Adoption de politiques harmonisées pour le marché des TIC dans les pays ACP

Cybersécurité:

Projets de Lois Types de la Communauté Economique des Etats de l'Afrique Centrale (CEEAC) et projets de Directives de la Communauté Economique et Monétaire de l'Afrique Centrale (CEMAC)

HIPSSA

Harmonisation des politiques en matière de TIC en Afrique Subsaharienne

Adoption de politiques harmonisées pour le marché des TIC dans les pays ACP

Cybersécurité :

Projets de Lois Types de la Communauté Economique des Etats de l'Afrique Centrale (CEEAC) et Projets de Directives de la Communauté Economique et Monétaire de l'Afrique Centrale (CEMAC)

HIPSSA

Harmonisation des politiques en matière de TIC en Afrique subsaharienne

Avis de non-responsabilité

Le présent document a été réalisé avec l'aide financière de l'Union européenne. Les opinions exprimées dans les présentes ne reflètent pas nécessairement la position de l'Union européenne.

Les appellations utilisées et la présentation de matériaux, notamment des cartes, n'impliquent en aucun cas l'expression d'une quelconque opinion de la part de l'UIT concernant le statut juridique d'un pays, d'un territoire, d'une ville ou d'une région donnés, ou concernant les délimitations de ses frontières ou de ses limites. La mention de sociétés spécifiques ou de certains produits n'implique pas qu'ils sont agréés ou recommandés par l'UIT de préférence à d'autres non mentionnés d'une nature similaire.

Avant d'imprimer ce rapport, pensez à l'environnement.

Avant-Propos

Les technologies de l'information et de la communication (TIC) sont à la base du processus de mondialisation. Conscients qu'elles permettent d'accélérer l'intégration économique de l'Afrique et donc, d'en renforcer la prospérité et la capacité de transformation sociale, les ministres responsables des communications et des technologies de l'information, réunis sous les auspices de l'Union africaine, ont adopté, en mai 2008, un cadre de référence pour l'harmonisation des politiques et réglementations des télécommunications/TIC, dont la mise en place se faisait d'autant plus nécessaire que les Etats étaient de plus en plus nombreux à adopter des politiques pour libéraliser ce secteur.

La coordination dans l'ensemble de la région est essentielle si l'on veut que les politiques, la législation et les pratiques résultant de la libéralisation dans chaque pays ne freinent pas, par leur diversité, le développement de marchés régionaux compétitifs.

Notre projet d'"Appui à l'harmonisation des politiques en matière de TIC en Afrique subsaharienne (HIPSSA)" cherche à remédier à ce problème potentiel en en regroupant et accompagnant tous les pays de la région au sein du Groupe des Etats d'Afrique, des Caraïbes et du Pacifique (ACP). Ces pays formulent et adoptent des politiques, des législations et des cadres réglementaires harmonisés dans le domaine des TIC. Exécuté par l'Union internationale des télécommunications (UIT) sous la coprésidence de l'Union africaine, ce projet est entrepris en étroite collaboration avec les communautés économiques régionales (CER) et les associations régionales de régulateurs qui sont membres de son comité directeur. Un comité de pilotage global constitué de représentants du Secrétariat ACP et de la Direction générale du développement et de la coopération – EuropeAid (DEVCO, Commission européenne) supervise la mise en oeuvre du projet dans son ensemble.

Inscrit dans le cadre du programme ACP sur les technologies de l'information et de la communication (@CP-ICT), le projet est financé par le 9ème Fonds européen de développement (FED), principal vecteur de l'aide européenne à la coopération au service du développement dans les Etats ACP, et cofinancé par l'UIT. La finalité du programme @CT-ICT est d'aider les gouvernements et les institutions ACP à harmoniser leurs politiques dans le domaine des TIC, grâce à des conseils, des formations et des activités connexes de renforcement des capacités, fondés sur des critères mondiaux tout en étant adaptés aux réalités locales.

Pour tous les projets rassembleurs impliquant de multiples parties prenantes, l'objectif est double: créer un sentiment partagé d'appartenance et assurer des résultats optimaux pour toutes les parties. Une attention particulière est prêtée à ce problème, depuis les débuts du projet HIPSSA en décembre 2008. Une fois les priorités communes arrêtées, des groupes de travail réunissant des parties prenantes ont été créés pour agir concrètement. Les besoins propres aux régions ont ensuite été définis, de même que les pratiques régionales pouvant donner de bons résultats, qui ont été comparées aux pratiques et normes établies dans d'autres régions du monde.

Ces évaluations détaillées, qui tiennent compte des spécificités de la sous-région et de chaque pays, ont servi de point de départ à l'élaboration de modèles de politiques et de textes législatifs constituant un cadre législatif dont l'ensemble de la région peut être fier. Il ne fait aucun doute que ce projet servira d'exemple pour les parties prenantes qui cherchent à mettre le rôle de catalyseur joué par les TIC au service de l'accélération de l'intégration économique et du développement socio-économique.

Avant-propos

Je saisis cette occasion pour remercier la Commission européenne et le Secrétariat ACP pour leur soutien financier. Je remercie également la Communauté économique des Etats de l'Afrique de l'Ouest (CEDEAO), l'Union économique et monétaire ouest-africaine (UEMOA), la Communauté économique des Etats de l'Afrique centrale (CEEAC), la Communauté économique et monétaire de l'Afrique centrale (CEMAC), la Communauté d'Afrique de l'Est (CAE), le Marché commun de l'Afrique orientale et australe (COMESA), la Communauté de développement de l'Afrique australe (SADC), l'Autorité intergouvernementale pour le développement (IGAD) l'Association des régulateurs des communications de l'Afrique australe (CRASA), l'Association des régulateurs de télécommunications d'Afrique centrale (ARTAC), la Commission économique des Nations Unies pour l'Afrique (CEA) et l'Assemblée des régulateurs des télécommunications de l'Afrique de l'Ouest (ARTAO) d'avoir contribué à la réalisation du projet. Sans la volonté politique des pays bénéficiaires, les résultats auraient été bien maigres. Aussi, je tiens à exprimer ma profonde gratitude à tous les gouvernements des pays ACP pour leur détermination, qui a assuré le grand succès de ce projet.

Brahima Sanou
Directeur du BDT

Remerciements

Le présent document représente l'aboutissement d'une activité régionale réalisée dans le cadre du projet HIPSSA (« Appui à l'harmonisation des politiques en matière de TIC en Afrique subsaharienne ») officiellement lancée à Addis Abeba en décembre 2008.

En réponse à la fois aux défis et aux possibilités qu'offrent les technologies de l'information et de la communication (TIC) en termes de développement politique, social, économique et environnemental, l'Union internationale des télécommunications (UIT) et la Commission européenne (CE) ont uni leurs forces et signé un accord (projet UIT-CE) destiné à fournir un "Appui pour l'établissement de politiques harmonisées sur le marché des TIC dans les pays ACP", dans le cadre du Programme "ACP-Technologies de l'information et de la communication" (@CP-TIC) financé par le 9ème Fonds européen de développement (FED). Il s'agit du projet UIT-CE-ACP.

Ce projet global UIT-CE-ACP est mené à bien dans le cadre de trois sous-projets distincts adaptés aux besoins spécifiques de chaque région: l'Afrique subsaharienne (HIPSSA), les Caraïbes (HIPCAR) et les Etats insulaires du Pacifique (ICB4PAC).

En leur qualité de membres du Comité de pilotage du projet HIPSSA, coprésidé par la Commission de l'Union africaine (CUA) et l'UIT, le Secrétariat général de la Communauté Economique des Etats l'Afrique Centrale (CEEAC), la Commission de la Communauté Economique et Monétaire de l'Afrique Centrale (CEMAC) et le secrétariat permanent de l'Assemblée des régulateurs de l'Afrique centrale (ARTAC) ont activement participé au développement des projets de lois types de la CEEAC et des projets de Directives de la CEMAC et apporté leur soutien aux consultants du projet. [

Pour cette activité particulière du projet HIPSSA, l'UIT a bénéficié de l'appui technique et financier de la Communauté Economique des Nations Unies pour l'Afrique (CEA). La mise en œuvre conjointe de cette activité s'inscrit dans une collaboration continue en matière de coopération au développement.

L'UIT tient à remercier les délégués des ministères en charge des questions de cybersécurité et des Autorités/Agences de régulation des Etats membres de la CEEAC, du milieu universitaire, de la société civile, des opérateurs de télécommunications/TIC et des organisations régionales et internationales pour leur travail remarquable et l'engagement dont ils ont fait preuve pour le développement et la validation des projets de lois types de la CEEAC. Nous exprimons en outre notre profonde reconnaissance au Secrétariat général de la CEEAC et à la Commission de la CEMAC pour leur remarquable contribution.

Sans la participation active de tous ces intervenants, il aurait été impossible de produire des projets de lois types et de directives reflétant l'ensemble des exigences et conditions générales de la CEEAC/CEMAC tout en intégrant les bonnes pratiques internationales.

Remerciements

Les activités ont été mises en œuvre par Mme Ida Jallow, chargée de la coordination des activités en Afrique subsaharienne (Coordonnatrice principale du projet HIPSSA), et M. Sandro Bazzanella, chargé de la gestion de l'ensemble du projet couvrant l'Afrique subsaharienne, les Caraïbes et le Pacifique (Directeur du projet UIT-CE-ACP), avec l'appui de Mme Hiwot Mulugeta, Assistante du projet HIPSSA, et de Mme Silvia Villar, Assistante du projet UIT-CE-ACP. Le travail a été réalisé sous la direction générale de M. Cosmas Zavazava, Chef du Département de l'appui aux projets et de la gestion des connaissances (PKM). Le document a été établi sous la supervision directe de M. Jean-François Le Bihan, qui était alors Coordonnateur principal du projet, et ses auteurs ont bénéficié des commentaires de la Division de l'environnement réglementaire et commercial (RME) et de la Division des initiatives spéciales (SIS) du Bureau de développement des télécommunications (BDT) de l'UIT. Ils ont aussi bénéficié de l'appui de Ms. Marcelino Tayob et Emmanuel Kamdem, respectivement Conseiller principal et Coordinateur des programmes au Bureau régional de l'UIT pour l'Afrique. L'équipe du Service de composition des publications de l'UIT a été chargée de la publication.

Table des matières

Table des matières

Page

Table of contents

Partie 1 :
INTRODUCTION

Partie 1

De nos jours, il ne fait aucun doute que l'accès au haut débit doit être un droit pour le citoyen compte tenu de son importance vitale pour communiquer, accéder à une éducation, à une formation professionnelle et à des soins de santé de qualité, effectuer de chez soi et en toute sécurité des transactions commerciales et financières.
A cette fin, les Gouvernements des Etats membres de la CEEAC s'emploient depuis 2008, avec l'appui de leurs partenaires en tête desquels l'UIT et l'Union Européenne à travers le projet HIPSSA, à trouver des voies et de déployer des actions/moyens de renforcement de la confiance des citoyens aux TIC. En réalité, il s'agit pour eux de faire en sorte qu'à l'horizon 2015 des réponses juridiques, administratives et technologiques soient apportées aux problèmes de sécurité de l'information et de l'accès à celle-ci.

Les projets de Lois types de la CEEAC relatives respectivement à la protection des données à caractère personnel, aux transactions électroniques et à la lutte contre la cybercriminalité ont été développés, avec la participation active de toutes les parties prenantes, dans le cadre du projet HIPSSA. Ils prennent en compte les évolutions nationale et internationale et se fondent non seulement sur une évaluation critique des législations des Etats membres de la CEEAC/CEMAC et des conventions internationales en matière de cybersecurité, mais également sur des interventions et pratiques réglementaires en vigueur dans les Etats membres de la CEEAC, les bonnes pratiques internationales et les principes généraux suivants :

- La réglementation repose sur des objectifs politiques clairement définis ;
- les règlements, directives et cadre de référence communautaires ne portent pas atteinte à la possibilité dont dispose chaque Etat membre de la CEEAC d'adopter les mesures nécessaires pour garantir la protection de ses intérêts essentiels en matière de sécurité, assurer l'ordre public et la sécurité publique et permettre la recherche , la détection et la poursuite d'infractions pénales, y compris la mise en place par les Autorités réglementaires nationales d'obligations spécifiques applicables aux prestataires de services de communications électroniques ;

Ces projets de Lois types / Directives ont été discutés et validés avec un large consensus par les participants aux ateliers régionaux de validation, organisés en collaboration avec la Commission Economique des Nations Unies pour l'Afrique (CEA), le Gouvernement de la République Gabonaise, le Gouvernement de la République du Cameroun, le Secrétariat général de la CEEAC et la Commission de la CEMAC, qui se sont tenu, d'une part du 28 novembre 2011 au 2 décembre2011 à Libreville, au Gabon, et d'autre part du 16 au 18 juillet 2012 à Douala, au Cameroun.

Par ailleurs, l'Atelier de Douala a formulé, à l'attention du Secrétariat général de la CEEAC les recommandations portées en annexe.

Partie 2 :
PROJETS DE LOIS TYPES DE LA CEEAC
ET
PROJETS DE DIRECTIVES DE LA CEMAC

Partie 2

PROJET DE LOI-TYPE/DIRECTIVE RELATIF A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Préambule

La protection des données est considérée, par nombre d'institutions ou organisations internationales, fondamentale pour le développement de l'individu dans une société démocratique et à la construction de son bien-être. Elle est au service de l'Homme.

L'on doit également relever que cette protection s'étend également à la vie professionnelle de l'individu qui mérite également d'être protégé sur son lieu de travail.

Si cette protection est souvent liée à la protection de la vie privée, l'on doit relever qu'elle est beaucoup plus vaste que cela. En effet, plusieurs droits fondamentaux sont concernés. Pensons à la liberté d'expression, à la liberté d'association.

Par ailleurs, une telle protection permet également d'éviter les différences entre individus basées, entre autres, sur les croyances religieuses, les appartenances syndicales, le sexe, la race, la filiation et les données relatives à la santé.

Outre ces considérations basées sur les droits humains fondamentaux eux-mêmes, l'on doit constater une réelle explosion des technologies de la communication et de l'information pouvant porter atteinte à ce droit à la protection des données à caractère personnel. Ces technologies ne se limitent aux activités commerciales mais aussi publiques avec l'émergence du concept de gouvernement électronique.

Le développement de ces technologies implique la prolifération de bases de données informatiques servant d'endroit de stockage et de traitement de nombreuses données à caractère personnel. Ensuite, l'interconnexion de ces bases de données peut dévier vers une traçabilité de l'individu dans ses diverses activités qu'elles soient privées ou professionnelles.

Nous constatons dès lors que les technologies de la communication et de l'information prennent de plus en plus d'importance dans les prises de décision concernant des individus. Nombre de décisions reposent ainsi sur des informations contenues dans ces bases de données.

Il faut donc éviter de voir les avantages de l'utilisation des technologies de l'information et de la communication affaiblir la protection des données à caractère personnel.

Cela implique que les informations doivent être correctes mais aussi pertinentes par rapport à l'objectif déterminé et déclaré. Il faut mettre en œuvre le principe selon lequel on ne peut collecter et traiter que les données à caractère personnel nécessaires à cette finalité. Par ailleurs, le responsable de traitement (c'est-à-dire la personne qui va déterminer la finalité/but du traitement et les moyens qui vont être mis en œuvre) a, une obligation de mise à jour des données et une limitation dans la collecte et le traitement.

Par ailleurs, il doit veiller à ce que ces données ne soient pas divulguées sans autorisation de la personne concernée ou d'une disposition légale. Cela implique donc la mise en place de mesures organisationnelles et techniques assurant la sécurité du traitement impliquant, entre autres, la collecte et le stockage des données à caractère personnel.

Cette obligation de sécurité implique une responsabilisation du responsable (principe d'accountability) renforcée en fonction des données traitées. Il existe, en effet, des données qui sont moins sensibles que d'autres et qui demande une protection éventuellement moindre. A titre d'exemple, nous pouvons donner l'hypothèse d'un base de données ne contenant que des noms et prénoms. Cette base de données contient des données qui ne sont, normalement, pas sensibles et donc générant moins de risques et, en conséquence, d'une sécurité moins perfectionnée. Par contre, ce sera le contraire pour une base de données contenant des données à caractère personnel relative à la santé, à la race.

Nous constatons qu'il existe deux catégories de données qui peuvent être référencées. Il y a, d'une part, les données sensibles qui sont celles qui touchent l'individu dans ce qu'il a de plus précieux en termes de sphère privée et, d'autre part, les autres données. La première catégorie concerne des données à caractère personnel révélant, par exemple, l'appartenance religieuse, les origines ethniques, ou relatives à la santé. Cela peut également être les données génétiques qui ont cette particularité de concerner un grand nombre de personnes, à savoir celles d'une même fratrie.

Nous devons donc définir des règles particulières pour cette catégorie particulière de données dites sensibles.

Parallèlement à cela, il faut nécessairement donner à la personne concernée les moyens de contrôle sur le responsable via un droit d'accès duquel découlera, entre autres, un droit de rectification, d'opposition.

Par ailleurs, on est dans l'obligation de mettre en place un régime de sanction afin de rendre la loi pleinement efficace. En effet, l'on constate qu'une loi sans sanction fait l'objet d'une désobéissance qui la rend parfaitement inefficace.

De plus, il faut constater que les frontières deviennent de plus en plus perméables. Cela implique donc que les données à caractère personnel les traverseront dans le cadre de traitements transfrontaliers qui deviennent de plus en plus fréquents. Les pays doivent déterminer les règles qui régiront ces transferts afin qu'ils s'effectuent dans des conditions garantissant la protection des données à caractère personnel.

Ces règles seront d'autant plus faciles à déterminer qu'un grand nombre de pays adoptent des règles de protection équivalentes. Cela mène donc à des textes adoptés sur une échelle régionale. Il est, en effet, important, que plusieurs pays adoptent ensemble des règles communes afin d'assurer une protection efficace du droit à la protection des données à caractère personnel. L'objectif du projet de loi-type est de créer un régime uniforme dans une région donnée afin de pouvoir créer un contexte sécurisant pour les citoyens.

Cette mise en place d'un régime uniforme de règles implique une coopération entre pays qu'il faut promouvoir afin de garantir une continuité dans l'uniformisation. Cette coopération peut s'opérer à travers la collaboration des autorités de protection des données à caractère personnel ad hoc via un groupe de travail international.

Par ailleurs, le régime de protection des données à caractère personnel doit nécessairement se fonder sur les cultures sociales, religieuses et politiques régionales pour atteindre son objectif de protection et d'harmonisation. Les outils existants tels que le projet de convention de l'Union africaine sur la mise en place d'un cadre juridique de confiance pour la cybersecurité en Afrique (Union africaine), les textes de la CEEAC/CEMAC, les textes nationaux existant y compris les dispositions constitutionnelles.

La mise en place d'un régime de protection des données à caractère personnel ne sera effective qu'avec la création d'une Autorité de contrôle qui devra assurer cette fonction de contrôle du bon respect de la législation et de la protection de la vie privée en général.

Cette autorité doit également être dotée de pouvoir réglementaire afin de pouvoir, par exemple, préciser certains principes énoncés par la loi-type.

La protection des données à caractère personnel implique la mise en place d'un régime spécifique et adapté aux particularismes de chaque région.

Chapitre 1. Définitions

Article 1.

1. Autorité de contrôle

Autorité administrative indépendante chargée du respect, sur le territoire national, des dispositions de la présente loi-type.

2. Catégories particulières de données:

Données génétiques, données liées à des mineurs, données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté, données biométriques ainsi que, pour autant qu'elles soient traitées pour ce qu'elles révèlent ou contiennent, les données à caractère personnel qui révèlent l'origine raciale ou ethnique, la filiation, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, le sexe ainsi que le traitement des données relatives à la santé et à la vie sexuelle.

3. Catégories non particulières de données:

Données qui ne peuvent pas être qualifiées de sensibles.

4. Code de conduite:

Vise les chartes d'utilisation élaborées par le responsable du traitement afin d'instaurer un usage correct des ressources informatiques, de l'Internet et des communications électroniques de la structure concernée et homologué par l'Autorité de contrôle.

5. Consentement:

Toute manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire ou conventionnel accepte que ses données à caractère personnel fassent l'objet d'un traitement.

6. Destinataire:

La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données, qu'il s'agisse ou non d'un tiers; les autorités qui sont susceptibles de recevoir communication de données dans le cadre d'une mission d'enquête particulière ne sont toutefois pas considérées comme des destinataires;

7. Données à caractère personnel:

Toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique.

8. Données génétiques:

Il s'agit de toute information découlant d'une analyse de l'ADN.

9. Fichier:

Tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

10. Flux transfrontières

Flux internationaux de données à caractère personnel par l'intermédiaire de la transmission électronique ou tous autres moyens de transmission. Ne sont donc pas visés les flux de données à caractère personnel propres aux États fédéraux.

Au sens de la présente loi-type, les flux transfrontières englobent la transmission des données par satellite.

11. Mineur:

Toute personne physique qui n'a pas le statut de majeur ou similaire en vertu de sa loi nationale.

12. Personne concernée:

Toute personne physique qui fait l'objet d'un traitement des données à caractère personnel et qui est identifié ou identifiable.

Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne.

13. Professionnel des soins de santé:

Toute personne définie comme telle par la législation nationale.

14. Représentant du responsable de traitement

Toute personne physique ou morale établit de manière stable sur le territoire du [pays concerné], qui se substitue au responsable de traitement dans l'accomplissement des obligations prévues par la présente loi-type.

15. Responsable de traitement:

La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national;

16. Sous-traitant:

La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement et sous ses instructions;

17. Système d'alerte professionnelle (whisteblowing)

Disposition permettant à des individus de signaler un comportement d'un membre de leur organisation contraire, selon eux, à une législation ou à une réglementation ou aux règles primordiales établies par leur organisation.

