

Loi n° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun

L'Assemblée Nationale a délibéré et adopté, le président de la République promulgue la loi dont la teneur suit :

Titre premier : Dispositions générales

Article 1^{er} : - La présente loi régit le cadre de sécurité des réseaux de communications électroniques et des systèmes d'information, définit et réprime les infractions liées à l'utilisation des technologies de l'information et de la communication au Cameroun.

A ce titre, elle vise notamment à :

Instaurer la confiance dans les réseaux de communications électroniques et les systèmes d'information ;

Fixer le régime juridique de la preuve numérique, des activités de sécurité, de cryptographie et de certification électronique ;

Protéger les droits fondamentaux des personnes physiques notamment le droit à la dignité humaine, à l'honneur et au respect de la vie privée, ainsi que les intérêts légitimes des personnes morales.

Art. 2. - Sont exclues du champ de la présente loi, les applications spécifiques utilisées en matière de défense et de sécurité nationale.

Art. 3. - Les réseaux de communications électroniques visés par la présente loi comprennent : les réseaux satellitaires, les réseaux terrestres, les réseaux électroniques lorsqu'ils servent à l'acheminement de communications électroniques, les réseaux assurant la diffusion ou la distribution de services de communications audiovisuelles.

Art. 4. - Au sens de la présente loi et de ses textes d'application, les définitions ci-après, sont admises :

Accès illicite : accès intentionnel, sans en avoir le droit, à l'ensemble ou à une partie d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal ;

Administration chargée des Télécommunications : ministère ou ministre, selon les cas, investi pour le compte du gouvernement, d'une compétence générale sur le secteur des télécommunications et des technologies de l'information et de la communication ;

Algorithme : suite d'opérations mathématiques élémentaires à appliquer à des données pour aboutir à un résultat désiré ;

Algorithme asymétrique : algorithme de chiffrement utilisant une clé publique pour chiffrer et une clé privée (différente) pour déchiffrer les messages ;

Algorithme symétrique : algorithme de déchiffrement utilisant une même clé pour chiffrer et déchiffrer les messages ;

Attaque active : acte modifiant ou altérant les ressources ciblées par l'attaque (atteinte à l'intégrité, à la disponibilité et à la confidentialité des données) ;

Attaque passive : acte n'altérant pas sa cible (écoute passive, atteinte à la confidentialité) ;

Atteinte à l'intégrité : fait de provoquer intentionnellement une perturbation grave ou une interruption de fonctionnement d'un système d'information, d'un réseau de communications électroniques ou d'un équipement terminal, en introduisant, transmettant, endommageant, effaçant, détériorant, modifiant, supprimant ou rendant inaccessibles des données ;

Audit de sécurité : examen méthodique des composantes et des acteurs de la sécurité, de la politique, des mesures, des solutions, des procédures et des moyens mis en œuvre par une organisation, pour sécuriser son environnement, effectuer des contrôles de conformité, des contrôles d'évaluation de l'adéquation des moyens (organisationnels, techniques, humains, financiers) investis au regard des risques encourus, d'optimisation, de rationalité et de performance ;

Authentification : critère de sécurité défini par un processus mis en œuvre notamment pour vérifier l'identité d'une personne physique ou mo-

rale et s'assurer que l'identité correspond à l'identité de cette personne préalablement enregistrée ;

Autorité de certification : autorité de confiance chargée de créer et d'attribuer des clés publiques et privées ainsi que des certificats électroniques ;

Autorité de Certification Racine : organisme investi de la mission d'accréditation des autorités de certification, de la validation de la politique de certification des autorités de certification accréditées, de la vérification et de la signature de leurs certificats respectifs ;

Certificat électronique : document électronique sécurisé par la signature électronique de la personne qui l'a émis et qui atteste après constat, la véracité de son contenu ;

Certificat électronique qualifié : certificat électronique émis par une autorité de certification agréée ;

Certification électronique : émission de certificats électroniques ;

Chiffrement : procédé grâce auquel on transforme à l'aide d'une convention secrète appelée clé, des informations claires en informations intelligibles par des tiers n'ayant pas la connaissance de la clé ;

