l'article 108, 5ème alinéa du code de procédure pénale, sont apportées les modifications suivantes : « Le juge d'instruction ou l'officier de police judiciaire commis par lui peut requérir tout agent qualifié d'un service, organisme placé sous l'autorité ou la tutelle du Ministre chargé des communications électroniques ou tout agent qualifié d'un opérateur, en vue de procéder à l'installation d'un dispositif d'interception. » A l'article 108 du code de procédure pénale, deux nouveaux alinéas sont ajoutés après l'alinéa 5 : « Un agent qualifié d'un service, organisme placé sous l'autorité ou la tutelle du Ministre chargé des communications électroniques ou tout agent qualifié d'un opérateur visé à l'alinéa précédent est tenu au secret. Toute violation du secret est punie par les dispositions prévues par le code pénal relatives au secret professionnel. »

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	**CdN** **Article 597** : Compétences Les juridictions béninoises sont compétentes lorsque : 1- l'infraction a été commise sur internet sur le territoire de la République du Bénin dès lors que le contenu illicite est accessible depuis la République du Bénin ; 2- la personne physique ou morale s'est rendue coupable sur le territoire de la République du Bénin, comme complice, d'un crime ou d'un délit commis à l'étranger si le crime ou le délit est puni à la fois par la loi béninoise et par la loi étrangère et s'il a été constaté par une décision définitive de la juridiction étrangère ; 3- les délits ont été commis par des Béninois hors du territoire de la République du Bénin si les faits sont punis par la législation du pays où ils ont été commis ; 4- tout délit puni d'emprisonnement, a été commis par un Béninois ou par un étranger hors du territoire de la République du Bénin lorsque la victime est de nationalité béninoise au moment de l'infraction.
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.	***L'extradition est régie par les articles 727 à 758 de la loi n°2012-15 du 18 mars 2013 portant code de procedure pénale en République du Bénin***

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	**CdN** **Article 613**: Coopération Pour les infractions relevant de sa competence définie au 1er alinéa de l'article 609, l'OCRC constitue, pour le République du Bénin, le point de contact central dans les échanges internationaux. Il contribute au niveau national à l'animation et à la coordination des travaux préparatoires nécessaires et participle aux activités des organs et enceintes internationaux. Sans prejudice de l'application des conventions internationals, il entretient les liaisons opérationnelles avec les services spécialisés des autres pays et avec les organismes internationaux en vue de rechercher toute information relative aux infractions ainsi qu'à l'identification et à la localisation de leurs auteurs.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.	

Back to the Table of Contents

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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice;	**CdN** **Article 613**: Coopération Pour les infractions relevant de sa competence définie au 1er alinéa de l'article 609, l'OCRC constitue, pour le République du Bénin, le point de contact central dans les échanges internationaux. Il contribute au niveau national à l'animation et à la coordination des travaux préparatoires nécessaires et participle aux activités des organs et enceintes internationaux.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	

Back to the Table of Contents