18. Tiers:

La personne physique ou morale, l'autorité publique, le service ou tout autre organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données;

19.Traitement:

Toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés entièrement ou partiellement automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Chapitre 2. Champ d'application matériel

Article 2.

1. La présente loi-type s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

2. La présente loi-type ne s'applique pas au traitement de données à caractère personnel effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques.

3. La présente loi-type ne peut limiter:

a. des modes de production d'informations disponibles en vertu d'une loi pour une partie dans quelque procédure judiciaire qu'il soit;

b. le pouvoir des Cours et tribunaux judiciaires de contraindre un témoin de témoigner ou de contraindre la production de preuves.

Chapitre 3. Champ d'application territorial

Article 3.

1. La présente loi-type est applicable aux traitements de données à caractère personnel lorsque:

a. le responsable est établi sur le territoire [pays]. Le responsable d'un traitement qui exerce une activité sur le territoire [pays] dans le cadre d'une installation, quelle que soit sa forme juridique, y est considéré comme établi ;

b. le responsable, sans être établi sur le territoire [pays], recourt à des moyens de traitement situés sur le territoire [pays], à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire.

2. Pour les traitements mentionnés au paragraphe 1 alinéa b du présent article, le responsable désigne à l'Autorité de contrôle un représentant; cette désignation ne fait pas obstacle aux actions qui pourraient être introduites contre lui.

Chapitre 4. Principes auxquels le traitement doit répondre;

Section 1. Qualité des données

Article 4.

1. Les données à caractère personnel:

a. doivent être collectées pour des finalités déterminées, explicites et légitimes et ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités. Est considéré comme compatible la finalité qui répond aux attentes raisonnables de la personne concernée ou lorsqu'elle est prévue par une loi.

Le bon usage de la notion d'attente raisonnable sera contrôlé par l'autorité de contrôle visée au chapitre 7 dans le cadre de son droit de contrôle visé à l'Article 32.1 alinéa b de la présente loi-type.

b. doivent être traitées loyalement, licitement et de manière non frauduleuse;

c. doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement.

d. doivent être exactes et, si nécessaire, mises à jour;

e. ne peuvent pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui excède la période nécessaire aux finalités pour lesquelles elles ont été collectées ou traitées.

L'Autorité de contrôle prévoit, par voie d'arrêté ou acte équivalent, des garanties appropriées pour les données à caractère personnel qui sont conservées au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques..

2. Le responsable du traitement est tenu de prendre toute mesure utile pour assurer que les données à caractère personnel traitées pourront être exploitées quel que soit le support technique utilisé.

Il doit particulièrement s'assurer que l'évolution de la technologie ne sera pas un obstacle à cette exploitation.

3. Le responsable de traitement s'assure du respect des règles prévues aux paragraphes 1 et 2 par toute personne travaillant sous son autorité ou tout sous-traitant.

Section 2. Légitimité

Sous-section 1. Traitement portant sur des catégories non particulières de données

Article 5.

1. Le traitement de données à caractère personnel non sensibles est, sans le consentement indubitable de la personne concernée, autorisé s'il est nécessaire:

a. à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à sa demande

ou

b. au respect d'une obligation légale à laquelle le responsable du traitement est soumis

ou

c. à la sauvegarde de l'intérêt vital de la personne concernée

ou

d. à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées

ou

e. à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui peut prétendre à une protection au titre de la présente loi-type.

2. Le responsable de traitement s'assure que, à tout instant du traitement, ledit traitement est légitime tant dans son chef que dans celui de son sous-traitant.

3. L'Autorité de contrôle peut, par voie d'arrêté ou acte équivalent, préciser les cas où la condition mentionnée sous e) est considérée ne pas être remplie.

Sous-section 2. Des catégories particulières de données

Article 6.

1. Le traitement de données biométriques et de données à caractère personnel qui, si elles sont traitées pour ce qu'elles révèlent ou contiennent, révèlent l'origine raciale ou ethnique, la filiation, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, le sexe ainsi que le traitement des données relatives à la vie sexuelle est interdit sauf si:

a. la personne concernée a donné son consentement explicite écrit, que ce soit sur un support papier, support électronique ou tout autre support équivalent, à un tel traitement sauf dans le cas où la loi prévoit que l'interdiction visée à l'alinéa 1er ne peut être levée par le consentement écrit de la personne concernée.

Le consentement peut être retiré à tout moment sans frais par la personne concernée.

ou

b. le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail;

ou

c. le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ou n'est pas représentée.

ou

d. le traitement est effectué par des associations dotées de la personnalité juridique ou par des établissements d'utilité publique qui ont pour objet social principal la défense et la promotion des droits de l'homme et des libertés fondamentales, en vue de la réalisation de cet objet, à condition que ce traitement soit autorisé par l'Autorité de contrôle, par voie d'arrêté ou acte équivalent et que les données ne soient pas communiquées à des tiers sans le consentement écrit des personnes concernées, que ce soit sur un support papier, support électronique ou tout autre support équivalent.

ou

e. lorsque le traitement est nécessaire à la réalisation d'une finalité fixée par ou en vertu de la loi, en vue de l'application de la sécurité sociale;

ou

f. le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou dans une procédure judiciaire ou une enquête pénale est ouverte moyennant des garanties appropriées;

ou

g. le traitement porte sur des données manifestement rendues publiques par la personne concernée ;

ou

h. le traitement est nécessaire à des recherches à des fins historiques, statistiques ou scientifiques.

L'Autorité de contrôle déterminera, par voie d'arrêté ou acte équivalent, les conditions régissant de tels traitements.

ou

i. lorsque le traitement est effectué en exécution de lois relatives à la statistique publique;

ou

j. lorsque le traitement est nécessaire aux fins de médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements soit à la personne concernée, soit à un parent, ou de la gestion de services de santé agissant dans l'intérêt de la personne concernée et le traitement est effectué sous la surveillance d'un professionnel des soins de santé;

ou

k. lorsque le traitement des données à caractère personnel visé au premier alinéa est permis par une loi pour un autre motif important d'intérêt public.

2. Le traitement des données à caractère visés au présent article ne peut, sauf dans le cas d'un consentement écrit de la personne concernée ou lorsque le traitement est nécessaire pour la prévention d'un danger concret ou la répression d'une infraction pénale déterminée, uniquement être effectué sous la responsabilité d'un professionnel des soins de santé.

3. Lors d'un traitement de données à caractère personnel visé au présent article, le professionnel des soins de santé et ses préposés ou mandataires sont au secret.

Article 7.

1. Le traitement de données génétiques ou de données à caractère personnel qui, si elles sont traitées pour ce qu'elles révèlent ou contiennent, sont relatives à la santé est interdit sauf si:

a. la personne concernée a donné son consentement explicite écrit, que ce soit sur un support papier, support électronique ou tout autre support équivalent, à un tel traitement sauf dans le cas où la loi prévoit que l'interdiction visée à l'alinéa 1er ne peut être levée par le consentement écrit de la personne concernée.

Ce consentement peut être retiré à tout moment sans frais et sans motivation à moins que cela ne porte atteinte à la personne concernée ou, de manière disproportionnée, aux intérêts du responsable de traitement

ou

b. le traitement est nécessaire afin d'exécuter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail;

ou

c. le traitement est nécessaire à la réalisation d'une finalité fixée par ou en vertu de la loi, en vue de l'application de la sécurité sociale;

ou

d. le traitement est nécessaire à la promotion et à la protection de la santé publique y compris le dépistage;

ou

e. le traitement est rendu obligatoire par ou en vertu d'une loi ou tout acte législatif équivalent pour des motifs d'intérêt public importants;

ou

f. le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement et n'est pas représentée;

ou

g. le traitement est nécessaire pour la prévention d'un danger concret ou la répression d'une infraction pénale déterminée;

ou

h. le traitement porte sur des données manifestement rendues publiques par la personne concernée;

ou

i. le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice;

ou

j. le traitement est nécessaire à des recherches à des fins historiques, statistiques ou scientifiques.

L'Autorité de contrôle déterminera, par voie d'arrêté ou acte équivalent, les conditions régissant de tels traitements.

ou

k. lorsque le traitement est nécessaire aux fins de médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements soit à la personne concernée, soit à un parent [à déterminer par l'Etat adoptant], ou de la gestion de services de santé agissant dans l'intérêt de la personne concernée et les données sont traitées sous la surveillance d'un professionnel des soins de santé;

2. Le traitement des données à caractère personnel visées par le présent article ne peut, sauf dans le cas d'un consentement écrit de la personne concernée ou lorsque le traitement est nécessaire pour la prévention d'un danger concret ou la répression d'une infraction pénale déterminée, uniquement être effectué sous la responsabilité d'un professionnel des soins de santé.

3. Lors d'un traitement de données à caractère personnel visé au présent article, le professionnel des soins de santé et ses préposés ou mandataires sont soumis au secret.

Article 8.

Dans le cadre des articles 6 littera j et 7 littera d et k, le traitement de données génétiques et de données à caractère personnel qui, si elles sont traitées pour ce qu'elles révèlent ou contiennent, sont relatives à la santé ne peuvent être traitées que moyennant l'octroi à la personne concernée d'un identifiant patient unique différent de tout autre numéro d'identification par l'autorité publique désignée par la loi pour ce faire.

L'interconnexion de ce numéro avec tout autre numéro identifiant ou permettant d'identifier la personne concernée, au sens de l'Article 1.12 de la présente loi type, ne pourra être possible que moyennant autorisation de l'Autorité de contrôle visée au chapitre 7.

Article 9.

1. Le traitement de données à caractère personnel relatives à des litiges soumis aux cours et tribunaux ainsi qu'aux juridictions administratives, à des suspicions, des poursuites ou des condamnations ayant trait à des infractions, ou à des sanctions administratives ou des mesures de sûreté est interdit, sauf si le traitement est effectué:

a. sous le contrôle d'une autorité publique ou d'un officier ministériel au sens de la loi de l'Etat adoptant, lorsque le traitement est nécessaire à l'exercice de leurs tâches;

ou

b. par d'autres personnes lorsque le traitement est nécessaire à la réalisation de finalités fixées par ou en vertu d'une loi;

ou

c. par des personnes physiques ou par des personnes morales de droit public ou de droit privé pour autant que la gestion de leurs propres contentieux l'exige;

ou

d. par des avocats ou d'autres conseils juridiques, lorsque la défense de leurs clients l'exige;

2. Le traitement de données à caractère personnel relatives à des litiges soumis aux cours et tribunaux ainsi qu'aux juridictions administratives, à des suspicions, des poursuites ou des condamnations ayant trait à des infractions, ou à des sanctions administratives ou des mesures de sûreté est interdit, sauf si le traitement est nécessaire à des recherches à des fins historiques, statistiques ou scientifiques.

L'Autorité de contrôle déterminera, par voie d'arrêté ou acte équivalent pris, les conditions régissant de tels traitements.

3. Les personnes qui, en vertu du présent article, sont autorisées à traiter les données à caractère personnel, sont soumises au secret professionnel.

Article 10.

Les données à caractère personnel relatives aux mineurs ne pourront être traitées que dans le respect des règles de représentation et à l'association du mineurs à l'exercice de ses droits prévues à l'Article 26 de la présente loi-type.

Article 11.

L'Autorité de contrôle peut, par voie d'arrêté, prévoir des exceptions au présent chapitre, au chapitre 5 section 3 et au chapitre 6 lorsque le traitement est effectué par un avocat, ou toute personne assimilée en vertu du droit nationale, dans l'exercice de sa mission dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant l'exercice de sa mission.

L'alinéa 1 ne s'applique cependant pas à l'égard du client de l'avocat.

Chapitre 5. Les obligations du responsable de traitement et du sous-traitant

Section 1. Information

Article 12.

Lorsque les données à caractère personnel sont collectées auprès de la personne concernée, le responsable du traitement ou son représentant doit fournir à la personne concernée au moins les informations énumérées ci-dessous, sauf si la personne en est déjà informée:

a. l'identité du responsable du traitement et, le cas échéant, de son représentant;

b. les finalités du traitement auquel les données sont destinées;

c. toute information supplémentaire, dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées pour assurer un traitement loyal des données, si elle est nécessaire à l'égard de la personne concernée telles que:

- les destinataires ou les catégories de destinataires des données,

- le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse,

- l'existence de ses droits d'accès, de rectification, d'effacement et d'opposition aux données à caractère personnel la concernant.

Article 13.

1. Lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, le responsable du traitement ou son représentant doit, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard lors de la première communication de données, fournir à la personne concernée au moins les informations énumérées ci-dessous, sauf si la personne en est déjà informée:

a. l'identité du responsable du traitement et, le cas échéant, de son représentant;

b. les finalités du traitement;

c. dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, toute information supplémentaire, si elle est nécessaire pour assurer à l'égard de la personne concernée un traitement loyal des données, telles que:

- les catégories de données concernées,

- les destinataires ou les catégories de destinataires des données,

- l'existence de ses droits d'accès, de rectification, d'effacement et d'opposition aux données à caractère personnel la concernant,

2. Le paragraphe 1 ne s'applique pas lorsque, en particulier pour un traitement à finalité statistique ou de recherche historique ou scientifique, l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés ou si la législation prévoit expressément l'enregistrement ou la communication des données.

L'Autorité de contrôle déterminera, par voie d'arrêté ou acte équivalent, les conditions régissant de tels traitements.

Section 2. Confidentialité

Article 14.

Toute personne agissant sous l'autorité du responsable du traitement ou celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel ne peut les traiter que sur instruction du responsable du traitement, sauf en vertu d'obligations légales.

Section 3. Sécurité

Article 15.

1. Le responsable du traitement et son sous-traitant doivent mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, l'interception notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.

Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger.

2. Le responsable du traitement et son sous-traitant, lorsque le traitement est effectué pour son compte, doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer et qu'il doit veiller au respect de ces mesures.

3. La réalisation de traitements en sous-traitance doit être régie par un contrat ou un acte juridique qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que:

- le sous-traitant n'agit que sur la seule instruction du responsable du traitement,

- les obligations visées au paragraphe 1 incombent également à celui-ci.

4. Aux fins de la conservation des preuves, les éléments du contrat ou de l'acte juridique relatifs à la protection des données et les exigences portant sur les mesures visées au paragraphe 3 du présent article sont consignés par écrit ou sous une autre forme équivalente mais garantissant la pérennité et l'inaltérabilité du document.

Article 16.

1. Le responsable de traitement doit notifier, sans délai, à l'Autorité de contrôle et à la personne concernée toute rupture de la sécurité ayant affecté les données à caractère personnel de la personne concernée.

2. Les sous-traitant doit avertir, sans délai, le responsable de traitement de toute rupture de la sécurité ayant affecté les données à caractère personnel qu'il traite pour le compte et au nom du responsable de traitement.

Section 4. Notification du traitement à l'Autorité de contrôle

Sous-section 1. Obligation de notification

Article 17.

1. Le responsable du traitement, ou le cas échéant son représentant légal, doit adresser une notification à l'Autorité de contrôle préalablement à la mise en œuvre d'un traitement ou d'un ensemble de tels traitements ayant une même finalité ou des finalités liées.

Tout changement affectant les informations visées à l'Article 18 doit également être notifié à l'Autorité de contrôle.

2. Le paragraphe précédent ne s'applique pas aux traitements ayant pour seul objet la tenue d'un registre qui, par ou en vertu d'une loi ou d'un acte législatif équivalent, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime.

3. L'Autorité de contrôle peut, par voie d'arrêté ou tout acte équivalent, exempter certaines catégories de la déclaration visée au présent article lorsque:

a. compte tenu des données traitées, il n'y a manifestement pas de risque d'atteinte aux droits et libertés individuelles des personnes concernées et que sont précisées les finalités du traitement, les catégories de données traitées, les catégories de personnes concernées, les catégories de destinataires et la durée de conservation des données

b. lorsque le responsable du traitement désigne un délégué à la protection des données à caractère personnel pour garantir que les traitements ne soient pas susceptibles de porter atteinte aux droits et libertés des personnes concernées qui est chargé notamment:

– d'assurer, d'une manière indépendante, l'application interne des dispositions de la présente loi-type,

– de tenir un registre des traitements effectués par le responsable du traitement, contenant les informations visées à l'Article 18 de la présente loi-type.

L'Autorité de contrôle établit, par voie d'arrêté ou tout acte équivalent, des règles spécifiques établissant la fonction de délégué à la protection des données à caractère personnel.

4. Les traitements effectués par les autorités publiques ne peuvent faire l'objet d'aucune dérogation ou simplification prévue au paragraphe 2 du présent article.

5. Le bénéfice de la simplification ou de l'exonération de l'obligation de notification ne dispense pas le responsable du traitement de données à caractère personnel d'aucune des autres obligations découlant de la présente loi-type.

Sous-section 2. Contenu de la notification

Article 18.

1. La notification doit contenir, au moins, les informations suivantes:

a. le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant légal;

b. la ou les finalités du traitement;

c. les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement ;

d. une description de la ou des catégories de personnes concernées et des données ou des catégories de données s'y rapportant;

e. le ou les services chargés de mettre en œuvre le traitement ainsi que les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées ;

f. les interconnexions envisagées ou toutes autres formes de mise en relation avec d'autres traitements ;

g. la durée de conservation des données traitées ;

h. les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées;

i. l'indication du recours à un sous-traitant ;

j. les transferts de données envisagés à destination de pays tiers;

k. une description générale permettant d'apprécier de façon préliminaire le caractère approprié des mesures prises pour assurer la sécurité du traitement en application du chapitre 5, section 3 de la présente loi-type.

2. L'Autorité de contrôle peut, par voie d'arrêté ou acte équivalent, définir d'autres informations devant être contenues dans la notification.

Sous-section 3. Autorisations

Article 19.

1. L'Autorité de contrôle détermine les catégories de traitements qui présentent des risques particuliers au regard des droits et libertés fondamentaux des personnes concernées et qui requièrent une autorisation de l'Autorité de contrôle.

2. De telles autorisations sont accordées après réception de la notification du responsable du traitement ou par le détaché à la protection des données, qui, en cas de doute, doit consulter l'Autorité de contrôle.

Sous-section 4. Mise à la connaissance du public des traitements

Article 20.

1. L'Autorité de contrôle prend les mesures nécessaires pour porter à la connaissance du public les traitements qui lui ont été notifiés ou acceptés par elle.

Le registre contient au minimum les informations énumérées à l'Article 18.

Le registre peut être consulté par toute personne.

2. Afin de remplir l'obligation prévue au paragraphe 1, l'Autorité de contrôle tient un registre des traitements notifiés tel que cela est fixé par l'Article 32 alinéa k de la présente loi-type.

3. Dans le cas des traitements exonérés de notification en vertu de l'Article 17 paragraphe 2 de la présente loi-type, le responsable du traitement ou son représentant communique sous une forme appropriée à toute personne qui en fait la demande au moins les informations visées à l'Article 18 de la présente loi-type.

Ceci ne s'applique pas aux traitements ayant pour seul objet la tenue d'un registre qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime.

Section 5. Responsabilité assumée

Article 21.

Le responsable de traitement doit:

a. Prendre toutes les mesures nécessaires pour s'assurer du respect de la présente loi type tant par lui-même que par les personnes travaillant pour lui dans un lien de hiérarchie que par son sous-traitant.

et

b. Avoir des mécanismes internes pour pouvoir le prouver tant à l'autorité de contrôle visée au chapitre 7 de la présente loi-type qu'à la personne concernée.

Chapitre 6. Les droits de la personne concernée

Section 1. Droit d'accès

Article 22.

1. Toute personne concernée a le droit d'obtenir du responsable du traitement ou de son représentant, sans contrainte, à première demande et gratuitement:

a. la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées,

b. la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine des données,

c. la connaissance de ce qui sous-tend tout traitement automatisé des données la concernant;

2. Toute personne a le droit d'obtenir, soit directement, soit par l'intermédiaire d'un professionnel des soins de santé, la communication des données à caractère personnel relatives à sa santé et qui font l'objet d'un traitement.

A la demande du responsable du traitement ou de la personne concernée, la communication peut être effectuée par l'intermédiaire d'un professionnel des soins de santé choisi par la personne concernée.

3. Lorsque les données relatives à la santé de la personne concernée sont traitées aux fins de recherches médico-scientifiques, qu'il est manifeste qu'il n'existe aucun risque qu'il soit porté atteinte à la vie privée de cette personne et que les données ne sont pas utilisées pour prendre des mesures à l'égard d'une personne concernée individuelle, la communication peut, pour autant qu'elle soit susceptible de nuire gravement auxdites recherches, être différé au plus tard jusqu'à l'achèvement des recherches.

Dans ce cas, la personne concernée doit avoir préalablement donné son autorisation écrite au responsable du traitement que les données à caractère personnel la concernant peuvent être traitées à des fins médico-scientifiques et que la communication de ces données peut dès lors être différée.

4. La gratuité et l'accès prévus au présent article peut être refusée par le responsable de traitement, sous réserve des droits de recours ouverts au profit de la personne concernée par la présente loi-type, en cas d'abus de requêtes d'accès dans le chef de la personne concernée.

Section 2. Droit de rectification, d'effacement et de limitation temporaire d'accès

Article 23.

1. La personne concernée a le droit, selon le cas et gratuitement, de rectification, d'effacement des données à caractère personnel ou de limitation temporaire d'accès aux dites données dont le traitement n'est pas conforme à la présente loi type, notamment en raison du caractère incomplet ou inexact des données;

2. Le responsable de traitement a l'obligation de notification aux tiers auxquels les données ont été communiquées de toute rectification, tout effacement ou toute limitation temporaire d'accès aux dites données effectué conformément au paragraphe 1, si cela ne s'avère pas impossible ou ne suppose pas un effort disproportionné.

3. La gratuité prévue au paragraphe 1 du présent article peut être refusée par le responsable de traitement, sous réserve des droits de recours ouverts au profit de la personne concernée par la présente loi-type, en cas d'abus de requêtes d'accès dans le chef de la personne concernée.