Clé : dans un système de chiffrement, elle correspond à une valeur mathématique, un mot, une phrase qui permet, grâce à l'algorithme de chiffrement, de chiffrer ou de déchiffrer un message ;

Clé privée : clé utilisée dans les mécanismes de chiffrement asymétrique (ou chiffrement à clé publique), qui appartient à une entité et qui doit être secrète ;

Clé publique : clé servant au chiffrement d'un message dans un système asymétrique et donc librement diffusé ;

Clé secrète : clé connue de l'émetteur et du destinataire servant de chiffrement et de déchiffrement des messages et utilisant le mécanisme de chiffrement symétrique ;

Code source : ensemble des spécifications techniques, sans restriction d'accès ni de mise en œuvre, d'un logiciel ou protocole de communication, d'interconnexion, d'échange ou d'un format de données ;

Communication audiovisuelle : communication au public de services de radiodiffusion télévisuelle et sonore ;

Communication électronique : émission, transmission ou réception de signes, signaux, d'écrits, d'images ou de sons, par voie électromagnétique ;

Confidentialité : maintien du secret des informations et des transactions afin de prévenir la divulgation non autorisée d'informations aux non destinataires permettant la lecture, l'écoute, la copie illicite d'origine intentionnelle ou accidentelle durant leur stockage, traitement ou transfert ;

Contenu : ensemble d'informations relatives aux données appartenant à des personnes physiques ou morales, transmises ou reçues à travers les réseaux de communications électroniques et les systèmes d'information ;

Contenu illicite : contenu portant atteinte à la dignité humaine, à la vie privée, à l'honneur ou à la sécurité nationale ;

Courrier électronique : message, sous forme de texte, de voix, de son ou d'image, envoyé par un réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier le récupère ;

Cryptage : utilisation de codes ou signaux non usuels permettant la conservation des informations à transmettre en des signaux incompréhensibles par les tiers ;

Cryptanalyse : ensemble des moyens qui permet d'analyser une information préalablement chiffrée en vue de la déchiffrer ;

Cryptogramme : message chiffré ou codé ;

Cryptographie : application des mathématiques permettant d'écrire l'information, de manière à la rendre inintelligible à ceux ne possédant pas les capacités de la déchiffrer ;

Cybercriminalité : ensemble des infractions s'effectuant à travers le cyberspace par des moyens autres que ceux habituellement mis en œuvre, et de manière complémentaire à la criminalité classique ;

Cybersécurité : ensemble de 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 sécurité fixés à travers les réseaux de communications électroniques, les systèmes d'information et pour la protection de la vie privée des personnes ;

Déclaration des pratiques de certification : ensemble des pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'autorité de certification compétente applique dans le cadre de la fourniture de ce service et en conformité avec la (les) politique (s) de certification qu'elle s'est engagée(s) à respecter ;

Déchiffrement : opération inverse du chiffrement ;

Déni de service : attaque par saturation d'une ressource du système d'information ou du réseau de communications électroniques, afin qu'il s'effondre et ne puisse plus réaliser les services attendus de lui ;

Déni de service distribué : attaque simultanée des ressources du système d'information ou du réseau de communications électroniques, afin de les saturer et amplifier les effets d'entrave ;

Disponibilité : critère de sécurité permettant que les ressources des réseaux de communications électroniques, des systèmes d'information ou des équipements terminaux soient accessibles et utilisables selon les besoins (le facteur temps) ;

Dispositif de création de signature électronique : ensemble d'équipements et/ou logiciels privés de cryptage, homologués par une autorité compétente, configurés pour la création d'une signature électronique ;

Dispositif de vérification de signature électronique : ensemble d'équipements et/ou logiciels publics de cryptage, homologués par une autorité compétente, permettant la vérification par une autorité de certification d'une signature électronique ;

Données : représentation de faits, d'informations ou de notions sous une forme susceptible d'être traitée par un équipement terminal, y compris un programme permettant à ce dernier d'exécuter une fonction ;

Données de connexion : ensemble de données relatives au processus d'accès dans une communication électronique ;

Données de trafic : données ayant trait à une communication électronique indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type du service sous-jacent ;

Équipement terminal : appareil, installation ou ensemble d'installations destiné à être connecté à un point de terminaison d'un système d'information et émettant, recevant, traitant, ou stockant des données d'information ;