Section 3. Droit d'opposition

Article 24.

1. La personne concernée a le droit:

a. de s'opposer à tout moment et gratuitement, pour des raisons prépondérantes et légitimes tenant à sa situation particulière telle que, par exemple, une procédure judiciaire en cours, à ce que des données la concernant fassent l'objet d'un traitement, sauf en cas de disposition contraire du droit national. En cas d'opposition justifiée, le traitement mis en œuvre par le responsable du traitement ne peut plus porter sur ces données à caractère personnel;

b. de s'opposer, sur demande et gratuitement, au traitement des données à caractère personnel la concernant envisagé par le responsable du traitement à des fins de prospection commerciale ou assimilée;

ou

c. d'être informée gratuitement avant que des données à caractère personnel ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection et de se voir expressément offrir le droit de s'opposer, gratuitement, à ladite communication ou utilisation.

2. La gratuité prévue au présent article peut être refusée par le responsable de traitement, sous réserve des droits de recours ouverts au profit de la personne concernée par la présente loi-type, en cas d'abus de requêtes d'accès dans le chef de la personne concernée.

Section 4. Délais

Article 25.

Le responsable de traitement doit donner suite à la requête de la personne concernée dans un délai qui n'excède pas (…) jours sous peine d'une plainte déposée auprès de l'autorité de contrôle visée au chapitre 7 de la présente loi type.

Section 5. Représentation de la personne concernée

Article 26.

1. Si la personne concernée est mineure, les droits fixés par la présente loi sont exercés par les parents exerçant l'autorité sur le mineur ou par son tuteur.

2. Suivant son âge et sa maturité, le mineur doit être associé à l'exercice de ses droits.

Article 27.

1. En cas d'incapacité physique ou mentale dûment attestée par un professionnel de la santé, les droits, tels que fixés par la présente loi type, d'une personne concernée majeure, sont exercés par l'époux cohabitant, le partenaire cohabitant légal ou le partenaire cohabitant de fait.

Si cette personne ne souhaite pas intervenir ou si elle fait défaut, les droits sont exercés, en ordre subséquent, par un enfant majeur, un parent, un frère ou une sœur majeur de la personne concernée.

Si une telle personne ne souhaite pas intervenir ou si elle fait défaut, c'est un tuteur ad hoc désigné par [le Tribunal compétent] qui veille aux intérêts de la personne concernée.

Cela vaut également en cas de conflit entre deux ou plusieurs des personnes mentionnées dans le présent paragraphe.

2. La personne concernée est associée à l'exercice de ses droits autant qu'il est possible et compte tenu de sa capacité de compréhension.

Chapitre 7. L'Autorité de contrôle

Section 1. Constitution

Article 28.

Il est institué une autorité administrative indépendante appelée l'Autorité de contrôle chargée du respect, sur le territoire national, des dispositions de la présente loi type ainsi que la protection à la vie privée en général.

Article 29

1. L'Autorité de contrôle est composée de magistrats désignés par leurs pairs, de représentant désigné par le [Chef de l'Etat ou du Gouvernement], de députés désignés par leurs pairs, de personnes désignées par les associations nationales dans le domaine des droits fondamentaux de l'homme, de personnes désignées par les associations nationales de professionnels de technologies de l'information et de la communication. Ce sont les membres effectifs.

Par ailleurs, l'Autorité de contrôle est également composée de membres suppléants avec la même répartition que celle prévue au premier alinéa

Tous doivent avoir des compétences en matière de protection des données à caractère personnel ou de protection de la vie privée et de nouvelles technologies.

2. Pour être nommés et rester membre, effectif ou suppléant, de l'Autorité de contrôle, les candidats doivent remplir les conditions suivantes :

a. être [nationalité du pays adoptant];

b. jouir de leurs droits civils et politiques;

c. ne pas être membre d'un organe de la CEMAC ou de la CEEAC ou des Chambres législatives hormis, pour ces dernières, des membres de l'Autorité de contrôle qu'elles nomment pour être effectif ou suppléant en vertu du présent article.

d. [L'Etat adoptant devra prévoir des règles d'incompatibilité entre la fonction de membre de l'Autorité de contrôle et d'autres fonctions ainsi que des règles spécifiques pour éviter tout conflit d'intérêts survenant avant ou en cours d'exercice du mandat de membre de l'Autorité de contrôle]

2. Il est interdit aux membres de l'Autorité de contrôle d'être présents lors de la délibération sur les objets pour lesquels ils ont un intérêt personnel ou pour lesquels leurs parents ou alliés jusqu'au quatrième degré ont un intérêt personnel.

3. Les membres de l'Autorité de contrôle sont soumis au secret professionnel en vertu des règles légales.

4. Les membres de l'Autorité de contrôle sont nommés pour un terme de (…) ans renouvelable (…) fois.

Ils peuvent être relevés de leur charge par l'organe (association, pouvoir législatif, [Chef d'Etat ou de gouvernement], Cour) qui les a nommés en cas de manquement à leurs devoirs prévus par la présente loi-type ou d'atteinte à la dignité de leur fonction.

5. Les membres de l'Autorité de contrôle jouissent d'une immunité totale pour les opinions émises dans l'exercice ou à l'occasion de l'exercice de leur fonction. Ils ne peuvent être relevés de leur charge en raison des opinions qu'ils émettent ou des actes qu'ils accomplissent pour remplir leurs fonctions

Dans l'exercice de leur attribution, ils ne reçoivent d'instruction d'aucune autorité.

6. Sans préjudice de l'Article 32.1 alinéa f, les membres et membres du personnel de l'Autorité de contrôle ainsi que les experts dont le concours est requis sont tenus d'une obligation de confidentialité à l'égard des faits, actes ou renseignements dont ils ont eu connaissance en raison de leurs fonctions.

7. Le Président de l'Autorité de contrôle exerce ses fonctions à temps plein.

Pendant la durée de son mandat, il ne peut exercer aucune autre activité professionnelle.

Il jouit d'un traitement égal à celui de (…), ainsi que des augmentations et avantages y afférents.

8. Avant leur entrée en fonction, le Président et les membres effectifs ou suppléants prêtent entre les mains du [Chef d'Etat ou de gouvernement] le serment suivant :

"Je jure de remplir en toute conscience et impartialité devoirs de ma charge."

Section 2. Compétences

Article 30.

L'Autorité de contrôle:

a. est chargée de veiller à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente loi-type.

b. émet soit d'initiative, soit sur demande du Gouvernement, des Chambres législatives des avis sur toute question relative à l'application des principes fondamentaux de la protection de la vie privée dans le cadre de la présente loi-type, ainsi que des lois contenant des dispositions relatives à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

c. peut attaquer devant l'autorité judiciaire ou administrative tout acte législatif ou règlementaire qui contreviendrait aux principes fondamentaux de la protection de la vie privée dans le cadre de la présente loi-type, ainsi que des lois contenant des dispositions relatives à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

d. peut prendre des arrêtés ou tout acte équivalent en vertu des compétences spécifiques qui lui sont données par la présente loi-type qui ont valeur de loi.

Article 31.

L'Autorité de contrôle doit être consultée pour avis lors de l'élaboration de tout acte législatif ou réglementaire touchant à la protection des données à caractère personnel.

Article 32.

1. L'Autorité de contrôle doit:

a. répondre à toute demande d'avis portant sur un traitement de données à caractère personnel ;

b. recevoir les formalités préalables à la création de traitements des données à caractère personnel et opérer le contrôle de conformité à la présente loi-type;

c. recevoir, par voie postale ou courrier électronique, les réclamations, les pétitions et les plaintes relatives à la mise en œuvre des traitements des données à caractère personnel et informer leurs auteurs des suites données à celles-ci.

d. L'Autorité de contrôle doit statuer dans un délai de (…) jours.

L'Autorité de contrôle possède un pouvoir d'enquête qui, s'il l'exerce, double le délai prévu au paragraphe précédent.

e. Recevoir, par voie postale ou courrier électronique ou tout autre moyens équivalents, les plaintes relatives aux droits de la personnes concernées prévus au chapitre 6 de la présente loi type.

Toute plainte doit être introduite dans les (…) jours, date de la poste ou date de réception dans le cas d'utilisation du courrier électronique faisant foi, auprès de L'Autorité de contrôle qui doit se prononcer dans les (…) jours de la réception de la plainte.

L'Autorité de contrôle possède un pouvoir d'enquête qui, s'il l'exerce, double le délai prévu au paragraphe précédent pour se prononcer sur la plainte.

f. informer sans délai l'autorité judiciaire d'infractions dont elle a connaissance et qu'elle estime devoir porter à la connaissance de l'autorité judiciaire;

g. procéder, par le biais d'agents assermentés, à des vérifications portant sur tout traitement des données à caractère personnel ;

h. prononcer des sanctions, administratives tel que le retrait de l'autorisation de traitement et pécuniaires telles qu'une amende pécuniaire ou des dommages et intérêts au profit de la personne concernée lésée, à l'égard d'un responsable de traitement en cas de violation des dispositions de la présente loi type;

i. recevoir les notifications prévues à l'Article 17 de la présente loi-type;

j. donner les autorisations visées à l'Article 19 de la présente loi-type;

k. créer et tenir à jour un répertoire des traitements des données à caractère personnel et le tenir à la disposition du public tel que prévu à l'Article 20 de la présente loi-type.

Le registre peut être consulté par toute personne.

l. recevoir les notifications de rupture de sécurité visées à l'Article 16.1 de la présente loi-type.

m. ecueillir et autoriser les projets, modifications ou prorogation des codes de conduites tel que cela est prévu au chapitre 12 de la présente loi-type;

n. émettre des recommandations susceptibles de simplifier et d'améliorer le cadre législatif et réglementaire à l'égard du traitement des données ;

o. mettre en place des mécanismes de coopération avec les autorités de protection des données à caractère personnel de pays tiers ;

p. participer aux négociations internationales en matière de protection des données à caractère personnel ;

q. établir, selon une périodicité bien définie, un rapport d'activités remis aux hautes autorités du pays.

2. Dans le cadre de sa compétence d'enquête prévue au présent article, le pouvoir de l'Autorité de contrôle est équivalent à celui d'un juge d'instruction [ou fonction équivalente] dans les limites des compétences de ladite autorité de contrôle et sans pouvoir empiéter sur les compétences du pouvoir judiciaire.

Article 33.

1. L'Autorité de contrôle prononce les mesures suivantes :

a. un avertissement à l'égard du responsable du traitement ne respectant pas les dispositions adoptées par les Etats membres en application de la présente loi type;

b. une mise en demeure de faire cesser les manquements concernés dans le délai qu'elle fixe.

2. Si le responsable du traitement ne se conforme pas à la mise en demeure qui lui a été adressée, l'Autorité de contrôle peut prononcer à son encontre, après procédure contradictoire, les sanctions suivantes :

a. un retrait provisoire de l'autorisation accordée ou une interdiction provisoire de traitement ;

b. le retrait définitif de l'autorisation ou une interdiction définitive de traitement ;

c. une amende pécuniaire de (…);

3. En cas d'urgence, lorsque la mise en œuvre d'un traitement ou l'exploitation de données à caractère personnel entraîne une violation de droits et libertés individuelles, l'Autorité de contrôle, après procédure contradictoire, peut décider :

a. l'interruption de la mise en œuvre du traitement ;

b. l'interdiction temporaire ou définitive d'accès à certaines données à caractère personnel traitées ;

c. l'interdiction temporaire ou définitive d'un traitement contraire aux dispositions de la présente loi type.

4. Les sanctions et décisions prises par l'Autorité de contrôle sont susceptibles de faire l'objet d'un recours devant les autorités judiciaires.

Article 34.

L'Autorité de contrôle peut être saisie par toute personne, agissant par elle-même ou par son représentant au sens des articles 26 et 27 de la présente loi-type, par l'entremise de son avocat ou par toute autre personne physique ou morale dûment mandatée.

Article 35.

1. L'Autorité de contrôle établit un règlement intérieur qui précise, notamment:

   a. les règles relatives aux délibérations, à l'instruction et à la présentation des dossiers;

   b. les règles relatives au traitement des plaintes;

   c. les règles relatives à la procédure contradictoire visée au présent article.

2. Le règlement d'ordre intérieur doit être adopté par l'Autorité de contrôle dans les (…) jours de l'entrée en exercice de la mise.

Section 3. Financement

Article 36.

1. Pour l'accomplissement de ses missions, l'Autorité de contrôle devrait recevoir une dotation budgétaire de l'Etat.

2. Elle recueillerait également les amendes pécuniaires infligées aux responsables de traitement en vertu de ce qui est prévu au présent chapitre.

3. L'Autorité de contrôle devrait rendre un rapport annuel à la Cour des comptes [s'il n'en existe pas, à la Cour supérieure dans lequel est reprise sa gestion financière].

Chapitre 8. Recours à l'autorité judiciaire

Article 37.

Sans préjudice du recours administratif qui peut être organisé, notamment devant l'Autorité de contrôle visée au chapitre 7, antérieurement à la saisine de l'autorité judiciaire, toute personne dispose d'un recours juridictionnel en cas de violation des droits qui lui sont garantis par les dispositions de la présente loi-type.

Article 38.

Le législateur doit favoriser les actions collectives au profit des personnes concernées afin de leur permettre de faire valoir leurs droits issus de la présente loi-type.

Article 39.

Responsabilité

1. Toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec les dispositions de la présente loi-type a le droit d'obtenir du responsable du traitement réparation du préjudice subi.

2. Le responsable du traitement peut être exonéré partiellement ou totalement de cette responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable.

Chapitre 9. Les sanctions.

Article 40.

1. Est puni d'une amende de (…), tout membre ou tout membre du personnel de l'Autorité de contrôle ou tout expert requis par elle qui a violé l'obligation de confidentialité à laquelle il est astreint sur la base de l'Article 29.6 de la présente loi-type.

2. Est puni d'une amende de (…) le responsable du traitement, son représentant, son préposé ou mandataire qui n'a pas respecté une des obligations prévues aux Articles 14 ou 15.1 ou 16 de la présente loi-type.

3. Est puni d'une amende de (…) :

a. Le responsable du traitement, son représentant, son préposé ou mandataire qui traite des données à caractère personnel en infraction aux conditions imposées par l'Article 4.1 de la présente loi-type;

b. Le responsable du traitement, son représentant, son préposé ou mandataire qui traite des données en dehors des cas prévus à l'Article 4 de la présente loi-type;

c. Le responsable du traitement, son représentant, son préposé ou mandataire qui a traité des données en violation des Articles 5, 6, 7, 8, 9 ou 10 de la présente loi-type;

d. Le responsable du traitement, son représentant, son préposé ou mandataire qui n'a pas respecté les obligations prévues à l'Article 12 de la présente loi-type;

e. Le responsable du traitement, son représentant, son préposé ou mandataire, qui n'a pas donné communication, dans les (…) jours de la réception de la demande, des renseignements visés à l'Article 22.1 de la présente loi-type ou donné sciemment des renseignements inexacts ou incomplets;

f. Quiconque, pour contraindre une personne à lui communiquer les renseignements obtenus par l'exercice du droit consacré par l'Article 22.1 de la présente loi-type, ou à donner son autorisation au traitement de données à caractère personnel la concernant, a usé à son égard de voies de fait, de violence ou menaces, de dons ou de promesses

g. Le responsable du traitement, son représentant, son préposé ou mandataire qui met en œuvre ou gère, continue de gérer ou supprime un traitement automatisé de données à caractère personnel sans avoir satisfait aux exigences imposées par les Articles 17 et 19 de la présente loi-type;

h. Le responsable du traitement, son représentant, son préposé ou mandataire, qui fournit des informations incomplètes ou inexactes dans les déclarations prescrites par l'Article 18 de la présente loi-type;

i. Quiconque a transféré, fait ou laissé transférer des données à caractère personnel vers un pays non membre de la CEMAC ou CEEAC qui figure sur la liste visée à l'Article 43.2, § 2, sans qu'il ait été satisfait aux exigences prévues à l'Article 44 de la présente loi-type;

j. Quiconque a empêché l'Autorité de contrôle, ses membres ou les experts requis par elle de procéder aux vérifications visées au chapitre 7 de la présente loi-type.

4. En condamnant du chef d'infraction au présent article, l'autorité judiciaire doit ordonner l'insertion du jugement, intégralement ou par extraits, dans un ou plusieurs journaux, dans les conditions qu'il détermine, aux frais du condamné.

5. En condamnant du chef d'infraction au présent article, le juge peut prononcer la confiscation des supports matériels des données à caractère personnel formant l'objet de

l'infraction, tels que les fichiers manuels, disques et bandes magnétiques, à l'exclusion des ordinateurs ou de tout autre matériel, ou ordonner l'effacement de ces données.

La confiscation ou l'effacement peuvent être ordonnés même si les supports matériels des données à caractère personnel n'appartiennent pas au condamné.

Les objets confisqués doivent être détruits lorsque la décision est passée en force de chose jugée.

6. Le présent article ne fait pas obstacle au mesures de clémences prévus par les lois tels que la suspension ou le sursis à l'exception des peines prévues aux paragraphes 4 et 5.

7. Sans préjudice des interdictions énoncées par des dispositions particulières, le tribunal peut, lorsqu'il condamne du chef d'infraction au présent article, interdire de gérer, personnellement ou par personne interposée, et pour deux ans au maximum, tout traitement de données à caractère personnel.

8. Toute infraction à l'interdiction édictée par le paragraphe 7 ou toute récidive relative aux infractions visées au présent article sont punies d'un emprisonnement de (…) mois à (…) ans et d'une amende de (…) ou d'une de ces peines seulement.

9. Le responsable du traitement ou son représentant en [pays] est civilement responsable du paiement des amendes auxquelles son préposé ou mandataire a été condamné.

Chapitre 10. Limitations

Article 50.

1. Les États membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus à l'Article 4 paragraphe 1, à la section 1 du chapitre 5, aux sections 1, 2 et 3 du chapitre 6 et à l'Article 22 lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder:

a. la sûreté de l'État;

b. la défense;

c. la sécurité publique;

d. la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas des professions réglementées;

e. un intérêt économique ou financier important d'un État membre ou de l'organisation régionale, y compris dans les domaines monétaire, budgétaire et fiscal;

f. une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points c), d) et e);

g. la protection de la personne concernée ou des droits et libertés d'une autre personne.

2. L'Article 4.1 alinéas d, les Articles 6, 7, 8, 9, 12, 13, 17, 18, 19, 22, 23, 24 ne s'appliquent pas aux traitements de données à caractère personnel mis en œuvre aux seules fins :

a. D'expression littéraire et artistique ;

b. D'exercice, à titre professionnel, de l'activité de journaliste, dans le respect des règles déontologiques de cette profession.

Toutefois, pour les traitements mentionnés à l'alinéa b, la dispense de l'obligation de déclaration prévue par les Articles 17 et 18 est subordonnée à la désignation par le responsable du traitement d'un délégué à la protection des données appartenant à un

organisme de la presse écrite ou audiovisuelle, chargé de tenir un registre des traitements mis en œuvre par ce responsable et d'assurer, d'une manière indépendante, l'application des dispositions de la présente loi. Cette désignation est portée à la connaissance de l'Autorité de contrôle.

En cas de non-respect des dispositions de la loi applicables aux traitements prévus par le présent article, le responsable du traitement est enjoint par l'Autorité de contrôle de se mettre en conformité avec la présente loi-type. En cas de manquement constaté à ses devoirs, le délégué à la protection des données est déchargé de ses fonctions sur demande, ou après consultation, de l'Autorité de contrôle.

Les dispositions des alinéas précédents ne font pas obstacle à l'application des dispositions [du code civil, des lois relatives à la presse écrite ou audiovisuelle et du code pénal] qui prévoient les conditions d'exercice du droit de réponse et qui préviennent, limitent, réparent et, le cas échéant, répriment les atteintes à la vie privée et à la réputation des personnes.

Chapitre 11. Flux transfrontaliers

Article 51.

Sans préjudice des dispositions du chapitre 4 de la présente loi-type:

1. Les données à caractère personnel ne peuvent faire l'objet de transferts transfrontaliers que si elles sont nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire.

2. Lorsque les données sont transférées à la suite d'une demande du destinataire, tant le responsable du traitement que le destinataire assument la responsabilité de la légitimité de ce transfert.

Le responsable du traitement est tenu de vérifier la compétence du destinataire et d'évaluer à titre provisoire la nécessité du transfert de ces données. Si des doutes se font jour quant à la nécessité de ce transfert, le responsable du traitement demande au destinataire un complément d'informations.

Le destinataire veille à ce que la nécessité du transfert des données puisse être ultérieurement vérifiée.

3. Le destinataire traite les données à caractère personnel uniquement aux fins qui ont motivé leur transmission.

Section 1. Vers un état non membre de la CEMAC et de la CEEAC

Article 60.

1. Le transfert de données à caractère personnel faisant l'objet d'un traitement après leur transfert vers un état non membre de la CEMAC ou de la CEEAC, ne peut avoir lieu que si l'Etat en question assure un niveau de protection adéquat et moyennant le respect des autres dispositions de la présente loi-type et de ses arrêtés d'exécution.

Le caractère adéquat du niveau de protection s'apprécie au regard de toutes les circonstances relatives à un transfert de données ou à une catégorie de transferts de données; il est notamment tenu compte de la nature des données, de la finalité et de la durée du ou des traitements envisagés, des pays d'origine et de destination finale, des règles de droit, générales et sectorielles, en vigueur dans le pays en cause, ainsi que des règles professionnelles et des mesures de sécurité qui y sont respectées.

2. l'Autorité de contrôle détermine par voie d'arrêté ou acte équivalent pour quelles catégories de traitements de données à caractère personnel et dans quelles circonstances la transmission de données à caractère personnel vers des Etats non-membres de la CEMAC ou de la CEEAC n'est pas autorisée.

Article 61.