Fiabilité : aptitude d'un système d'information ou d'un réseau de communications électronique à fonctionner sans incident pendant un temps suffisamment long ;

Fournisseur des services de communications électroniques : personne physique ou morale fournissant les prestations consistant entièrement ou principalement en la fourniture de communications électroniques ;

Gravité de l'impact : appréciation du niveau

de gravité d'un incident, pondéré par sa fréquence d'apparition ;

Intégrité des données : critère de sécurité définissant l'état d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal qui est demeuré intact et permet de s'assurer que les ressources n'ont pas été altérées (modifiées ou détruites) d'une façon tant intentionnelle qu'accidentelle, de manière à assurer leur exactitude, leur fiabilité et leur pérennité ;

Interception illégale : accès sans en avoir le droit ou l'autorisation, aux données d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal ;

Interception légale : accès autorisé aux données d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal ;

Intrusion par intérêt : accès intentionnel et sans droit dans un réseau de communications électroniques ou dans un système d'information, dans le but soit de nuire soit de tirer un bénéfice économique, financier, industriel, sécuritaire ou de souveraineté ;

Intrusion par défi intellectuel : accès intentionnel et sans droit dans un réseau de communications électroniques ou dans un système d'information, dans le but de relever un défi intellectuel pouvant contribuer à l'amélioration des performances du système de sécurité de l'organisation ;

Logiciel trompeur : logiciel effectuant des opérations sur un équipement terminal d'un utilisateur sans informer préalablement cet utilisateur de la nature exacte des opérations que ce logiciel va effectuer sur son équipement terminal ou sans demander à l'utilisateur s'il consent à ce que le logiciel procède à ces opérations ;

Logiciel espion : type particulier de logiciel trompeur collectant les informations personnelles (sites web les plus visités, mots de passe, etc.) auprès d'un utilisateur du réseau de communications électroniques ;

Logiciel potentiellement indésirable : logiciel représentant des caractéristiques d'un logiciel trompeur ou d'un logiciel espion ;

Message clair : version intelligible d'un message et compréhensible par tous ;

Moyen de cryptographie : équipement ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser une opération inverse avec ou sans convention secrète afin de garantir la sécurité du stockage ou de la transmission de données, et d'assurer leur confidentialité et le contrôle de leur intégrité ;

Non répudiation : critère de sécurité assurant la disponibilité de preuves qui peuvent être opposées à un tiers et utilisées pour prouver la traçabilité d'une communication électronique qui a eu lieu ;

Politique de certification : ensemble de règles identifiées, définissant les exigences auxquelles l'autorité de certification se conforme dans la mise en place de ses prestations et indiquant l'applicabilité d'un service de certification à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes ;

Politique de sécurité : référentiel de sécurité établi par une organisation, reflétant sa stratégie de sécurité et spécifiant les moyens de la réaliser ;

Prestation de cryptographie : opération visant à la mise en œuvre, pour le compte d'autrui, de moyens de cryptographie ;

Réseau de communications électroniques : système de transmission, actif ou passif et, le cas échéant, les équipements de commutation et de

Loi n° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun

routage et les autres ressources qui permettent l'acheminement des signaux par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques comprenant les réseaux satellitaires, les réseaux terrestres fixes (avec commutation de circuits ou de paquets, y compris l'Internet) et mobiles, les systèmes utilisant le réseau électrique, pour autant qu'ils servent à la transmission des signaux, les réseaux utilisés pour la radiodiffusion sonore et télévisuelle et les réseaux câbles de télévision, quel que soit le type d'information transmise ;

Réseau de télécommunications : installation ou ensemble d'installations assurant soit la transmission et l'acheminement de signaux de télécommunications, soit l'échange d'informations de commande et de gestion associés à ces signaux entre les points de ce réseau ;

Sécurité : situation dans laquelle quelqu'un, quelque chose n'est exposé à aucun danger. Mécanisme destiné à prévenir un événement dommageable, ou à limiter les effets.

Service de certification : prestation fournie par une autorité de certification ;

Service de communications électroniques : prestation consistant entièrement ou principalement en la fourniture de communications électroniques à l'exclusion des contenus des services de communications audiovisuelles ;

Signataire : personne physique, agissant pour son propre compte ou pour celui de la personne physique ou morale qu'elle représente, qui met à contribution un dispositif de création de signature électronique ;

Signature électronique : signature obtenue par un algorithme de chiffrement asymétrique permettant d'authentifier l'émetteur d'un message et d'en vérifier l'intégrité ;

Signature électronique avancée : signature électronique obtenue à l'aide d'un certificat électronique qualifié ;

Standard ouvert : protocole de communication, d'interconnexion ou d'échange et format de données interopérable, dont les spécifications techniques sont publiques et sans restriction d'accès ni de mise en œuvre ;

Système de détection : système permettant de détecter les incidents qui pourraient conduire aux violations de la politique de sécurité et permettant de diagnostiquer des intrusions potentielles ;

Système d'information : dispositif isolé ou groupe de dispositifs interconnectés ou apparentés, assurant par lui-même ou par un ou plusieurs de ses éléments, conformément à un programme, un traitement automatisé de données ;

Vulnérabilité : défaut de sécurité se traduisant soit intentionnellement, soit accidentellement par une violation de la politique de sécurité, dans l'architecture d'un réseau de Communications électroniques, dans la conception d'un système d'information.

Art. 5. Les termes et expressions non définis dans cette loi, conservent leurs définitions ou significations données par les instruments juridiques internationaux auxquels l'Etat du Cameroun a souscrit, notamment, la Constitution et la Convention de l'Union Internationale des télécommunications, le règlement des radiocommunications et le règlement des télécommunications internationales.

Titre II

De la cyber sécurité

Chapitre I - De la politique générale de sécurité électronique

Art. 6. L'administration chargée des télécommunications élabore et met en œuvre, la politique de sécurité des communications électroniques et des systèmes d'information en tenant compte de l'évolution technologique et des priorités du gouvernement dans ce domaine.

A ce titre, elle :

- 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 ;

Arrête la liste des autorités de certification ;

Assure la représentation du Cameroun aux instances internationales chargées des activités liées à la sécurisation et à la protection des réseaux de communications électroniques et des systèmes d'information.

Chapitre II

De la régulation et suivi des activités de sécurité électronique

Art. 7. (1) L'Agence Nationale des Technologies de l'information et de la communication, ci-après désignée l'agence, instituée par la loi régissant les communications électroniques au Cameroun, est chargée de la régulation des activités de sécurité électronique, en collaboration avec l'Agence de Régulation des Télécommunications.

(2) L'Agence prévue à l'alinéa 1 ci-dessus, 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 électroniques, et à la certification électronique. A ce titre, elle a notamment pour missions :

- d'instruire les demandes d'accréditation et de préparer les cahiers des charges des autorités de certification et de les soumettre à la signature du ministre chargé des télécommunications ;

- de contrôler la conformité des signatures électroniques émises ;

- de participer à l'élaboration de la politique nationale de sécurité des réseaux de communications électroniques et de certification ;

- d'émettre un avis consultatif sur les textes touchant à son domaine de compétence ;

- de contrôler les activités de sécurité des réseaux de communications électroniques, des systèmes d'information et de certification ;

- d'instruire les demandes d'homologation des moyens de cryptographie et de délivrer les certificats d'homologation des équipements de sécurité ;

- de préparer les conventions de reconnaissance mutuelle avec les parties étrangères et de les soumettre à la signature du ministre chargé des télécommunications ;

- 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 des cybercriminels ;
- d'exercer toute autre mission d'intérêt général que pourrait lui confier l'autorité de tutelle.

(3) Un décret du Premier ministre précise les modalités d'application des dispositions de l'alinéa 1 ci-dessus.

Art ; 8. (1) L'Agence est l'autorité de certification racine.

(2) L'Agence est l'autorité de certification de l'administration publique.

Art. 9 (1) Les autorités de certification accréditées, les auditeurs de sécurité, les éditeurs de logiciels de sécurité 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 sécurité électronique », au titre du financement de la recherche, du développement, de la formation et des études en matière de cybersécurité.