1. Par dérogation à l'Article 42, un transfert ou une catégorie de transferts de données à caractère personnel vers un pays non membre de la CEMAC ou de la CEEAC et n'assurant pas un niveau de protection adéquat, peut être effectué dans un des cas suivants:

a. la personne concernée a indubitablement donné son consentement au transfert envisagé;

b. le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou des mesures préalables à la conclusion de ce contrat, prises à la demande de la personne concernée;

c. le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers;

d. le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice;

e. le transfert est nécessaire a la sauvegarde de l'intérêt vital de la personne concernée;

f. le transfert intervient au départ d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier.

Sans préjudice des dispositions de l'alinéa précédent, l'Autorité de contrôle peut autoriser un transfert ou un ensemble de transferts de données à caractère personnel vers un pays non membre de la CEMAC ou de la CEEAC et n'assurant pas un niveau de protection adéquat, lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants; ces garanties peuvent notamment résulter de clauses contractuelles appropriées.

Chapitre 12. Code de conduite

Article 62.

1. L'élaboration de codes de conduite destinés à contribuer, en fonction de la spécificité des secteurs, à la bonne application des dispositions de la présente loi-type est encouragée.

2. Les associations professionnelles et les autres organisations représentant d'autres catégories de responsables du traitement qui ont élaboré des projets de codes nationaux ou qui ont l'intention de modifier ou de proroger des codes nationaux existants doivent les soumettre à l'autorisation de l'Autorité de contrôle.

Elle s'assure, entre autres, de la conformité des projets qui lui sont soumis avec les dispositions de la présente loi-type. Si elle l'estime opportun, elle recueille les observations des personnes concernées ou de leurs représentants.

Chapitre 13. Système d'alerte professionnelle (whistelblowing)

Article 63.

L'Autorité de contrôle, par arrêté ou acte équivalent, doit mettre en place des règles autorisant et régissant les systèmes d'alerte professionnelle.

Ces règles doivent assurer le respect:

a. des règles de loyauté, de licéité et de finalité du traitement;

b. des règles relatives à la proportionnalité tel que la limitation du champ d'application, d'exactitude et de précision des données à caractère personnel destinées au traitement;

c. du principe de transparence tant au niveau collectif en mettant en place une information adéquate qu'individuel en mettant en place une information individuelle portant sur:

– du champ d'application et des finalités du système d'alerte;

– de la procédure d'introduction et de traitement des signalements;

– des conséquences de signalements justifiés et injustifiés;

– de la manière dont les droits d'accès, de rectification et de suppression peuvent être exercés ainsi que de l'instance auprès de laquelle ces droits peuvent être exercés ;

– des tiers à qui des données à caractère personnel concernant le dénonciateur et la personne mise en cause peuvent être transmises dans le cadre du traitement du signalement, par exemple le service d'audit interne si «le gestionnaire de plaintes» doit faire vérifier certaines choses.

La personne mise en cause doit être informée le plus rapidement possible par «le gestionnaire de plaintes» de l'existence d'un signalement et des faits qui lui sont reprochés afin de lui permettre d'exécuter ses droits prévus par la présente loi-type.

L'information de la personne mise en cause peut être reportée dans des circonstances exceptionnelles (par exemple, en cas de risque de destruction de preuves).

d. des règles de sécurité tant organisationnelle que technique;

e. des règles relatives aux droits des personnes concernées en précisant que le droit d'accès ne permet pas d'accéder aux données à caractère personnel d'autrui à moins qu'ils aient donné leur accord express et écrit;

f. des règles de notification à l'Autorité de contrôle.

PROJET DE LOI-TYPE/DIRECTIVE RELATIF AUX TRANSACTIONS ELECTRONIQUES

Préambule

Avec le développement constant des technologies de l'information et de la communication, en particulier l'internet et ses principales applications (notamment le web et le courrier électronique, qui peuvent inclure la voix et la vidéo), de nombreuses transactions sont désormais réalisées par voie électronique. Du point de vue de l'utilisateur, ces transactions électroniques vont généralement se traduire par un ensemble cohérent d'échanges d'informations relatifs à une même idée ou à un même acte, entre deux ou plusieurs terminaux, à travers un réseau de communication électronique.

Compte tenu de ses caractéristiques, l'internet constitue un vecteur privilégié de messages publicitaires, à travers les sites web (notamment par des bandeaux publicitaires, des pop up, etc.) ou par l'envoi de courriers électroniques. Il est en effet possible de proposer aux internautes des publicités personnalisées et interactives, à un coût plus réduit que dans l'environnement traditionnel. De nombreux contrats peuvent également être conclus en ligne. Ils peuvent avoir pour objet des biens (livres, vêtements, bouteilles de vin, etc.) ou des services (voyage, conseils, etc.). En outre, il n'est plus rare que des contrats soient conclus et exécutés en ligne, en particulier lorsqu'ils ont pour objet des contenus numériques, tels que des morceaux de musique téléchargés en ligne, des films visionnés en *streaming* ou des jeux vidéos exécutés dans le contexte du *cloud computing* (*cloud gaming*). Enfin, et de manière plus large, diverses informations peuvent être communiquées à travers les réseaux.

L'avènement d'une société de l'information s'est également traduit par l'apparition de nouveaux métiers, indispensables au fonctionnement des réseaux. On songe aux activités d'hébergement des données, de stockage sous forme de copie temporaire ou de simple transport (comprenant notamment la fourniture d'accès à l'internet). Des prestataires dits « de confiance » peuvent également intervenir, pour délivrer des certificats de signature électronique (permettant de faire le lien entre le procédé de signature électronique utilisé et une personne, en confirmant son identité) ou proposer des services de recommandé électronique, par exemple.

Sur le plan socio-économique, le recours aux technologies de l'information et de la communication pour réaliser des transactions électroniques est un facteur de développement considérable, qu'il convient de soutenir par l'adoption d'un cadre normatif approprié.

Dans les Etats membres de la [à compléter], le potentiel de croissance des transactions électroniques est important mais on peut considérer qu'actuellement, celui-ci reste sous-exploité, en l'absence de cadre normatif satisfaisant et harmonisé.

Il importe ainsi de lever les obstacles d'ordre formels, en consacrant et en appliquant le principe d'équivalence fonctionnelle. Pour la plupart, les exigences de forme – écrit, signature, exemplaires multiples, mentions manuscrites, etc. – ont en effet été pensées dans un environnement « papier », qu'elles soient requises à des fins probatoires ou pour protéger l'un des cocontractants, supposé en position de faiblesse. L'insécurité juridique persistera aussi longtemps que des garanties ne seront pas apportées quant à l'efficacité des procédés susceptibles d'être mis en œuvre dans l'environnement numérique pour accomplir ces formalités (notamment la signature électronique, l'écrit électronique, le recommandé électronique, etc.). Aussi est-il crucial de lever rapidement les obstacles rencontrés en consacrant le principe d'équivalence fonctionnelle, et dans le respect du principe de neutralité technologique.

S'agissant spécifiquement des services de la société de l'information, les obstacles tiennent aussi à l'absence, ou l'insuffisance, de dispositions légales ou réglementaires encadrant les publicités en ligne ou la conclusion des contrats par voie électronique, en particulier dans les relations entre un prestataire professionnel et un consommateur. Dès lors que les parties ne sont pas en présence physique l'une de l'autre, on peut craindre que leur consentement ne soit pas aussi libre et éclairé qu'il aurait pu l'être. L'utilisation de technologies nouvelles, insuffisamment maîtrisées par certaines parties, peut être source d'erreurs dans la saisie des données ou pourrait conduire des personnes à biaiser les données à des fins malhonnêtes.

On peut craindre également que les prestataires indispensables au fonctionnement des réseaux, en ce qu'ils permettent l'échange et la conservation des informations transmises par le biais des réseaux, hésitent à poursuivre leurs activités ou, pire, appliquent des mesures de censure préventive si leur responsabilité civile ou pénale peut être engagée systématiquement en cas d'informations illicites. Ces mesures doivent être évitées, sous peine de porter atteinte à la liberté d'expression (un droit de l'homme consacré de manière universelle) qui doit nécessairement être préservée sur les réseaux de communication.

Les transactions électroniques réalisées par le biais des réseaux ne connaissent pas les frontières étatiques. Par conséquent, leur développement pérenne ne sera garanti que si la sécurité juridique des relations contractuelles présentant un élément d'extranéité est renforcée. Dans cette perspective, il importe que les prestataires puissent connaître les règles qui gouvernent leurs activités et que toute entrave injustifiée à l'exercice de celles-ci soit levée. On comprend sans peine que les divergences entre les législations nationales pourraient dissuader les prestataires d'offrir leurs services par-delà les frontières. En conséquence, les règles doivent également être harmonisées autant que possible, pour soutenir la mise en place d'un véritable marché intérieur rassemblant les Etats membres de la [à compléter]. Les bénéfices de ce marché intérieur des services de la société de l'information seront en effet recueillis par tous les opérateurs économiques, en ce compris les consommateurs.

La présente loi type a précisément pour objet de lever tous ces obstacles. Ce faisant, il établit les conditions nécessaires au développement économique et à la croissance dans le secteur des technologies de l'information et même au-delà, au profit des citoyens, des entreprises et de l'intérêt général. Le transfert des connaissances sera également assuré, contribuant, en parallèle, à ce développement économique.

Titre 1 – Dispositions communes à toutes les transactions électroniques

Chapitre 1 – Définitions et champ d'application

Article 1. Définitions

Au sens de la présente loi type, on entend par :

1° Service de la société de l'information : toute activité économique, accomplie à distance et par voie électronique, portant sur des biens, des services, des droits ou des obligations.

Constituent notamment des services de la société de l'information, la conclusion en ligne de contrats portant sur des biens ou services (même si la livraison de bien ou la prestation de services a lieu hors ligne) ; la fourniture d'informations en ligne ; la diffusion de publicités en ligne, la fourniture d'outils de recherche en ligne, la fourniture de services d'hébergement en ligne ou de stockage sous forme de cache. Le fait que la rémunération du service ne soit pas nécessairement acquittée par le destinataire de celui-ci est sans incidence sur la qualification.

2° Prestataire de service : toute personne physique ou morale qui fournit un service entrant dans le champ d'application de la présente loi type.

3° Destinataire de service de la société de l'information : toute personne physique ou morale qui reçoit un service entrant dans le champ d'application de la présente loi type.

4° Professionnel : toute personne physique ou morale, qu'elle soit publique ou privée, qui agit, y compris par l'intermédiaire d'une autre personne agissant en son nom et pour son compte, à des fins qui entrent dans le cadre de son activité professionnelle qu'elle soit commerciale, industrielle, artisanale ou libérale.

5° Consommateur : toute personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité professionnelle, qu'elle soit commerciale, industrielle, artisanale ou libérale.

6° Contrat à distance : tout contrat conclu entre un professionnel et un consommateur, sans la présence physique simultanée du professionnel et du consommateur, par le recours exclusif à une ou plusieurs techniques de communication à distance, jusqu'au moment, et y compris, au moment où le contrat est conclu.

7° Publicité : toute forme de communication destinée à promouvoir, directement ou indirectement, des biens, des services, ou l'image d'une entreprise, d'une organisation ou d'une personne ayant une activité commerciale, industrielle, artisanale ou libérale.

Ne constituent pas en tant que telles de publicités :

– les informations permettant l'accès direct à l'activité de l'entreprise, de l'organisation ou de la personne, notamment un nom de domaine ou une adresse de courrier électronique ;

– les communications relative aux biens, aux services ou à l'image de l'entreprise, de l'organisation ou de la personne, élaborée d'une manière indépendante, en particulier lorsqu'elles sont fournies sans contrepartie financière.

8° Courrier électronique : tout message sous forme de texte, de voix, de son ou d'image envoyé par un réseau public ou privé de communication, qui peut être stocké dans le réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère.

9° Code de conduite : un accord ou un ensemble de règles qui ne sont pas imposés par les dispositions législatives, réglementaires ou administratives et qui définissent le comportement des entreprises qui s'engagent à être liées par lui en ce qui concerne une ou plusieurs pratiques commerciales ou un ou plusieurs secteurs d'activité.

10° Message EDI : un ensemble de segments, structurés selon une norme agréée, se présentant sous une forme permettant une lecture par ordinateur et pouvant être traités automatiquement et de manière univoque.

11° Profession réglementée : toute activité professionnelle dont l'accès ou l'exercice ou l'une des modalités d'exercice est subordonné, directement ou indirectement, par des dispositions législatives, réglementaires ou administratives, à la possession d'un diplôme, d'un titre de formation, d'une attestation de compétence ou d'une affiliation à un ordre professionnel.

12° Signature électronique avancée : donnée électronique, jointe ou liée logiquement à d'autres données électroniques, servant de méthode d'authentification et satisfaisant aux exigences suivantes :

a. être liée uniquement au signataire;

b. permettre l'identification du signataire;

c. être créée par des moyens que le signataire puisse garder sous son contrôle exclusif;

d. être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectée.

13° Certificat qualifié : une attestation électronique qui lie des données afférentes à la vérification de signature à une personne physique ou morale tout en confirmant l'identité de cette personne et qui, en outre, satisfait aux exigences visées à l'annexe I de la présente loi type et est fourni par un prestataire de service de certification satisfaisant aux exigences visées à l'annexe II de la présente loi type.

14° Dispositif sécurisé de création de signature électronique : dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la création de signature qui satisfait aux exigences de l'annexe III de la présente loi type.

15° Communication électronique : toute communication dans laquelle les informations sont créées, transmises, reçues ou conservées par des moyens électroniques, magnétiques ou optiques ou par des moyens analogues.

Article 2. Champ d'application matériel et personnel

Sans préjudice de l'Article 3 et de l'Article 24, la présente loi type s'applique aux transactions électroniques, qui couvrent notamment :

– les services de la société de l'information, au sens de l'Article 1, 1;

– les activités dépourvues de caractère économique, accomplies à distance et par voie électronique, portant sur des biens, des services, des droits ou des obligations ;

– les activités accomplies à distance et par voie électronique, portant sur des biens, des services, des droits ou des obligations, lorsqu'elles mettent en relation des personnes agissant à des fins qui n'entrent pas dans le cadre de leur activité professionnelle, qu'elle soit commerciale, industrielle, artisanale ou libérale ;

– [Au choix de l'Etat adoptant : d'autres hypothèses peuvent être ajoutées, telles que les procédures judiciaires ou administratives dématérialisées].

Article 3. Exclusion du champ d'application matériel et personnel

La présente loi type ne s'applique pas :

– au domaine de la fiscalité ;

– aux activités suivantes :

- les activités de notaire ou les professions équivalentes, dans la mesure où elles comportent une participation directe et spécifique à l'exercice de l'autorité publique ;
- la représentation d'un client et la représentation de ses intérêts devant les tribunaux ;
- les activités de jeux d'argent impliquant des mises ayant une valeur monétaire dans des jeux de hasard, y compris les loteries, et les transactions portant sur des jeux de hasard.

Chapitre 2 – Règles directrices

Article 4. Non-autorisation préalable

L'accès à l'activité d'un prestataire de services et l'exercice de celle-ci ne peuvent être soumis à un régime d'autorisation préalable ou à toute autre exigence ayant un effet équivalent.

L'alinéa premier est sans préjudice des régimes d'autorisation qui pourraient être établis par les autorités publiques compétentes pour des motifs d'ordre public, de protection de la santé publique, de sécurité publique ou de protection des consommateurs.

Article 5. Assimilation et non-discrimination

A défaut de disposition légale contraire, l'efficacité d'un acte juridique, comprenant sa validité et sa force probatoire ou exécutoire, ne peut être contestée au seul motif qu'il a été posé par voie électronique.

Dans le respect des conditions du chapitre 3 et à défaut de disposition légale contraire, les actes juridiques posés par voie électronique sont équivalents aux actes qui ne sont pas accomplis par ce moyen et leurs effets juridiques sont identiques.

Article 6. Liberté dans le recours aux moyens électroniques

A défaut de disposition légale contraire, nul ne peut être contraint de poser un acte juridique par voie électronique.

Les informations échangées au cours du processus contractuel peuvent être transmises par voie électronique si le destinataire a accepté, même tacitement, l'usage de ce moyen. Cette acception peut par exemple se déduire de l'utilisation des moyens électroniques par le destinataire.

Les informations destinées à un professionnel peuvent lui être adressées par courrier électronique dès lors qu'il a communiqué son adresse professionnelle électronique.

Chapitre 3 – Accomplissement des règles de forme par voie électronique

Section 1 – Principes fondamentaux

Article 7. Principe d'équivalence fonctionnelle

§ 1er. Toute exigence légale ou réglementaire de forme est réputée satisfaite lorsque les qualités fonctionnelles de cette exigence ont été préservées.

Pour l'application du présent paragraphe, il est tenu compte du contexte et de l'objet de l'information à laquelle s'appliquent les exigences de forme, ainsi que de toutes les circonstances y ayant trait.

§ 2. Pour l'application du § 1er, il y a lieu de considérer que :

– l'exigence d'une signature est satisfaite dans les conditions prévues soit à l'Article 11, soit à l'Article 12;

– l'exigence d'un écrit est satisfaite dans les conditions prévues à l'Article 18;

– l'exigence d'un original est satisfaite dans les conditions prévues à l'Article 19;

– l'exigence d'exemplaires multiples est satisfaite dans les conditions prévues à l'Article 20;

– l'exigence d'une mention manuscrite est satisfaite dans les conditions prévues à l'Article21;

– l'exigence d'un recommandé est satisfaite dans les conditions prévues à l'Article 22;

– l'exigence d'une facture est satisfaite dans les conditions prévues à l'Article 23.

Article 8. Principe de non-discrimination

Un acte ne peut être privé de son efficacité juridique sous prétexte que les exigences légales ou réglementaires de forme auquel il est soumis ont été accomplies par voie électronique.

Article 9. Objectifs poursuivis par les règles de forme

Les dispositions du présent chapitre s'appliquent quelles que soient les finalités poursuivies par les règles forme. Sont notamment visées les formalités requises :

– à titre probatoire ;

– pour protéger l'un des cocontractants en position de faiblesse et constituant des conditions de validité de l'acte juridique ou

– pour protéger les tiers.

Article 10. Exclusions du champ d'application

Le présent chapitre ne s'applique pas aux contrats qui relèvent des catégories suivantes :

a. les contrats qui créent ou transfèrent des droits sur des biens immobiliers, à l'exception des droits de location ;

b. les contrats pour lesquels la loi requiert l'intervention des tribunaux, des autorités publiques ou des professions exerçant une autorité publique ;

c. les contrats de sûretés et garantie fournis par des personnes agissant à des fins qui n'entrent pas dans le cadre de leur activité professionnelle ou commerciale ;

d. les contrats relevant du droit de la famille ou du droit des successions.

Section 2 – Signature

Sous-section 1. Principe d'assimilation

Article 11. Fonctions de la signature

Satisfait à l'exigence d'une signature tout procédé permettant d'authentifier l'identité du signataire et de marquer son adhésion au contenu de l'acte, pour autant que la fiabilité de ce procédé soit suffisante au regard de l'objet de l'information pour laquelle la signature est requise, compte tenu de toutes les circonstances, y compris de tout accord en la matière.

Article 12. Signature électronique qualifiée

Lorsqu'un procédé de signature électronique préserve les fonctions minimales de la signature énoncées à l'Article 11 et qu'en outre, il constitue une signature électronique avancée, réalisée sur la base d'un certificat qualifié et conçue au moyen d'un dispositif sécurisé de création de signature électronique, ce procédé est assimilé de plein droit à une signature manuscrite, qu'il soit réalisé par une personne physique ou morale.

Sous-section 2. Activités du prestataire de services de certification délivrant des certificats qualifiés

Article 13. Accès à l'activité et missions du prestataire de services de certification

§ 1. Sans préjudice de l'Article 4, l'accès à l'activité de prestataire de service certification est soumis aux exigences prescrites par la présente loi type.

§ 2. Préalablement à la délivrance d'un certificat, le prestataire de service de certification vérifie la complémentarité des données afférentes à la création et à la vérification de signature.

Après avoir vérifié son identité et, le cas échéant, ses qualités spécifiques, le prestataire de service de certification délivre un ou plusieurs certificats à toute personne qui en fait la demande.

En ce qui concerne les personnes morales, le prestataire de services de certification tient un registre contenant le nom et la qualité de la personne physique qui représente la personne morale et qui fait usage de la signature liée au certificat, de telle manière qu'à chaque utilisation de cette signature, on puisse établir l'identité de la personne physique.

§ 2. Le prestataire de service de certification fournit un exemplaire du certificat au candidat titulaire.

§ 3. Le prestataire de service de certification conserve un annuaire électronique comprenant les certificats qu'il délivre et le moment de leur expiration.

Article 14. Révocation des certificats qualifiés

§ 1. A la demande du titulaire du certificat, préalablement identifié, le prestataire de service de certification révoque immédiatement le certificat.

§ 2. Le prestataire de service de certification révoque également un certificat lorsque :

1° il existe des raisons sérieuses pour admettre que le certificat a été délivré sur la base d'informations erronées ou falsifiées, que les informations contenues dans le certificat ne sont plus conformes à la réalité ou que la confidentialité des données afférentes à la création de signature a été violée;

2° le prestataire de service de certification arrête ses activités sans qu'il n'y ait reprise de celles-ci par un autre prestataire de service de certification garantissant un niveau de qualité et de sécurité équivalent;

3° le prestataire de service de certification est informé du décès de la personne physique ou de la dissolution de la personne morale qui en est le titulaire.

Le prestataire de service de certification informe le titulaire de certificat, sauf en cas de décès, de la révocation et motive sa décision. Un mois avant l'expiration d'un certificat, le prestataire de service de certification informe son titulaire de celle-ci.

§ 3. La révocation d'un certificat est définitive.

§ 4. Le prestataire de service de certification prend les mesures nécessaires afin de répondre à tout moment et sans délai à une demande de révocation.

§ 5. Immédiatement après la décision de révocation, le prestataire de service de certification inscrit la mention de la révocation du certificat dans l'annuaire électronique visé à l'Article 13, § 3.

La révocation est opposable aux tiers à partir de cette inscription.

Article 15. Responsabilité du prestataire de service de certification délivrant des certificats qualifiés

§ 1. Un prestataire de service de certification qui délivre à l'intention du public un certificat présenté comme qualifié ou qui garantit au public un tel certificat est responsable du préjudice causé à tout organisme ou personne physique ou morale qui, en bon père de famille, se fie raisonnablement à ce certificat pour ce qui est de :

a. l'exactitude de toutes les informations contenues dans le certificat qualifié à la date où il a été délivré et la présence, dans ce certificat, de toutes les données prescrites pour un certificat qualifié;

b. l'assurance que, au moment de la délivrance du certificat, le signataire identifié dans le certificat qualifié détenait les données afférentes à la création de signature correspondant aux données afférentes à la vérification de signature fournies ou identifiées dans le certificat;

c. l'assurance que les données afférentes à la création de signature et celles afférentes à la vérification de signature puissent être utilisées de façon complémentaire, dans le cas où le prestataire de service de certification génère ces deux types de données;

sauf si le prestataire de service de certification prouve qu'il n'a commis aucune négligence.

§ 2. Un prestataire de service de certification qui a délivré à l'intention du public un certificat présenté comme qualifié est responsable du préjudice causé à un organisme ou à une personne physique ou morale qui se prévaut raisonnablement du certificat, pour avoir omis de faire enregistrer la révocation du certificat, sauf si le prestataire de service de certification prouve qu'il n'a commis aucune négligence.

§ 3. Un prestataire de service de certification peut indiquer, dans un certificat qualifié, les limites fixées à son utilisation, à condition que ces limites soient discernables par des tiers. Le prestataire de service de certification ne doit pas être tenu responsable du préjudice résultant de l'usage d'un certificat qualifié qui dépasse les limites fixées par le prestataire à son utilisation.

§ 4. Un prestataire de service de certification peut indiquer, dans un certificat qualifié, la valeur maximale des transactions pour lesquelles le certificat peut être utilisé, à condition que cette valeur soit discernable par des tiers. Le prestataire de service de certification n'est pas responsable des dommages qui résultent du dépassement de cette valeur maximale.

Article 16. Arrêt des activités du prestataire de services de certification délivrant des certificats qualifiés

§ 1. Le prestataire de service de certification informe les autorités publiques compétentes [à préciser par l'Etat adoptant], dans un délai raisonnable n'excédant pas [à définir par l'Etat membre adoptant] jours, de son intention de mettre fin à ses activités de prestataire de service de certification qualifiée ainsi que de toute action qui pourrait conduire à la cessation de ses activités. Dans ce cas, il doit s'assurer de la reprise de celles-ci par un autre prestataire de service de certification garantissant un même niveau de qualité et de sécurité, ou à défaut, le prestataire de service de certification délivrant des certificats révoque les certificats deux mois après en avoir averti les titulaires. Dans ce cas, le prestataire de service de certification prend les mesures nécessaires pour satisfaire à l'obligation prévue à l'Annexe II, i).

§ 2. Le prestataire de service de certification qui arrête ses activités pour des raisons indépendantes de sa volonté ou en cas de faillite en informe immédiatement les autorités publiques compétentes [à préciser par l'Etat adoptant]. Il procède, le cas échéant, à la révocation des certificats et prend les mesures nécessaires pour satisfaire à l'obligation prévue à l'Annexe II, i).

Article 17. Certificats délivrés à titre de certificats qualifiés par des prestataires de service de certification étrangers

§ 1. Un certificat qualifié délivré à l'intention du public par un prestataire de service de certification qui est établi dans un Etat membre de la [à compléter] est assimilé aux certificats qualifiés délivrés par un prestataire de service de certification établi sur le territoire [de l'Etat adoptant].

§ 2. Les certificats délivrés à titre de certificats qualifiés à l'intention du public par un prestataire de service de certification établi dans un pays tiers sont reconnus équivalents, sur le plan juridique, aux certificats délivrés par un prestataire de service de certification établi sur le territoire [de l'Etat adoptant] :

a. si le prestataire de service de certification remplit les conditions visées dans la présente loi type, vérifiées par les autorités compétentes

ou

b. si un prestataire de service de certification établi sur le territoire d'un Etat membre de la [à compléter], qui satisfait aux exigences visées dans la présente loi type, garantit le certificat

ou

c. si le certificat ou le prestataire de service de certification est reconnu en application d'un accord bilatéral ou multilatéral entre la [à compléter] et des pays tiers ou des organisations internationales.

Section 3 – Ecrit et autres formalités

Article 18. Ecrit

L'exigence d'un écrit est satisfaite par une suite de signes intelligibles et accessibles pour être consultés ultérieurement, quels que soient leur support et leurs modalités de transmission, pour autant que les exigences d'intégrité et la pérennité de l'information, adaptées aux fins auxquelles celle-ci est destinée, aient été préservées.

Article 19. Original

L'exigence d'un original est satisfaite par tout procédé respectant les exigences cumulatives de l'écrit, au sens de l'Article 18, et de la signature, au sens de l'Article 11 ou de l'Article 12.

Article 20. Exemplaires multiples

L'exigence d'exemplaires multiples est satisfaite par tout procédé garantissant que les informations figurant dans le document sont conservées dans le respect des fonctions d'intégrité et de pérennité, tout en permettant à chacune des parties d'y avoir accès et de les reproduire.

Article 21. Mention manuscrite

L'exigence d'une mention écrite de la main de celui qui s'oblige, qui permet d'attirer l'attention de ce dernier, en authentifiant l'origine de la marque manuscrite et en préservant l'intégrité de l'information, peut être satisfaite par tout procédé garantissant que l'attention de celui qui s'oblige a été attirée avec la même efficacité.

Article 22. Recommandé

L'exigence d'un recommandé est satisfaite par tout procédé dans lequel un tiers dûment identifié intervient pour acheminer le message et qui établit avec un niveau de fiabilité élevé la réalité et la date de l'envoi d'une transmission de données électroniques et, le cas échéant, de leur réception par le destinataire du message.

Article 23. Facture

§ 1er. Eu égard à leurs fonctions fiscales, les factures doivent faire l'objet d'un écrit permettant d'assurer la lisibilité, l'intégrité et la pérennité du contenu. L'authenticité de l'origine doit également être garantie.

Parmi les méthodes susceptibles d'être mises en œuvre pour atteindre les finalités fiscales de la facture et assurer que ses fonctions ont été satisfaites figure la réalisation de contrôles de gestion qui établiraient une piste d'audit fiable entre une facture et une livraison de biens ou de services.

§ 2. Outre le type de contrôles de gestion décrits au §1er, les méthodes suivantes constituent des exemples de technologies permettant d'assurer l'authenticité de l'origine et l'intégrité du contenu d'une facture électronique :

a. une signature électronique qualifiée, telle que définie à l'Article 12;

b. un échange de données informatisées (EDI), compris comme le transfert électronique, d'un ordinateur à un autre, de données commerciales et administratives sous la forme d'un message EDI structuré conformément à une norme agréée, pour autant que l'accord relatif à cet échange prévoie l'utilisation de procédures garantissant l'authenticité de l'origine et l'intégrité des données.

Titre 2 - Dispositions exclusivement applicables aux transactions électroniques constituant des services de la société de l'information

Chapitre 1 – Champ d'application du présent titre

Article 24. Champ d'application matériel et personnel

Le présent titre de la loi type s'applique à certains aspects juridiques des services de la société de l'information fournis par un prestataire, agissant en qualité de professionnel, à un destinataire de service, agissant en qualité de professionnel ou de consommateur.

Article 25. Champ d'application dans l'espace et droit applicable

Sans préjudice de la liberté dont disposent les parties de choisir la loi applicable, les services de la société de l'information régis par la présente loi type sont soumis à la loi [de l'Etat adoptant] sur le territoire duquel le prestataire exerce, d'une manière effective, une activité économique au moyen d'une installation stable et durable.

Par dérogation à l'alinéa 1er, les contrats conclus entre un professionnel et un consommateur sont régis par la loi de l'Etat où le consommateur a sa résidence habituelle, à condition que le professionnel exerce son activité dans l'Etat dans lequel le consommateur a sa résidence habituelle ou, par tout moyen, dirige cette activité vers cet Etat ou vers plusieurs Etats, dont celui-ci et que la loi ainsi désignée soit plus favorable au consommateur que celle désignée par application de l'alinéa 1er. Si les parties conviennent de la loi applicable au contrat, ce choix ne peut avoir pour résultat de priver le consommateur de la protection que lui assurent les dispositions auxquelles il ne peut être dérogé conventionnellement et qui auraient été applicables en l'absence de choix.

Par dérogation à l'alinéa 1er, la loi applicable aux obligations extracontractuelles constituant un service de la société de l'information est déterminée par le lieu de survenance du dommage ou par le lieu du fait générateur.

Chapitre 2 – Obligations générales d'information

Article 26. Informations relatives au prestataire

Sans préjudice des autres exigences d'informations, le prestataire d'un service de la société de l'information doit au moins garantir un accès facile, direct et permanent, pour les destinataires du service et pour les autorités compétentes, aux informations suivantes :

a) le nom du prestataire de services ;

b) l'adresse géographique à laquelle le prestataire de services est établi;

c) les coordonnées du prestataire, comprenant notamment son adresse de courrier électronique, étant entendu que l'un des moyens de communication proposés doit permettre d'entrer en contact rapidement et de communiquer directement et efficacement avec lui (un numéro de téléphone, par exemple) ;

d) dans le cas où le prestataire est inscrit dans un registre de commerce ou dans un autre registre public similaire, le registre de commerce dans lequel il est inscrit et son numéro d'immatriculation, ou des moyens équivalents d'identification figurant dans ce registre;

e) dans le cas où l'activité est soumise à un régime d'autorisation, les coordonnées de l'autorité de surveillance compétente;

f) en ce qui concerne les professions réglementées:

- tout ordre professionnel ou organisme similaire auprès duquel le prestataire est inscrit,

- le titre professionnel et l'État dans lequel il a été octroyé,

- une référence aux règles professionnelles applicables et aux moyens d'y avoir accès;

g) dans le cas où le prestataire exerce une activité soumise à la taxe sur la valeur ajoutée, le numéro d'identification TVA.

Article 27. Informations relatives aux prix

Sans préjudice des autres dispositions légales ou réglementaires en matière d'indication des prix, lorsque les services de la société de l'information mentionnent des prix, ces derniers sont indiqués de manière claire et non ambigüe et précisent notamment si les taxes et les frais de livraison sont inclus.

Chapitre 3 – Publicité en ligne

Section 1 – Principes de transparence et de loyauté

Article 28. Identification de la publicité

Toute publicité doit être clairement identifiable comme telle. Cet objectif peut être atteint en raison de son effet global, en ce compris sa présentation. A défaut, elle doit comporter la mention « publicité » de manière lisible, apparente et non équivoque.

Article 29. Identification de la personne pour le compte de laquelle la publicité est faite

La personne physique ou morale pour le compte de laquelle la publicité est faite doit être clairement identifiable.

Article 30. Offres promotionnelles - Jeux ou concours promotionnels

[Pour autant que ces pratiques soient autorisées dans l'Etat adoptant]

Les offres promotionnelles, telles que les annonces de réductions de prix, les offres conjointes ou tout autre cadeau, doivent être clairement identifiables comme telles et les conditions pour en bénéficier doivent être aisément accessibles et présentées de manière précise et non équivoque;

Les concours ou jeux promotionnels doivent être clairement identifiables comme tels et leurs conditions de participation comprenant, le cas échéant le numéro d'autorisation dont le prestataire doit disposer, doivent être aisément accessibles et présentées de manière précise et non équivoque.

Article 31. Professions réglementées

Les publicités qui font partie d'un service de la société de l'information fourni par un membre d'une profession réglementée, ou qui constituent un tel service, sont autorisées, sous réserve du respect des règles professionnelles visant, notamment, l'indépendance, la dignité et l'honneur de la profession ainsi que le secret professionnel et la loyauté envers les clients et les autres membres de la profession.

Section 2 – Publicités non-sollicitées par courrier électronique

Article 32. Exigence du consentement préalable

L'utilisation du courrier électronique, de télécopieurs ou de systèmes automatisés d'appel et de communication sans intervention humaine (automates d'appel) à des fins de publicité est autorisée moyennant le consentement préalable, libre, spécifique et informé du destinataire des messages.

Article 33. Exceptions à l'exigence du consentement préalable

Par dérogation à l'Article 32, tout prestataire est dispensé de solliciter le consentement préalable à recevoir des publicités par voie électronique :

1.° auprès de ses clients, personnes physiques ou morales, lorsque chacune des conditions suivantes est remplie :

a. il a obtenu directement leurs coordonnées électroniques dans le cadre de la vente d'un bien ou d'un service, dans le respect des exigences légales et réglementaires relatives à la protection de la vie privée;

b. il exploite lesdites coordonnées électroniques à des fins de publicité exclusivement pour des biens ou services analogues à ceux que lui-même fournit;

c. il fournit à ses clients, au moment où leurs coordonnées électroniques sont recueillies, la faculté de s'opposer, sans frais et de manière simple et facile, à une telle exploitation.

2.° auprès de personnes morales si les coordonnées électroniques qu'il utilise à cette fin sont impersonnelles.

Article 34. Droit d'opposition

§ 1. Toute personne peut notifier directement à un prestataire déterminé, sans frais ni indication de motifs, sa volonté de ne plus recevoir, de sa part, des publicités par courrier électronique. Le prestataire concerné est tenu de :

1° délivrer, dans un délai raisonnable, un accusé de réception par courrier électronique confirmant à cette personne l'enregistrement de sa demande;

2° prendre, dans un délai raisonnable, les mesures nécessaires pour respecter la volonté de cette personne;

3° tenir à jour des listes reprenant les personnes ayant notifié leur volonté de ne plus recevoir, de sa part, des publicités par courrier électronique.

§ 2. Lors de l'envoi de toute publicité par courrier électronique, le prestataire :

1° fournit une information claire et compréhensible, sur le fond et dans la forme, concernant le droit de s'opposer, pour l'avenir, à recevoir les publicités ;

2° indique et met à disposition un moyen approprié d'exercer efficacement ce droit par voie électronique.

Article 35. Pratiques publicitaires interdites

Lors de l'envoi de publicités par courrier électronique, il est interdit au prestataire :

1° d'utiliser l'adresse électronique ou l'identité d'un tiers ;

2° de falsifier ou de masquer toute information permettant d'identifier l'origine du message de courrier électronique, son objet ou son chemin de transmission.

Article 36. Charge de la preuve

En cas de contestation, il incombe au prestataire de démontrer que l'envoi de publicités par courrier électronique a fait l'objet d'un consentement préalable, libre, spécifique et informé du destinataire des messages ou que les conditions de l'Article 33 étaient réunies.

Chapitre 4 - Contrats conclus à distance et par voie électronique

Section 1 – Règles applicables aux contrats conclus avec les consommateurs et avec les professionnels

Sous-section 1. Règles applicables avant la passation de la commande

Article 37. Obligations d'information

§ 1. Sans préjudice des autres exigences légales ou réglementaires en matière d'information, le prestataire de services fournit au moins les informations mentionnées ci-après, formulées, sur le fond et sur la forme, de manière claire, compréhensible et non équivoque et avant que le destinataire du service ne passe une commande par voie électronique :

a) les différentes étapes techniques à suivre pour conclure le contrat ;
b) si le contrat une fois conclu est archivé ou non par le prestataire de services, s'il est accessible ou non, ainsi que les modalités de cet archivage et les conditions de l'accessibilité;
c) les moyens techniques pour identifier et corriger des erreurs commises dans la saisie des données avant que la commande ne soit passée ;
d) les langues proposées pour la conclusion du contrat.

§ 2. Le prestataire indique les éventuels codes de conduite auxquels il est soumis ainsi que les informations sur la façon dont ces codes peuvent être consultés par voie électronique.

§ 3. Les clauses contractuelles et les conditions générales des contrats conclus par voie électronique, fournies au destinataire, doivent l'être d'une manière qui lui permette de les conserver et de les reproduire.

Article 38. Moyens techniques permettant d'identifier et de corriger les erreurs

Le prestataire met à la disposition du destinataire du service des moyens techniques appropriés, efficaces et accessibles lui permettant d'identifier les erreurs commises dans la saisie des données et de les corriger, et ce avant la passation de la commande.

Sous-section 2. Règles applicables après la passation de la commande

Article 39. Accusé de réception

§ 1. Lorsque le destinataire du service a passé une commande par voie électronique, le prestataire doit accuser réception de celle-ci sans délai injustifié et par voie électronique.

L'accusé de réception contient un récapitulatif de la commande.

§ 2. La commande et l'accusé de réception sont considérés comme reçus dans les conditions de l'Article 42, § 2.

Sous-section 3. Dispositions communes

Article 40. Dérogations conventionnelles possibles

Les parties qui ne sont pas des consommateurs peuvent déroger conventionnellement aux dispositions de l'Article 37, §§ 1er et 2, de l'Article 38, de l'Article 39.

Article 41. Exclusions du champ d'application

Les dispositions de l'Article 37, §§ 1er et 2, de l'Article38 et de l'Article39 ne sont pas applicables à des contrats conclus exclusivement par le biais d'un échange de courriers électroniques ou par des communications individuelles équivalentes, existantes ou à venir.

Article 42. Moment et lieu de l'expédition et de la réception des messages

§ 1er. Le moment de l'expédition d'un courrier électronique, d'un accusé de réception, d'une confirmation écrite ou de tout autre message envoyé dans le cadre du processus contractuel est le moment où ce message quitte un système d'information dépendant de l'expéditeur ou de la partie qui l'a envoyée au nom de l'expéditeur, ou bien, si la communication électronique n'a pas quitté un système d'information dépendant de l'expéditeur ou de la partie qui l'a envoyée au nom de l'expéditeur, le moment où elle est reçue.

§ 2. Le moment de la réception d'un message est le moment où celui-ci peut être relevé par le destinataire à une adresse électronique que celui-ci a désignée. Le moment de la réception d'un message à une autre adresse électronique du destinataire est le moment où ce message peut être relevé par le destinataire à cette adresse et où celui-ci prend connaissance du fait qu'il a été envoyé à cette adresse. Un message est présumé pouvoir être relevé par le destinataire lorsqu'il parvient à l'adresse électronique de celui-ci.

§ 3. Un message est réputée avoir été expédié du lieu où l'expéditeur a son établissement et avoir été reçu au lieu où le destinataire a son établissement, ces lieux étant déterminés conformément à l'Article 25.

§ 4. Le paragraphe 2 du présent article s'applique même si le lieu où est situé le système d'information qui constitue le support de l'adresse électronique est différent du lieu où la communication électronique est réputée avoir été reçue selon le paragraphe 3 du présent article.

Article 43. Utilisation de systèmes automatisés pour la conclusion des contrats

La validité ou la force probatoire ou exécutoire d'un contrat formé par l'interaction d'un système automatisé et d'une personne physique, ou bien par l'interaction de systèmes automatisés, ne peuvent être contestées au seul motif qu'une personne physique n'est pas intervenue ou n'a pas contrôlé chacune des opérations exécutées par les systèmes ni le contrat qui en résulte.

Section 2 – Règles applicables aux contrats conclus avec les consommateurs

Sous-section 1er. Obligations d'information

Article 44. Obligation d'information avant la conclusion du contrat

Sans préjudice des obligations d'information requises conformément à l'Article37, avant que le consommateur ne soit lié par un contrat à distance ou par une offre, le professionnel lui fournit également, sous une forme claire et compréhensible sur le fond et sur la forme, les informations suivantes :

a. concernant le prestataire, les données énumérées à l'Article 26 ;

b. concernant le bien ou le service, en ce compris les contenus numériques :

ses principales caractéristiques, dans la mesure appropriée au support de communication utilisé et au bien ou service concerné ;

s'il s'agit d'un contenu numérique, ses fonctionnalités, et s'il y a lieu, les mesures de protection technique applicables et toute interopérabilité du contenu numérique avec certains matériels ou logiciels dont le professionnel a ou devrait raisonnablement avoir connaissance ;

c. concernant le prix :

les données énumérées à l'Article 27 ;

le cas échéant, le coût de l'utilisation de la technique de communication à distance pour la conclusion du contrat, lorsque ce coût est calculé sur une base autre que le tarif de base ;

d. concernant le droit de rétractation :

l'existence d'un droit de rétractation ou l'absence d'un tel droit, dans les hypothèses visées à l'Article 51 ;

le cas échéant, si le consommateur peut bénéficier d'un droit de rétractation, les conditions, le délai et les modalités d'exercice de ce droit, conformément à l'Article 48 et suivants ;

le cas échéant, le fait que le consommateur devra supporter les frais de renvoi du bien en cas de rétractation et, si le bien, en raison de sa nature, ne peut normalement être renvoyé par la poste, le coût de renvoi du bien;

e. concernant les conditions auxquelles l'exécution du contrat est soumise :

– les modalités de paiement, de livraison (et l'existence d'éventuelles restrictions de livraisons) et d'exécution, la date à laquelle le professionnel s'engage à livrer les biens ou à exécuter les services et, le cas échéant, les modalités prévues par le professionnel pour le traitement des réclamations ;

– l'existence d'une assistance après-vente au consommateur, d'un service après-vente et de garanties commerciales, ainsi que les conditions y afférentes, le cas échéant;

– la durée du contrat, s'il y a lieu, ou, s'il s'agit d'un contrat à durée indéterminée ou à reconduction tacite, les conditions de résiliation du contrat;

– la durée minimale des obligations du consommateur au titre du contrat, s'il y a lieu;

– l'existence d'une caution ou d'autres garanties financières à payer ou à fournir par le consommateur à la demande du professionnel, ainsi que les conditions y afférentes, le cas échéant;

– le cas échéant, la possibilité de recourir à une procédure extrajudiciaire de réclamation et de recours à laquelle le professionnel est soumis et les conditions d'accès à celle-ci.

Article 45. Contraintes d'espace ou de temps

Lorsque la technique de communication utilisée aux fins de la conclusion du contrat impose des contraintes d'espace ou de temps pour la présentation des informations, le professionnel fournit, au moyen de cette technique de communication et avant la conclusion du contrat, au minimum les informations précontractuelles concernant les principales caractéristiques du bien ou du service, l'identité du professionnel, le prix total, le droit de rétractation, la durée du contrat et, dans le cas des contrats à durée indéterminée, les modalités pour mettre fin au contrat. Le professionnel fournit au consommateur les autres informations visées à l'Article 44 sous une forme adaptée, libérée de ces contraintes d'espaces ou de temps.

S'il apparaît que les finalités minimales des obligations d'information ont été atteintes moyennant la mise en place d'un autre procédé, fonctionnellement équivalent, cette obligation d'information est réputée satisfaite conformément aux dispositions légales ou réglementaires applicables.

Article 46. Obligation d'information après la conclusion du contrat

Le professionnel fournit au consommateur la confirmation du contrat conclu, par écrit et dans un délai raisonnable après la conclusion du contrat à distance et, au plus tard, au moment de la livraison du bien ou avant l'exécution du contrat de service.

Cette confirmation comprend toutes les informations visées à l'Article 44, sauf si le professionnel a déjà fourni ces informations au consommateur par écrit avant la conclusion du contrat à distance.

Article 47. Charge de la preuve

La charge de la preuve concernant le respect des obligations énoncées dans la présente sous-section incombe au professionnel.

Sous-section 2. Droit de rétractation

Article 48. Conditions d'exercice du droit de rétractation

§ 1. Le consommateur dispose d'un délai de quatorze jours calendrier pour se rétracter d'un contrat à distance, sans avoir à motiver sa décision et sans avoir à supporter d'autres coûts que les frais directs de renvoi du bien.

§ 2. Le délai de quatorze jours calendrier commence à courir :

a. en ce qui concerne les contrats de service, du jour de la conclusion du contrat ;

b. en ce qui concerne les contrats portant sur des biens, du jour où le consommateur prend physiquement possession du bien

Article 49. Droits et obligations du consommateur

Le consommateur informe le professionnel, avant l'expiration du délai de rétractation, de sa décision de se rétracter du contrat. Le droit de rétractation est exercé dans les délais prescrits si la communication concernant l'exercice du droit a été envoyée avant l'expiration du délai.

Le consommateur renvoie ou rend les biens au professionnel ou à une personne habilitée par ce dernier à les réceptionner sans retard excessif et, en tout état de cause, au plus tard 14 jours calendrier suivant la communication de sa décision de rétractation au professionnel conformément à l'alinéa précédent, sauf si le professionnel propose de reprendre lui-même ces biens. Ce délai est réputé respecté si le consommateur a renvoyé les biens avant l'expiration du délai de 14 jours.

Le consommateur supporte uniquement les coûts directs engendrés par le renvoi des biens, sauf si le professionnel accepte de les prendre à sa charge ou s'il a omis d'informer correctement et suffisamment le consommateur qu'il doit les prendre en charge.

Article 50. Droits et obligations du professionnel

Le professionnel rembourse tous les paiements reçus de la part du consommateur, y compris, le cas échéant, les frais de livraison, sans retard excessif et en tout état de cause dans les 14 jours calendrier suivant celui où il est informé de la décision du consommateur de se rétracter conformément à l'Article 49.

Le professionnel effectue le remboursement visé au premier alinéa en utilisant le même moyen de paiement que celui utilisé par le consommateur pour la transaction initiale, sauf accord exprès du consommateur et pour autant que le remboursement n'occasionne pas de frais pour le consommateur.

Sauf si le professionnel propose de reprendre lui-même les biens, concernant les contrats de vente, il peut différer le remboursement jusqu'à récupération des biens, ou jusqu'à ce que le consommateur ait fourni une preuve d'expédition des biens, la date retenue étant celle du premier de ces faits.

Article 51. Exceptions au droit de rétractation

Aucun droit de rétractation n'est octroyé au consommateur en ce qui concerne :

a. les contrats de service après que le service a été pleinement exécuté si l'exécution a commencé avec l'accord préalable exprès du consommateur, lequel a également pris acte qu'il perdrait son droit de rétractation une fois que le contrat aurait été pleinement exécuté par le professionnel;

b. la fourniture de biens ou de services dont le prix dépend de fluctuations sur le marché financier échappant au contrôle du professionnel et susceptibles de se produire pendant le délai de rétractation;

c. la fourniture de biens confectionnés selon les spécifications du consommateur ou nettement personnalisés;

d. la fourniture de biens susceptibles de se détériorer ou de se périmer rapidement ;

e. la fourniture de biens scellés ne pouvant être renvoyés pour des raisons de protection de la santé ou d'hygiène et qui ont été descellés par le consommateur après la livraison;

f. la fourniture de biens qui, après avoir été livrés, et de par leur nature, sont mélangés de manière indissociable avec d'autres articles;

g. la fourniture de boissons alcoolisées dont le prix a été convenu au moment de la conclusion du contrat de vente, dont la livraison ne peut être effectuée qu'après 30 jours et dont la valeur réelle dépend de fluctuations sur le marché échappant au contrôle du professionnel;

h. la fourniture d'enregistrements audio ou vidéo scellés ou de logiciels informatiques scellés et qui ont été descellés après livraison;

i. la fourniture d'un journal, d'un périodique ou d'un magazine sauf pour les contrats d'abonnement à ces publications;

j. les contrats conclus lors d'une enchère publique;

k. la prestation de services d'hébergement autres qu'à des fins résidentielles, de transport de biens, de location de voitures, de restauration ou de services liés à des activités de loisirs si le contrat prévoit une date ou une période d'exécution spécifique;

l. la fourniture d'un contenu numérique non fourni sur un support matériel, si l'exécution a commencé avec l'accord préalable exprès du consommateur ou si un moyen fonctionnellement équivalent au droit de rétractation permet de garantir le consentement du consommateur avec la même efficacité, le consommateur ayant pris acte qu'il perdrait son droit de rétractation.

Article 52. Charge de la preuve

Sous réserve des exigences prescrites à l'Article 49, la charge de la preuve concernant le respect des obligations énoncées dans la présente sous-section incombe au professionnel.

Chapitre 5 - Responsabilité des prestataires intermédiaires

Section 1 : Principes généraux

Article 53. Absence d'obligation générale de surveillance

Pour la fourniture des services visés à l'Article 55, à l'Article 56 et à l'Article 57, les prestataires de services n'ont aucune obligation générale de surveiller les informations qu'ils transmettent ou stockent, ni aucune obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites.

Cette absence d'obligation générale de surveillance, telle que prévue au § 1er, n'empêche pas les prestataires de services de rechercher volontairement les faits ou les circonstances révélant les activités illicites, pour autant que soient préservés, conformément aux règles en vigueur, le secret des communications électroniques et la protection de la vie privée des personnes concernées.

Article 54. Obligation particulière de surveillance et obligation de collaboration

§ 1er. Le principe énoncé à l'Article 53 ne vaut que pour les obligations à caractère général. Il n'empêche pas les autorités judiciaires compétentes d'imposer une obligation temporaire de surveillance dans un cas spécifique, lorsque cette possibilité est prévue par une loi.

§ 2. Les prestataires visés à l'Article 54 ont l'obligation d'informer sans délai les autorités judiciaires ou administratives compétentes des activités illicites alléguées qu'exerceraient les destinataires de leurs services, ou des informations illicites alléguées que ces derniers fourniraient.

Sans préjudice d'autres dispositions légales ou réglementaires, les mêmes prestataires sont tenus de communiquer aux autorités judiciaires ou administratives compétentes, à leur demande, toutes les informations dont ils disposent et utiles à la recherche et à la constatation des infractions commises par leur intermédiaire.

En cas de non-respect, par le prestataire, des obligations prévues par le présent article, la sanction pénale suivante s'applique [à déterminer par l'Etat adoptant étant entendu que la sanction doit être effective, proportionnée et dissuasive].

Section 2 : Exonération de responsabilité pour certaines activités exercées par les prestataires intermédiaires

Article 55. Activité de simple transport

§ 1. En cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par le destinataire du service ou à fournir un accès au réseau de communication, le prestataire de services n'est pas responsable des informations transmises, à condition que le prestataire:

a. ne soit pas à l'origine de la transmission;

b. ne sélectionne pas le destinataire de la transmission

et

c. ne sélectionne et ne modifie pas les informations faisant l'objet de la transmission.

§ 2. Les activités de transmission et de fourniture d'accès visées au paragraphe 1 englobent le stockage automatique, intermédiaire et transitoire des informations transmises, pour autant que ce stockage serve exclusivement à l'exécution de la transmission sur le réseau de communication et que sa durée n'excède pas le temps raisonnablement nécessaire à la transmission.

Article 56. Activité de stockage sous forme de copie temporaire des données

En cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par un destinataire du service, le prestataire n'est pas responsable au titre du stockage automatique, intermédiaire et temporaire de cette information fait dans le seul but de rendre plus efficace la transmission ultérieure de l'information à la demande d'autres destinataires du service, à condition que:

a) le prestataire ne modifie pas l'information;

b) le prestataire se conforme aux conditions d'accès à l'information;

c) le prestataire se conforme aux règles concernant la mise à jour de l'information, indiquées d'une manière largement reconnue et utilisées par les entreprises;

d) le prestataire n'entrave pas l'utilisation licite de la technologie, largement reconnue et utilisée par l'industrie, dans le but d'obtenir des données sur l'utilisation de l'information

et

e) le prestataire agisse promptement pour rendre l'accès impossible à l'information stockée dès qu'il a effectivement connaissance du fait que l'information à l'origine de la transmission a été retirée du réseau ou du fait que l'accès à l'information a été rendu impossible, ou du fait qu'une autorité judiciaire ou administrative a ordonné de retirer l'information ou d'en rendre l'accès impossible et pour autant qu'il agisse dans le respect de la procédure prévue à l'Article 57, § 3.

Article 57. Activité d'hébergement

§ 1. En cas de fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service, le prestataire n'est pas responsable des informations stockées à la demande d'un destinataire du service à condition que:

a) le prestataire n'ait pas effectivement connaissance de l'activité ou de l'information illicites et, en ce qui concerne une demande en dommages et intérêts, n'ait pas connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente

ou

b) le prestataire, dès le moment où il a de telles connaissances, à l'issue de contrôles volontaires ou sur la base d'informations sérieuses communiquées par un tiers, agisse promptement pour retirer les informations ou rendre l'accès à celles-ci impossible.

Le prestataire ne bénéficie de l'exonération de responsabilité établie à l'alinéa précédent que s'il n'a joué aucun rôle actif à l'égard des données.

§ 2. Le paragraphe 1 ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle du prestataire.

§ 3. Lorsque le prestataire a une connaissance effective d'une activité ou d'une information illicite, il les communique sur le champ au [magistrat de l'ordre judiciaire désigné par l'Etat adoptant], qui prend les mesures utiles quant à la saisie des données. Aussi longtemps que ce magistrat n'a pris aucune décision concernant le copiage, l'inaccessibilité et le retrait des documents stockés dans un système informatique, le prestataire peut uniquement prendre des mesures visant à empêcher l'accès aux informations.

Si le magistrat désigné au § 3 ne s'est pas prononcé dans les quarante-huit heures suivant la communication qui lui a été faite, le prestataire conserve le bénéfice de l'exonération de responsabilité même s'il met fin aux mesures visant à empêcher l'accès aux informations et pour autant que l'illicéité ne soit pas manifeste.

Chapitre 6 – Sanctions

Article 58. Sanction civile

Dans les contrats conclus entre un professionnel et un consommateur, le juge peut annuler le contrat ou appliquer toute autre mesure proportionnée permettant d'éviter ou de réparer le préjudice subi par le consommateur suite à l'inobservation des dispositions du chapitre 4 du présent titre de la loi type.

Ces mesures sont d'application sans préjudice des autres sanctions susceptibles d'être mises en œuvre par le consommateur sans l'intervention des cours et tribunaux et en particulier :

– l'octroi au consommateur d'un droit de rétractation lorsque le professionnel ne l'a pas informé qu'il ne possédait pas un tel droit, en violation de l'Article 44 ou de l'Article 46 ;

– l'octroi au consommateur d'un droit de rétractation, aussi longtemps que le professionnel ne l'a pas informé qu'il disposait d'un tel droit, en violation de l'Article 44 ou de l'Article 46, sans possibilité pour le professionnel de réclamer une quelconque indemnité pour l'utilisation du bien ou du service pendant cette période.

[L'Etat adoptant peut également prendre d'autres sanctions civiles, pénales ou administratives, applicables en cas de violation des dispositions adoptées en vue de transposer les règles établies par la présente loi type, pour autant que ces sanctions soient effectives, proportionnées et dissuasives.

Il veille également à prendre les mesures nécessaires pour garantir leur mise en œuvre.]

Titre III – Dispositions diverses

Article 59. Codes de conduite

§ 1. L'État adoptant encourage:

a) l'élaboration, par les associations ou organisations d'entreprises, professionnelles ou de consommateurs ou par toute association représentative de la société civile, de codes de conduite au niveau communautaire, destinés à contribuer à la bonne application des dispositions de la présente loi type ;

b) l'accessibilité par voie électronique des codes de conduite dans les langues de l'Etat adoptant …;

c) la communication à l'Etat adoptant, par les associations ou organisations d'entreprises, professionnelles ou de consommateurs ou par toute association représentative de la société civile, de leurs évaluations de l'application de leurs codes de conduite et de leur impact sur les pratiques, les us ou les coutumes relatifs aux transactions électroniques ;

d) l'établissement de codes de conduite pour ce qui a trait à la protection des mineurs et de la dignité humaine.

§ 2. L'État adoptant encourage les associations ou les organisations représentant les consommateurs, ainsi qu'à toute association représentative de la société civile, à participer à l'élaboration et à l'application des codes de conduite ayant des incidences sur leurs intérêts et élaborés en conformité avec le paragraphe 1, point a). Le cas échéant, les associations représentant les personnes souffrant d'un handicap visuel et, de manière générale, les personnes plus vulnérables devraient être consultées afin de tenir compte de leurs besoins spécifiques.

Article 60. Règlement extrajudiciaire des litiges

§ 1er. L'État adoptant veille à ce que, en cas de désaccord entre un prestataire de services et le destinataire du service, sa législation ne fasse pas obstacle à l'utilisation des mécanismes de règlement extrajudiciaire pour le règlement des différends, disponibles dans le droit national, y compris par des moyens électroniques appropriés.

§ 2. L'Etat adoptant encourage les organes de règlement extrajudiciaire, notamment en ce qui concerne les litiges en matière de consommation, à fonctionner de manière à assurer les garanties procédurales appropriées pour les parties concernées.

Annexes au projet de Loi type relatif aux transactions électroniques

Annexe 1 : Exigences concernant les certificats qualifiés

Tout certificat qualifié doit comporter:

a) une mention indiquant que le certificat est délivré à titre de certificat qualifié;

b) l'identification du prestataire de service de certification ainsi que le pays dans lequel il est établi;

c) le nom du signataire ou un pseudonyme qui est identifié comme tel;

d) la possibilité d'inclure, le cas échéant, une qualité spécifique du signataire, en fonction de l'usage auquel le certificat est destiné;

e) des données afférentes à la vérification de signature qui correspondent aux données pour la création de signature sous le contrôle du signataire;

f) l'indication du début et de la fin de la période de validité du certificat;

g) le code d'identité du certificat;

h) la signature électronique avancée du prestataire de service de certification qui délivre le certificat;

i) les limites à l'utilisation du certificat, le cas échéant et

j) les limites à la valeur des transactions pour lesquelles le certificat peut être utilisé, le cas échéant.

Annexe 2 : Exigences concernant les prestataires de service de certification délivrant des certificats qualifiés

Les prestataires de service de certification doivent:

a) faire la preuve qu'ils sont suffisamment fiables pour fournir des services de certification;

b) assurer le fonctionnement d'un service d'annuaire rapide et sûr et d'un service de révocation sûr et immédiat;

c) veiller à ce que la date et l'heure d'émission et de révocation d'un certificat puissent être déterminées avec précision;

d) vérifier, par des moyens appropriés et conformes au droit national, l'identité et, le cas échéant, les qualités spécifiques de la personne à laquelle un certificat qualifié est délivré;

e) employer du personnel ayant les connaissances spécifiques, l'expérience et les qualifications nécessaires à la fourniture des services et, en particulier, des compétences au niveau de la gestion, des connaissances spécialisées en technologie des signatures électroniques et une bonne pratique des procédures de sécurité appropriées; ils doivent également appliquer des procédures et méthodes administratives et de gestion qui soient adaptées et conformes à des normes reconnues;

f) utiliser des systèmes et des produits fiables qui sont protégés contre les modifications et qui assurent la sécurité technique et cryptographique des fonctions qu'ils assument;

g) prendre des mesures contre la contrefaçon des certificats et, dans les cas où le prestataire de service de certification génère des données afférentes à la création de signature, garantir la confidentialité au cours du processus de génération de ces données;

h) disposer des ressources financières suffisantes pour fonctionner conformément aux exigences prévues par la présente loi type, en particulier pour endosser la responsabilité de dommages, en contractant, par exemple, une assurance appropriée;

i) enregistrer toutes les informations pertinentes concernant un certificat qualifié pendant le délai utile, en particulier pour pouvoir fournir une preuve de la certification en justice. Ces enregistrements peuvent être effectués par des moyens électroniques;

j) ne pas stocker ni copier les données afférentes à la création de signature de la personne à laquelle le prestataire de service de certification a fourni des services de gestion de clés;

k) avant d'établir une relation contractuelle avec une personne demandant un certificat à l'appui de sa signature électronique, informer cette personne par un moyen de communication durable des modalités et conditions précises d'utilisation des certificats, y compris des limites imposées à leur utilisation, de l'existence d'un régime volontaire d'accréditation et des procédures de réclamation et de règlement des litiges. Cette information, qui peut être transmise par voie électronique, doit être faite par écrit et dans une langue aisément compréhensible. Des éléments pertinents de cette information doivent également être mis à la disposition, sur demande, de tiers qui se prévalent du certificat;

l) utiliser des systèmes fiables pour stocker les certificats sous une forme vérifiable de sorte que:

- seules les personnes autorisées puissent introduire et modifier des données,

- l'information puisse être contrôlée quant à son authenticité,

- les certificats ne soient disponibles au public pour des recherches que dans les cas où le titulaire du certificat a donné son consentement et

- toute modification technique mettant en péril ces exigences de sécurité soit apparente pour l'opérateur.

Annexe 3 : Exigences pour les dispositifs sécurisés de création de signature électronique

1. Les dispositifs sécurisés de création de signature doivent au moins garantir, par les moyens techniques et procédures appropriés, que:

a) les données utilisées pour la création de la signature ne puissent, pratiquement, se rencontrer qu'une seule fois et que leur confidentialité soit raisonnablement assurée;

b) l'on puisse avoir l'assurance suffisante que les données utilisées pour la création de la signature ne puissent être trouvées par déduction et que la signature soit protégée contre toute falsification par les moyens techniques actuellement disponibles;

c) les données utilisées pour la création de la signature puissent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres.

2. Les dispositifs sécurisés de création de signature ne doivent pas modifier les données à signer ni empêcher que ces données soient soumises au signataire avant le processus de signature.

Annexe 4 : Recommandations pour la vérification sécurisée de la signature

Durant le processus de vérification de la signature, il convient de veiller, avec une marge de sécurité suffisante, à ce que:

a) les données utilisées pour vérifier la signature correspondent aux données affichées à l'intention du vérificateur;

b) la signature soit vérifiée de manière sûre et que le résultat de cette vérification soit correctement affiché;

c) le vérificateur puisse, si nécessaire, déterminer de manière sûre le contenu des données signées;

d) l'authenticité et la validité du certificat requis lors de la vérification de la signature soient vérifiées de manière sûre;

e) le résultat de la vérification ainsi que l'identité du signataire soient correctement affichés;

f) l'utilisation d'un pseudonyme soit clairement indiquée et

g) tout changement ayant une influence sur la sécurité puisse être détecté.

PROJET DE LOI-TYPE/DIRECTIVE PORTANT SUR LA LUTTE CONTRE LA CYBERCRIMINALITE

Préambule

CONSIDERANT que les avancés réalisés par les Etats d'Afrique centrale dans le secteur des technologies de l'information et de la communication (TIC) ainsi que les applications de la société de l'information constituent un enjeu majeur consistant pour les gouvernements à améliorer la qualité de vie des populations et à atteindre les Objectifs du Millénaire pour le Développement (OMD)

Que cependant la révolution numérique et l'interconnexion sans cesse croissante des réseaux numériques ont favorisé l'apparition d'une nouvelle forme de criminalité appelée « cybercriminalité » constituée de l'ensemble des infractions pénales ayant pour objet ou pour moyen les technologies de l'information et de la communication.

Notant que la cybercriminalité qui constitue une véritable menace pour la sécurité des réseaux, présente des particularités par rapport aux formes traditionnelles de délinquance pour être une criminalité marquée par l'immatérialité et la volatilité de ses activités, l'anonymat qu'elle offre à ses délinquants et l'internationalité de ses implications.

Considérant que l'analyse des cadres législatifs en vigueur dans les Etats d'Afrique centrale a montré que le passage de l'analogique au numérique a entrainé une inadaptation de la plupart des textes pénaux des Etats.

Qu'en effet, les dispositifs législatifs classiques, qui ne procèdent pas d'une appréhension globale de la criminalité du cyberespace, peinent à saisir l'immatérialité et l'internationalité des comportements des cybercriminels.

Que pourtant, à l'exception de quelques Etats qui ont légiféré sur la cybercriminalité, les rares réglementations applicables dans ces Etats traitent de questions spécifiques aux communications électroniques, aux télécommunications et aux incidents et moyens de paiement électroniques.

Que l'audit des édifices pénaux des Etats a révélé l'existence de situations de vides juridiques et d'inadaptations juridiques constituant autant de « paradis informatiques » pour les cybercriminels.

Considérant le cyberespace n'est pas une zone de non droit rebelle à toute activité régulatrice de ses contenus, il a paru nécessaire d'élaborer et de mettre en œuvre dans les Etats d'Afrique centrale une véritable stratégie de lutte contre la cybercriminalité par la mise en place d'un cadre législatif propice au traitement efficace de ce phénomène.

Que cette option de politique criminelle répond aux enjeux majeurs de la dématérialisation des instruments répressifs, de la recherche de la preuve et de la détermination et de l'identification des personnes responsables dans l'univers numérique.

Considérant que sous l'angle purement pénal, la stratégie d'expansion du champ de la politique criminelle élaborée a permis d'attirer les comportements cybercriminels dans le champ pénal.

Qu'en droit pénal substantiel, la modernisation des infractions pénales a été recherchée à travers l'adoption d'infractions nouvelles spécifiques aux TIC et par l'adaptation des infractions classiques aux TIC.

Que le mouvement d'adoption d'infractions nouvelles spécifiques aux TIC a comblé les vides législatifs. Il a été dicté par le besoin de protection pénale des systèmes informatiques et des données informatiques, la sanction de la pornographie enfantine et des actes racistes et xénophobe. La pénalisation du spamming, de l'usurpation d'identité numérique et du copiage frauduleuse de données informatiques constitue à cet égard des innovations de présente loi-type ;

Que la politique d'adaptation des infractions classiques aux TIC s'est articulée autour de l'intégration des données informatiques dans l'objet des infractions contre les biens (escroquerie, recel et abus de confiance) et de la prise en compte des moyens de communication électroniques dans les moyens de commission des infractions de presse.

Que le développement du phénomène de l'escroquerie en ligne devenu un véritable fléau en Afrique a justifié l'érection de l'escroquerie en ligne en infraction aggravé.

Que sous l'angle de la responsabilité pénale, le principe de la responsabilité pénale des personnes morales est consacré en matière de cybercriminalité pour prendre en compte la diversité des entités juridiques pouvant voir leur responsabilité pénale engagée du fait de la commission de cyberinfractions.

Considérant qu'en procédure pénale, l'amélioration du processus de répression de la cybercriminalité s'est fondée sur une extension des pouvoirs d'investigation des autorités judiciaires en charge de la recherche de la preuve des cyberinfractions. D'une part, l'aménagement des mécanismes procéduraux classiques a permis l'admission de la perquisition électronique et de la saisie électronique ainsi que l'encadrement de l'admission de la preuve électronique en matière pénale. D'autre part, il a été envisagé l'institution de nouvelles techniques de recherche de preuve dans le cyberespace, à savoir la conservation rapide des données informatiques stockées, l'injonction de produire, l'interception de données relatives au contenu, et la collecte en temps réel des données relatives au trafic . En outre, le pouvoir donné à l'officier de police judiciaire sur autorisation du juge, d'utiliser un logiciel à distance ainsi que la mis en place dans les Etats d'une cellule de lutte conte la cybercriminalité (CLC) visent à faciliter la recherche et collecte de la preuve en matière de cybercriminalité.

Que cependant, l'extension des pouvoirs d'investigation des organes judiciaires nécessitée par l'impératif de cybersécurité ne devra pas entraver les droits et libertés des individus garanties par les conventions internationales, la Constitution et les lois nationales.

Considérant que la cybercriminalité constitue un phénomène criminel international ignorant les frontières des Etats, il est nécessaire pour les Etats d'Afrique centrale de renforcer leur coopération juridique et judiciaire en vue de mieux lutter contre les comportements cybercriminels.

Que les États Membres se doivent d'intensifier leur collaboration dans le cadre de la lutte contre les cybermenaces et de nouer des relations de coopération avec les Etats tiers, les unités spécialisées dans la lutte contre la cybercriminalité et d'autres autorités et organisations compétentes à l'échelle internationale, comme Interpol. .

Qu'à cet égard, les partenariats existants au niveau international, à l'image de l'UIT IMPACT, se présentent comme un cadre de coopération internationale appropriée en matière de lutte contre les cybermenaces.

Convaincus cependant qu'au-delà des aspects purement juridiques du traitement de la cybercriminalité, il est nécessaire d'intégrer dans la lutte contre ce phénomène des enjeux liés à la cybersécurité combinant les réponses étatiques, organisationnelles et techniques en vue de l'édification d'une société de l'information sécurisée.

Qu'à cet égard, la promotion de la culture de la cybersécurité au niveau des pouvoirs publics, des entreprises, de la société civile et des citoyens devra mettre l'accent sur la sécurité des informations circulant dans les systèmes et des réseaux électroniques, la confiance dans les transactions électroniques ainsi que la protection de la vie privée et des mineurs dans le cyberespace.

Que l'approche de cybersécurité a permis de mettre à la charge de l'Etat, en collaboration avec les parties prenantes l'obligation d'élaborer et de mettre en œuvre une politique nationale de cybersécurité et d'instituer des structures nationales de cybersécurité (Conseil national de la cybersécurité, agence nationale de la cybersécurité) chargées de la régulation des activités liées à la sécurité du cyberespace.

Que la politique de cybersécurité devra avoir pour axes stratégiques la promotion du comportement responsable dans le cyberespace, la sensibilisation des acteurs et des citoyens aux dangers que recèlent des réseaux numériques, le développement de la formation aux TIC ainsi que le renforcement de la coopération public-privé à la lutte contre les cybercontenus illicites.

Considérant que le dispositif de financement des activités de cybersécurité prévu, à travers la création du fonds spécial des activités de la cybersécurité, contribue à rendre plus effective dans les Etats d'Afrique centrale contre la cybercriminalité qui constitue une sérieuse menace pour la sécurité des réseaux et le développement d'une société de l'information à dimension humaine ouverte et inclusive.

TITRE I : DISPOSITIONS GENERALES

Chapitre I : Objet de la Loi type/ Directive

Article 1. Objet

La présente Loi type fixe le cadre juridique de la lutte contre la cybercriminalité dans les Etats Membres de la CEEAC /CEMAC dans le respect des droits et des libertés des individus.

Chapitre II : Définitions

Article 2. Terminologie

Au sens de la présente Loi type :

1. l'expression **« système informatique »** désigne: tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données;

2. l'expression **«données informatiques»** désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction;

3. l'expression **« confidentialité »** désigne: l'état de sécurité permettant de garantir le secret des informations et ressources stockées dans les réseaux et systèmes de communication électroniques, systèmes d'information ou des équipements terminaux, afin de prévenir la divulgation non autorisée d'informations à des tiers, par la lecture, l'écoute, la copie illicite d'origine intentionnelle ou accidentelle durant leur stockage, traitement ou transfert ;

4. l'expression **« cybersécurité »** désigne un ensemble des mesures de prévention, de protection et de dissuasion d'ordre technique, organisationnel, juridique, financier, humain, procédural et autres actions permettant d'atteindre les objectifs de sécurisation des réseaux de communications électroniques, des systèmes d'information et pour la protection de la vie privée des personnes ;

5. l'expression **« disponibilité »** désigne l'état de sécurité permettant de garantir que les informations et ressources des réseaux de communications électroniques, des systèmes d'information ou des équipements terminaux soient accessibles et utilisables selon les besoins ;

6. l'expression **« intégrité »** désigne l'état de sécurité assurant qu'un réseau de communications électroniques, système d'information ou équipement terminal qui est demeuré intact et que les ressources et informations y stockées n'ont pas été altérées, modifiées ou détruites, d'une façon intentionnelle ou accidentelle, de manière à assurer leur exactitude, leur fiabilité et leur pérennité ;

7. l'expression **«pornographie enfantine»** comprend toute donnée quelle qu'en soit la nature ou la forme ou le support représentant:

a. un mineur se livrant à un comportement sexuellement explicite;

b. une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite;

c. des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.

8. l'expression **« mineur »** désigne toute personne âgée de moins de dix huit (18) ans au sens de la Convention des Nations Unies sur les droits de l'enfant ou toute personne qui apparaît comme mineur ;

9. l'expression **« matériel raciste et xénophobe »** désigne tout matériel écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence, contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments, ou qui incite à de tels actes ;

10. l'expression **«données relatives au trafic»** désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

11. l'expression **« prestataire de service de sécurité »** désigne toute personne physique ou morale qui exerce des activités liées à la sécurité électronique notamment, la délivrance et la gestion des certificats électroniques ou la fourniture d'autres services liés aux signatures électroniques, la création des logiciels de sécurité, la surveillance des réseaux, la détection d'intrusions, l'audit des réseaux et systèmes de sécurité.

12. l'expression **« technologies de l'information et de la communication » (TIC)** désigne les technologies employées pour recueillir, stocker, utiliser et envoyer des informations ainsi que celles qui impliquent l'utilisation des ordinateurs ou de tout système de communication y compris de télécommunication ;

TITRE II : MESURES A PENDRE AU NIVEAU NATIONAL

CHAPITRE I : DROIT PENAL SUBSTANTIEL

Section I : Des infractions spécifiques aux TIC

Sous-section I : Des atteintes aux systèmes informatiques

Paragraphe I : atteintes à la confidentialité des systèmes informatiques

Article 3 : Accès frauduleux à un système informatique

Une personne qui accède ou tente d'accéder frauduleusement à tout ou partie d'un système informatique commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines.

Article 4 : Maintien frauduleux dans un système informatique

Une personne qui se maintient ou tente de se maintenir frauduleusement dans tout ou partie d'un système informatique commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines.

Paragraphe II: atteintes à l'intégrité des systèmes informatiques

Article 5 : Entrave ou action de fausser le fonctionnement du système

Une personne qui frauduleusement entrave, tente d'entraver, fausse ou tente de fausser le fonctionnement d'un système informatique commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines.

Paragraphe III: Introduction frauduleuse de données informatiques dans un système informatique

Article 6 : Introduction frauduleuse de données dans un système

Une personne qui introduit ou tente d'introduire frauduleusement des données informatiques dans un système informatique commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines.

Sous-section II : Des atteintes aux données informatiques

Article 7 : Interception frauduleuse de données informatiques

Une personne qui intercepte ou tente d'intercepter frauduleusement 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 commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines.

Article 8 : Atteintes à l'intégrité des données informatiques

Une personne qui endommage ou tente d'endommager, efface ou tente d'effacer, détériore ou tente de détériorer, altère ou tente d'altérer, supprime ou tente de supprimer frauduleusement des données informatiques commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines.

Sous-section III : Des autres abus

Article 9 : Des abus de dispositifs

Une personne qui produit, vend, importe, détient, diffuse, offre, cède ou met à disposition :

a. un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions visées par les Articles 3 à 8 ci-dessus;

b. un mot de passe, un code d'accès ou des données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les Articles 3 à 8 ci-dessus commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines.

Article 10 : De l'association de malfaiteurs informatiques

Une personne qui participe à une association formée ou à une entente établie en vue de préparer ou de commettre une ou plusieurs des infractions prévues par la présente Loi-type commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines.

Sous-Section IV : Des infractions informatiques

Article 11 : Falsification informatique

Une personne qui introduit ou tente d'introduire, altère ou tente d'altérer efface ou tente d'effacer, supprime ou tente de supprimer frauduleusement des données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines.

Article 12 : Usage des données falsifiées

Une personne qui, en connaissance de cause, fait usage des données obtenues dans les conditions énoncées par l'Article 11 ci-dessus commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines.

Article 13 : Fraude informatique

Une personne qui, intentionnellement, et sans droit cause un préjudice patrimonial à autrui ou tente de causer un préjudice patrimonial à autrui :

a. par toute introduction, altération, effacement ou suppression de données informatiques;

b. par toute forme d'atteinte au fonctionnement d'un système informatique,

dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines.

Sous-section V : Des infractions relatives au contenu

Paragraphe I : De la pornographie enfantine

Article 14 : Production, diffusion, offre de pornographie enfantine

Une personne qui produit en vue de sa diffusion, tente de produire en vue de la vente, offre, met à disposition, diffuse ou tente de diffuser de la pornographie enfantine par le biais d'un système informatique commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines.

Article 15 : Importation, exportation de pornographie enfantine

Une personne qui se procurer ou procure à autrui, importe ou fait importer, exporter ou fait exporter de la pornographie enfantine par le biais d'un système informatique commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines.

Article 16 : Possession de pornographie enfantine

Une personne qui possède intentionnellement de la pornographie enfantine dans un système informatique ou dans un moyen quelconque de stockage de données informatiques commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines.

Article 17 : Facilitation de l'accès des mineurs à des contenus pornographiques

Une personne qui facilite l'accès des mineurs à des images, des documents, du son ou une représentation présentant un caractère de pornographie commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines

Article 18 : Sollicitation d'enfants à des fins sexuelles

Un adulte qui propose intentionnellement, par le biais des technologies de communication et d'information, une rencontre à un enfant mineur, dans le but de commettre à son encontre une des infractions prévues par les Articles 14, 15 et 16 ci-dessus, commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines

Lorsque la proposition sexuelle a été suivie d'actes matériels conduisant à ladite rencontre, l'auteur commet une infraction aggravé punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines

Paragraphe II : Des actes racistes et xénophobe par le biais d'un système informatique

Article 19 : Diffusion de matériel raciste et xénophobe

Une personne qui crée, télécharge, diffuse ou met à disposition sous quelque forme que ce soit, par le biais d'un système informatique du matériel raciste et xénophobe commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines.

Article 20 : Menace avec une motivation raciste et xénophobe

Une personne qui profère une menace par le biais d'un système informatique, de commettre une infraction pénale telle que définie par le droit national, envers une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion dans la mesure où cette appartenance sert de prétexte à l'un ou l'autre de ces éléments, ou un groupe de personnes qui se distingue par une de ces caractéristiques commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines.

Article 21 : Insulte avec une motivation raciste et xénophobe

Une personne qui profère une insulte par le biais d'un système informatique envers une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion ou l'opinion politique dans la mesure où cette appartenance sert de prétexte à l'un ou l'autre de ces éléments, ou un groupe de personnes qui se distingue par une de ces caractéristiques commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines.

Article 22 : Négation, minimisation grossière, approbation ou justification du génocide ou des crimes contre l'humanité

Une personne qui diffuse ou met à disposition par le biais d'un système informatique des données qui nient, minimisent de manière grossière, approuvent ou justifient des actes constitutifs de génocide ou de crimes contre l'humanité tels que définis par le droit international et reconnus comme tels par une décision finale et définitive d'un tribunal national ou d'un tribunal international établi par des instruments internationaux pertinents et dont la juridiction est reconnue commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines.

Paragraphe III : Spamming

Article 23 : Spamming

1. Une personne qui, de manière intentionnelle et sans excuse ou justification légitime

a. déclenche intentionnellement la transmission de courriers électroniques multiples à partir ou par l'intermédiaire d'un système informatique ou

b. utilise un système informatique protégé pour relayer ou retransmettre des courriers électroniques multiples dans l'intention de tromper ou d'induire en erreur, quant à l'origine de ces messages les destinataires ou tout prestataire de services de courriers électroniques ou de services internet ou

c. falsifie matériellement les informations se trouvant dans les en-têtes de messages électroniques multiples et déclenche intentionnellement la transmission des messages,

d. commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines.

2. Un pays peut définir des critères plus restrictifs en ce qui concerne la criminalisation de la transmission de courriers électroniques multiples dans le cadre de relations clients ou commerciales. Un pays peut décider de ne pas criminaliser le comportement décrit à l'alinéa 1e du présent article, si d'autres recours efficaces existent.

Paragraphe IV : De l'usurpation d'identité numérique

Article 24 :

Une personne qui usurpe l'identité d'un tiers ou une ou plusieurs données permettant de l'identifier, en vue de troubler sa tranquillité ou celle d'autrui ou de porter atteinte à son honneur à sa considération ou à ses intérêts commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines.

Sous-section VI : De la complicité

Article 25.

Une personne qui intentionnellement commet un acte de complicité en vue de la perpétration d'une des infractions prévues par la présente loi type, dans l'intention qu'une telle infraction soit perpétrée, commet une infraction punissable des mêmes peines que celles prévues pour l'infraction principale.

Section II : De l'adaptation des infractions classiques aux TIC

Sous-section I : Des infractions contre les biens

Article 26 : Copiage frauduleuse de données informatiques

Une personne qui copie ou tente de copier frauduleusement des données informatiques au préjudice d'un tiers commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines.

Article 27 : Escroquerie portant sur des données informatiques

Une personne qui, soit en faisant usage de faux noms ou de fausses qualités, soit en employant des manœuvres frauduleuses quelconques, aura obtenu la remise ou aura tenté d'obtenir la remise de données informatiques et aura, par un de ces moyens, escroqué ou aura tenté d'escroquer la totalité ou partie de la fortune d'autrui commet une infraction punissable, sur déclaration de culpabilité, des mêmes peines que celles prévues pour l'escroquerie portant sur des biens corporels.

Article 28 : Abus de confiance portant sur des données informatiques

Une personne qui, ayant reçu des propriétaires, possesseurs, ou détenteurs, des données informatiques à titre de louage, de dépôt, de mandat, de nantissement, de prêt à usage ou pour un travail salarié ou non salarié, n'aura pas, après simple mise en demeure, exécuté son engagement de les rendre ou représenter ou d'en faire un usage ou un emploi déterminé, commet une infraction punissable, sur déclaration de culpabilité, des mêmes peines que celles prévues pour l'abus de confiance portant sur des biens corporels.

Article 29 : Recel portant sur des données informatiques

Une personne qui, sciemment, aura recelé, en tout ou en partie, des données informatiques enlevées, détournées ou obtenues à l'aide d'un crime ou d'un délit commet une infraction punissable, sur déclaration de culpabilité, des mêmes peines que celles prévues pour le recel portant sur des biens corporels

Article 30 : Escroquerie en ligne

Une personne qui, soit en faisant usage de faux noms ou de fausses qualités, soit en employant des manœuvres frauduleuses quelconques, se sera fait remettre ou délivrer, ou aura tenté de se faire remettre ou délivrer des fonds des meubles ou des obligations, dispositions, billets, promesses, quittances ou décharges par le biais d'un système informatique ou d'un réseau de communication électronique et aura, par un de ces moyens, escroqué ou tenté d'escroquer la totalité ou partie de la fortune d'autrui commet une infraction aggravée punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines.

Sous-section II : Des infractions de presse

Article 31 : Des moyens de communication électronique

Une personne qui commet une infraction de presse, notamment une diffamation, une injure publique, une apologie de crime, par le biais d'un moyen de communication électronique public, commet une infraction punissable, sur déclaration de culpabilité, des mêmes peines que celles prévues pour les infractions de presse commises par d'autres moyens.

Section III : De la responsabilité pénale des personnes morales

Article 32 : Principe de la responsabilité pénale des personnes morales

1. Les personnes morales autres que l'Etat, les collectivités locales et les établissements publics sont responsables des infractions prévue par la présente Loi-type/ Directive, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé:

a. sur un pouvoir de représentation de la personne morale;

b. sur une autorité pour prendre des décisions au nom de la personne morale;

c. sur une autorité pour exercer un contrôle au sein de la personne morale.

2. Outre les cas déjà prévus à l'alinéa précédent du présent article 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 la commission des infractions prévues par la présente loi-type pour le compte de ladite personne morale par une personne physique agissant sous son autorité.

3. La responsabilité des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits.

Article 33 : Des peines encourues par les personnes morales

Les peines encourues par les personnes morales sont :

1. l'amende dont le taux maximum est égal au quintuple de celui prévu pour les personnes physiques par la loi qui réprime l'infraction ;

2. la dissolution, lorsque la personne morale a été créée 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 (5) ans, détournée de son objet pour commettre les faits incriminés ;

3. l'interdiction à titre définitif ou pour une durée de cinq (5) 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 (5) ans au plus d'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

5. l'exclusion des marchés publics à titre définitif ou pour une durée de cinq (5) ans au plus ;

6. l'interdiction à titre définitif ou pour une durée de cinq (5) ans au plus de faire appel public à l'épargne ;

7. l'interdiction pour une durée de cinq (5) ans au plus d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès 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 ;

9. l'affichage de la décision prononcée ou la diffusion de celle-ci soit par la presse écrite soit par tout moyen de communication au public par voie électronique.

CHAPITRE II : DROIT PENAL PROCEDURAL

Section I : De l'aménagement des techniques classiques de recherche de la preuve

Article 34 : Perquisition informatique

1. Lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données informatiques sur son territoire, sont utiles à la manifestation de la vérité, le (juge procureur) peut perquisitionner, accéder ou ordonner de perquisitionner ou d'accéder au système informatique ou à une partie de celui-ci ou au support de stockage informatique.

2. Lorsque le (juge/procureur) perquisitionne, accède ou ordonne la perquisition ou l'accès d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément à l'alinéa précédent du présent article et a des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, le (juge/procureur) peut étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système.

Article 35 : Saisie informatique

1. Lorsque le (juge/procureur) découvre dans un système informatique des données informatiques qui sont utiles à la manifestation de la vérité, mais que la saisie du support ne paraît pas souhaitable, il peut saisir, ordonner la saisie ou obtenir d'une façon similaire des données informatiques pour lesquelles l'accès a été réalisé en application de l'Article précédent.

2. Cette mesure inclut les prérogatives suivantes:

a. saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage informatique;

b. réaliser et conserver une copie de ces données informatiques;

c. préserver l'intégrité des données informatiques stockées pertinentes;

d. rendre inaccessibles ou enlever ces données informatiques du système informatique consulté.

3. Le (juge/procureur) peut ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures prévues par le présent article et par l'article précédent.

Article 36 : De l'admissibilité de la preuve électronique en matière pénale

La preuve électronique en matière pénale est admise à établir les infractions à la loi pénale sous réserve des conditions suivantes :

D'une part, qu'elle soit apportée au cours des débats et discutée devant le juge. D'autre part, que puisse être dûment identifiée la personne dont elle émane et qu'elle soit établie et conservée dans des conditions de nature à garantir son intégrité.

Section II : L'institution de nouvelles méthodes de recherche de la preuve

Article 37 : Conservation rapide de données informatique stockées

1. Si les nécessités de l'information l'exigent, notamment lorsqu'il y a des raisons de penser que des données informatiques stockées dans un système informatique sont particulièrement susceptibles de perte ou de modification, le juge, le procureur ou l'officier de police judiciaire peut faire injonction à toute personne de conserver et de protéger l'intégrité des données en sa possession ou sous son contrôle, pendant une durée de deux ans maximum, pour la bonne marche des investigations judiciaires

2. Le gardien des données ou une autre personne chargée de conserver celles-ci est tenu de garder le secret sur la mise en œuvre desdites procédures.

Article 38 : Injonction de produire

Le juge/procureur peut ordonner:

a. à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique; et

b. à un fournisseur de services offrant des prestations sur le territoire, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

Article 39 : Interception de données relatives au contenu

1. Le (juge/procureur), pour des infractions définies par la présente loi, peut utiliser les moyens techniques appropriés pour collecter ou enregistrer en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique ou obliger un fournisseur de services, dans le cadre de ses capacités techniques à collecter ou à enregistrer, en application de moyens techniques existant sur son territoire ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer lesdites données.

2. Le fournisseur de services est tenu de garder le secret sur les informations reçues.

Article 40 : Collecte en temps réel des données relatives au trafic

Le (juge/procureur) peut collecter enregistrer ou ordonner la collecte ou l'enregistrement par l'application de moyens techniques existant sur son territoire ou à obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes:

1. à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou

2. à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

Le fournisseur de services est tenu de garder le secret le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.

Article 41 : Utilisation d'un logiciel à distance

Si un juge ou un procureur est convaincu que dans le cadre d'une enquête concernant une infraction prévue par la présente loi, il y a des motifs raisonnables de croire que des preuves essentielles ne peuvent pas être collectées par l'application d'autres instruments énumérés au chapitre II, du titre II de la présente loi type, il peut , sur demande, autoriser un officier de police à utiliser un logiciel à distance et l'installer dans le système informatique de la personne mise en cause afin de recueillir les éléments de preuve pertinents. La demande doit contenir les informations suivantes :

a. la personne mise en cause, si possible avec nom et adresse;
b. la description du système informatique ciblé;
c. la description de la mesure envisagée, l'étendue et la durée de l'utilisation ;
d. les raisons de la nécessité de l'utilisation du logiciel.

Article 42 : Refus d'assistance

Une personne, autre que le mis en cause qui omet intentionnellement sans excuse légitime ou justification de se conformer à une réquisition judiciaire donnée commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines.

Article 43 : Divulgation d'informations de l'enquête

Un fournisseur de service qui reçoit une injonction, dans le cadre d'une enquête criminelle, qui stipule explicitement que la confidentialité doit être maintenue ou qu'elle résulte de la loi et qui intentionnellement sans excuse légitime ou justification divulgue les informations relatives à l'enquête commet une infraction punissable, sur déclaration de culpabilité, d'un emprisonnement de (….) et d'une amende de (…) ou de l'une de ces deux peines.

Article 44 : De la cellule nationale de lutte contre la cybercriminalité (CLC)

Il est créé une cellule de lutte contre la cybercriminalité dotée de l'autonomie financière et constituée d'un personnel ayant des compétences juridiques et techniques en matière de lutte contre la cybercriminalité

La cellule de lutte contre la cybercriminalité est composée des magistrats, d'officiers de police judiciaire et d'informaticiens et de techniciens notamment.

Cette cellule doit veiller à établir un partenariat avec les prestataires techniques, notamment les fournisseurs d'accès et d'hébergement en vue de rendre efficace la lutte contre la cybercriminalité et de s'assurer de la participation de ces intermédiaires techniques à la lutte contre les contenus illicites.

La cellule de lutte contre la cybercriminalité a une compétence sur toute l'étendue du territoire national.

Elle a pour mission de rassembler les preuves des infractions prévues par la présente Loi type, de rechercher et d'identifier leurs auteurs et de les déférer devant les autorités judiciaires compétentes.

La Cellule de lutte contre la cybercriminalité sert de point de contact national en vue de réagir aux menaces de sécurité liées aux TIC au niveau national, régional et international.

Un décret précise la composition et l'organisation de la cellule de lutte contre la cybercriminalité

TITRE III : DE LA COOPERATION JUDICIAIRE INTERNATIONALE

Chapitre I : Principes généraux

Section I : Principes généraux relatifs à la coopération internationale

Article 45 : Principe de coopération

Les Etats Membres coopèrent les unes avec les autres, conformément aux dispositions du présent titre, en application des instruments internationaux pertinents sur la coopération internationale en matière pénale, des arrangements reposant sur des législations uniformes ou réciproques et de leur droit national, dans la mesure la plus large possible, aux fins d'investigations ou de procédures concernant les infractions pénales prévues par la présente Loi-type ou pour recueillir les preuves, sous forme électronique, d'une infraction pénale.

Section II : Principes relatifs à l'extradition

Article 46 : Infractions extraditionnelles

Le présent article s'applique à l'extradition entre les Etats pour les infractions pénales prévues par la présente Loi type, à condition qu'elles soient punissables dans la législation des deux Etats concernées par une peine privative de liberté pour une période maximale d'au moins un an, ou par une peine plus sévère.

Lorsqu'il est exigé une peine minimale différente, sur la base d'un traité d'extradition tel qu'applicable entre deux ou plusieurs partie ou d'un arrangement reposant sur des législations uniformes ou réciproques, la peine minimale prévue par ce traité ou cet arrangement s'applique.

Les infractions pénales prévues par la présente Loi type sont considérées comme incluses en tant qu'infractions pouvant donner lieu à extradition dans tout traité d'extradition existant entre ou parmi les Etats. Les Etats Membres s'engagent à inclure de telles infractions comme infractions pouvant donner lieu à extradition dans tout traité d'extradition pouvant être conclu entre ou parmi elles.

Lorsqu'une Partie conditionne l'extradition à l'existence d'un traité et reçoit une demande d'extradition d'une autre Partie avec laquelle elle n'a pas conclu de traité d'extradition, elle peut considérer la présente Loi type comme fondement juridique pour l'extradition au regard de toute infraction pénale prévues par la présente Loi type.

Les Etats qui ne conditionnent pas l'extradition à l'existence d'un traité reconnaissent les infractions pénales mentionnées à la présente Loi- comme des infractions pouvant donner lieu entre elles à l'extradition.

L'extradition est soumise aux conditions prévues par le droit interne de l'Etat requis ou par les traités d'extradition en vigueur, y compris les motifs pour lesquels la Partie requise peut refuser l'extradition.

Article 47 : Extrader ou punir

Si l'extradition pour une infraction pénale prévue par la présente Loi type est refusée uniquement sur la base de la nationalité de la personne recherchée ou parce que l'Etat requis s'estime compétente pour cette infraction, l'Etat requis soumet l'affaire, à la demande de l'Etat requérant, à ses autorités compétentes aux fins de poursuites, et rendra compte, en temps utile, de l'issue de l'affaire à l'Etat requérant. Les autorités en question prendront leur décision et mèneront l'enquête et la procédure de la même manière que pour toute autre infraction de nature comparable, conformément à la législation de cet Etat.

Section III : Principes généraux relatifs à l'entraide

Article 48 : Allégement de la demande d'entraide

Chaque Etat Membre peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'Etat requis l'exige. L'Etat requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.

Sauf disposition contraire, l'entraide est soumise aux conditions fixées par le droit interne de l'Etat requis ou par les traités d'entraide applicables, y compris les motifs sur la base desquels l'Etat requis peut refuser la coopération.

Article 49 : De la double incrimination

Lorsque, conformément aux dispositions du présent chapitre, l'Etat requis est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de l'Etat requérant.

Article 50 : Information spontanée

Un Etat Membre peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à un autre Etat des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider l'Etat destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cet Etat au titre du présent titre.

Avant de communiquer de telles informations, l'Etat qui les fournit peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions. Si l'Etat destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Etat, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si l'Etat destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières.

Chapitre II : Dispositions spécifiques

Section 1 : Entraide en matière de mesures provisoires

Article 51 : Conservation rapide de données informatiques stockées

1. Une Partie peut demander à une autre Partie d'ordonner ou d'imposer d'une autre façon la conservation rapide de données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, et au sujet desquelles la Partie requérante a l'intention de soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation desdites données.

2. Une demande de conservation faite en application du paragraphe 1 doit préciser:

a. l'autorité qui demande la conservation;

b. l'infraction faisant l'objet de l'enquête ou de procédures pénales et un bref exposé des faits qui s'y rattachent;

c. les données informatiques stockées à conserver et la nature de leur lien avec l'infraction;

d. toutes les informations disponibles permettant d'identifier le gardien des données informatiques stockées ou l'emplacement du système informatique;

e. la nécessité de la mesure de conservation; et

f. le fait que la Partie entend soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données informatiques stockées.

3. Après avoir reçu la demande d'une autre Partie, la Partie requise doit prendre toutes les mesures appropriées afin de procéder sans délai à la conservation des données spécifiées, conformément à son droit interne. Pour pouvoir répondre à une telle demande, la double incrimination n'est pas requise comme condition préalable à la conservation.

4. Une Partie qui exige la double incrimination comme condition pour répondre à une demande d'entraide visant la perquisition ou l'accès similaire, la saisie ou l'obtention par un moyen similaire ou la divulgation des données stockées peut, pour des infractions prévues par la présente Loi type, se réserver le droit de refuser la demande de conservation au titre du présent article dans le cas où elle a des raisons de penser que, au moment de la divulgation, la condition de double incrimination ne pourra pas être remplie.

5. En outre, une demande de conservation peut être refusée uniquement:

a. si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou

b. si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à d'autres intérêts essentiels.

6. Lorsque la Partie requise estime que la conservation simple ne suffira pas à garantir la disponibilité future des données, ou compromettra la confidentialité de l'enquête de la Partie requérante, ou nuira d'une autre façon à celle-ci, elle en informe rapidement la Partie requérante, qui décide alors s'il convient néanmoins d'exécuter la demande.

7. Toute conservation effectuée en réponse à une demande visée au paragraphe 1 sera valable pour une période d'au moins soixante jours afin de permettre à la Partie requérante de soumettre une demande en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données.

Après la réception d'une telle demande, les données doivent continuer à être conservées en attendant l'adoption d'une décision concernante la demande.

Article 52 : Divulgation rapide de données conservées

1. Lorsque, en exécutant une demande de conservation de données relatives au trafic concernant une communication spécifique formulée en application de l'Article 51, la Partie requise découvre qu'un fournisseur de services dans un autre Etat a participé à la transmission de cette communication, la Partie requise divulgue rapidement à la Partie requérante une quantité suffisante de données concernant le trafic, aux fins d'identifier ce fournisseur de services et la voie par laquelle la communication a été transmise.

2. La divulgation de données relatives au trafic en application du paragraphe 1 peut être refusée seulement:

a. si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou

b. si elle considère que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

Section II: Entraide aux fins d'investigation

Article 53 : Entraide concernant l'accès aux données stockées

Un Etat Membre peut demander à un autre Etat Membre de perquisitionner ou d'accéder de façon similaire, de saisir ou d'obtenir de façon similaire, de divulguer des données stockées au moyen d'un système informatique se trouvant sur le territoire de cet autre Etat.

L'Etat requis satisfait à la demande en appliquant les instruments internationaux, les arrangements et en se conformant aux dispositions pertinentes du présent titre.

La demande doit être satisfaite aussi rapidement que possible dans les cas suivants:

– il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification; ou

– les instruments, arrangements et législations mentionnés à l'Article 45 de la présente Loi type prévoient une coopération rapide.

Article 54 : Entraide dans la collecte en temps réel de données relatives au trafic

Les Etats Membres s'accordent l'entraide dans la collecte en temps réel de données relatives au trafic, associées à des communications spécifiées sur leur territoire, transmises au moyen d'un système informatique. Sous réserve des dispositions de l'alinéa 2, cette entraide est régie par les conditions et les procédures prévues en droit interne.

Chaque Etat accorde cette entraide au moins à l'égard des infractions pénales pour lesquelles la collecte en temps réel de données concernant le trafic serait disponible dans une affaire analogue au niveau interne.

Article 55 : Entraide en matière d'interception de données relatives au contenu

Les Etats s'accordent l'entraide, dans la mesure permise par leurs traités et lois internes applicables, pour la collecte ou l'enregistrement en temps réel de données relatives au contenu de communications spécifiques transmises au moyen d'un système informatique.

Section III : Du réseau 24/7

Article 56.

Chaque Etat Membre désigne un point de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes:

– apport de conseils techniques;

– conservation des données, conformément aux Articles 51 et 52;

– recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.

Le point de contact d'un Etat aura les moyens de correspondre avec le point de contact d'une autre Etat selon une procédure accélérée.

Si le point de contact désigné par un Etat ne dépend pas de l'autorité ou des autorités de cet Etat responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités, selon une procédure accélérée.

Chaque Etat fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.

TITRE III : AUTRES MESURES DE CYBERSECURITE

Chapitre I : Cadre de la cybersécurité nationale

Article 57 : De la politique nationale de cybersécurité

En collaboration avec les parties prenantes comprenant les gouvernements, l'industrie et les organisations professionnelles, la société civile et les citoyens L'Etat élabore et met en œuvre une politique nationale de cybersécurité en tenant compte de l'évolution technologique et des priorités du Gouvernement dans ce domaine.

A ce titre, l'Etat :

- assure la promotion de la sécurité des réseaux de communications électroniques et des systèmes d'information ainsi que le suivi de l'évolution des questions liées aux activités de sécurité et à la certification ;

- coordonne sur le plan national les activités concourant à la sécurisation et à la protection des réseaux de communications électroniques et des systèmes d'information ;

- veille à la mise en place d'un cadre adéquat pour la sécurité des communications électroniques ;

- assure la représentation de L'Etat aux instances internationales chargées des activités liées à la sécurisation et à la protection des réseaux de communications électroniques et des systèmes d'information.

La politique nationale de cybersécurité devra intégrer dans ses grandes lignes la protection de l'information dans les réseaux, la sécurité des transactions électroniques, la protection de la vie privée et des mineurs dans le cyberespace ainsi que la lutte contre la fracture numérique.

Chapitre II : Structures nationales de la cybersécurité

Article 58 : Du Conseil National de la cybersécurité

Il est créé un Conseil National de la cybersécurité (CNC), entité spécifique qui constitue un centre de liaison à haut niveau pour la cybersécurité au sein de l'État. Le Conseil National de la cybersécurité devra adopter et approuver les politiques proposées pour leur mise en œuvre par l'Autorité nationale de la cybersécurité (NCA) prévue par l'Article 59 de la présente loi type, en relation avec la politique et la stratégie en matière de cybersécurité nationale et les priorités et les initiatives en matière de cybersécurité nationale.

A ce titre, le Conseil National de la cybersécurité a pour mission de :

- coordonner des actions en matière de cybersécurité au niveau national ;

- Identifier des protagonistes chargés de la cybersécurité dans l'économie et établir des relations public-privé nécessaires pour aborder les questions de cybersécurité ;

-collaborer avec les services ou agences gouvernementaux tels que les services de renseignements, les services secrets, la Direction générale de la sécurité, les forces de police, l'unité de la criminalité technologique aux fins d'élaborer des normes, d'établir des procédures d'investigation uniformes et de développer un consensus institutionnel ;

-collaborer avec les organismes chargés de l'application de la loi au niveau régional ou international ;

-surveiller les systèmes gouvernementaux de l'information et des infrastructures essentielles de l'Etat ;

-coordonner des actions et le développement des systèmes d'identité numérique et la gestion et les bonnes pratiques en relation notamment avec les identités numériques ;

-développer des formations types et de programmes de développement des capacités pour les agences et la création d'une plateforme nationale aux fins de coordonner l'assistance technique et les initiatives de formation au niveau international.

Un décret précise les règles d'organisation et de fonctionnement du Conseil National de la cybersécurité.

Article 59 : Statut et organisation de l'Autorité Nationale de la Cybersécurité (ANC)

1. Il est crée une Autorité Nationale de la cybersécurité qui est un organisme doté de la personnalité juridique et de l'autonomie financière.

L'Autorité Nationale de la cybersécurité est juridiquement distincte et indépendante du pouvoir politique et des entreprises assurant la fourniture des services de sécurité électronique des systèmes d'information et des réseaux de communications électroniques, et de la surveillance des réseaux et systèmes ainsi que la détection d'intrusion.

2. A cet égard, les fonctions de prestataire de service de sécurité électronique, même pour le compte de l'Etat, sont incompatibles avec celles de l'Autorité Nationale de la cybersécurité prévue par la présente Loi type.

3. Elle dispose d'un personnel qualifié et des services en nombre suffisant pour exercer ses missions et ses pouvoirs dans des conditions optimales.

Article 60 : Mission de l'Autorité Nationale de la Cybersécurité (ANC)

L'Autorité Nationale de la cybersécurité assure pour le compte de l'Etat, la régulation, le contrôle et le suivi des activités liées à la sécurité des systèmes d'information et des réseaux de communications électronique.

A ce titre, elle a notamment pour mission :

- d'émettre un avis consultatif sur les textes touchant à son domaine de compétence ;

- d'adopter un programme efficace de sensibilisation à la cybersécurité nationale aux fins de promouvoir le partage d'informations avec toutes les parties prenantes sur des questions de cybersécurité

- d'adopter des mesures de développement des capacités afin de proposer une formation couvrant tous les domaines de la cybersécurité aux services spécialisés du gouvernement et aux citoyens, tout en fixant des normes pour le secteur privé.

-- de contrôler les activités de sécurité des réseaux de communications électroniques, des systèmes d'information;

- d'assurer la veille technologique et d'émettre des alertes et recommandations en matière de sécurité des réseaux de communications électroniques et de certification ;

- de participer aux activités de recherche, de formation et d'études afférentes à la sécurité des réseaux de communications électroniques, des systèmes d'informations et de certification ;

- de s'assurer de la régularité, de l'effectivité des audits de sécurité des systèmes d'information suivant les normes en la matière, des organismes publics et des autorités de certification ;

- d'assurer la surveillance, la détection et la fourniture de l'information sur les risques informatiques et les actes de malveillance des cybercriminels ;

- d'exercer toute autre mission d'intérêt général que pourrait lui confier l'autorité de tutelle.

Un décret précise les règles d'organisation et de fonctionnement de l'Autorité Nationale de la cybersécurité

Chapitre III : Cadre financier de la cybersécurité

Article 61 : Du fonds spécial des activités de cybersécurité

Les autorités de certification accréditées, les auditeurs de sécurité, les éditeurs de logiciels de sécurité, les prestataires techniques et les autres prestataires de services de sécurité agréés, sont assujettis au paiement d'une contribution de 1,5 % de leur chiffre d'affaires hors taxes, destinée au financement d'un fonds dénommé « Fonds Spécial des activités de cybersécurité », au titre du financement de la recherche, du développement, de la formation et des études en matière de cybersécurité.

Les ressources visées à l'alinéa 1 ci-dessus sont recouvrées par l'Agence et déposées dans un compte spécial placé sous le contrôle des services de l'Etat.

Les modalités de fonctionnement de ce fonds sont précisées par décret.

TITRE IV : DISPOSITIONS FINALES

Article 62 : Entrée en vigueur

La présente Loi type qui entre en vigueur à compter de la date de sa signature sera publiée au Bulletin officiel de la Communauté.

ANNEXE

Annexe

Recommandations de l'Atelier régional de Douala (27-28 juillet 2012)

Annexe 3

Recommandations

Les experts des Etats membres de la CEEAC, réunis à Douala du 26 au 27 juillet 2012, dans le cadre de l'atelier régional de validation des projets de lois-types de la CEEAC relatifs à la cybersécurité, recommandent :

Aux Etats Membres

Recommandation 1 :

De tenir compte de la convention de l'Union Africaine et des projets de lois-types ci-présentés pour finaliser leurs lois nationales en attendant leur validation par les instances statutaires de la CEEAC ;

Recommandation 2 :

D'organiser au niveau national, des ateliers de sensibilisation sur tous projets de lois-types et les lois en vue de leur appropriation par toutes les parties prenantes ;

Recommandation 3 :

De définir une cyberstratégie qui intègrera tous les objectifs de sécurité et de maîtrise des risques inter-états ;

Recommandation 4 :

de participer activement aux consultations en cours sur le projet de convention africaine sur la cybersécurité en préparation par la commission économique pour l'Afrique (CEA) et la commission de l'Union Africaine (UA), en vue de son examen par la réunion des ministres des Etats membres de l'Union Africaine en charge des TIC prévue à Khartoum (Soudan) du 02 au 06 septembre 2012 ;

Recommandation 5 :

De prendre toutes les dispositions pour s'accorder sur une définition commune de la cybersécurité ;

Bureau de développement des télécommunications (BDT)
Union internationale des télécommunications
Place des Nations
CH-1211 Genève

E-mail: bdtmail@itu.int
www.itu.int/ITU-D/projects/ITU_EC_ACP/

Genève, 2013