(2) Les ressources visées à l'alinéa 1 ci-dessus sont recouvrées par l'Agence et déposées dans un compte ouvert à la Banque centrale.

(3) Il est créé un comité chargé de la validation des projets prioritaires de recherche, de dévelop-

pement, de formation et des études en matière de cybersécurité.

Les modalités de fonctionnement de ce comité sont fixées dans un texte réglementaire.

(4) Le ministre chargé des télécommunications est l'ordonnateur des dépenses engagées sur le fonds visé à l'alinéa 1 ci-dessus.

(5) Les conditions et les modalités de perception et de gestion de cette redevance sont définies par voie réglementaire.

Chapitre III- Du régime juridique des activités de certification

Art. 10 (1) L'activité de certification électronique est soumise à autorisation préalable. Elle est exercée par des autorités de certification.

Art. 11. Peuvent faire l'objet d'une autorisation :

- la mise en place et l'exploitation d'une infrastructure en vue d'émettre, de conserver et de délivrer les certificats électroniques qualifiés ;

- la mise à la disposition du public, des clés publiques de tous les utilisateurs ;

- la mise à la disposition du public de la prestation d'audit de sécurité, d'édition de logiciels de sécurité et de toutes les autres prestations de services de sécurité.

Art. 12 : Les conditions et les modalités d'octroi de l'autorisation visée à l'article 10 ci-dessus sont fixées par voie réglementaire.

Chapitre IV

Des activités de sécurité

Art. 13. (1) Sont soumis à un audit de sécurité obligatoire, les réseaux de communications électroniques et les systèmes d'information des opérateurs, les autorités de certification et les fournisseurs de services de communications électroniques.

(2) Les conditions et les modalités de l'audit de sécurité prévus à l'alinéa 1 ci-dessus sont définies par voie réglementaire.

Art. 14. Le personnel de l'Agence et les experts commis en vue d'accomplir des opérations d'audits sont astreints au secret professionnel.

Chapitre V

De la certification électronique

Art. 15 (1) Les certificats électroniques qualifiés ne sont valables que pour les objets pour lesquels ils ont été émis.

(2) Les dispositifs de création et de vérification des certificats qualifiés sont du point de vue technologique neutres, normalisés, homologués et interopérables.

Art. 16 (1) Les autorités de certification sont responsables du préjudice causé aux personnes qui se sont fiées aux certificats présentés par elles comme qualifiés dans chacun des cas suivants.

- les informations contenues dans le certificat, à la date de sa délivrance, étaient inexactes ;

- les données prescrites pour que le certificat puisse être considéré comme qualifié étaient incomplètes ;

- la délivrance du certificat n'a pas donné lieu à la vérification que le signataire détient la convention privée correspondant à la convention publique de ce certificat ;

- les autorités de certification et les prestataires de certification n'ont pas, le cas échéant, fait procéder à l'enregistrement de la révocation du certificat qualifié et tenu cette information à la disposition des tiers.

(2) Les autorités de certification ne sont pas responsables du préjudice causé par un usage du certificat qualifié dépassant les limites fixées à son utilisation ou à la valeur des transactions pour lesquelles il peut être utilisé, à condition que ces limites figurent dans le certificat qualifié et soient accessibles aux utilisateurs.

(3) Les autorités de certification doivent justifier d'une garantie financière suffisante, spécialement affectée au paiement des sommes qu'elles pourraient devoir aux personnes s'étant fiées raisonnablement aux certificats qualifiés qu'elles délivrent, ou d'une assurance garantissant les conséquences pécuniaires de leur responsabilité civile professionnelle.

Chapitre VI

De la signature électronique

Art. 17 – La signature électronique avancée a la même valeur juridique que la signature manuscrite et produit les mêmes effets que cette dernière.

Art. 18 – Une signature électronique avancée doit remplir les conditions ci-après :

- les données afférentes à la création de la signature sont liées exclusivement au signataire et sont sous son contrôle exclusif ;

- toute modification à elle apportée, est facilement décelable ;

- elle est créée au moyen d'un dispositif sécurisé dont les caractéristiques techniques sont fixées par un texte du ministre chargé des télécommunications ;

- le certificat utilisé pour la génération de la signature est un certificat qualifié. Un texte du ministre chargé des Télécommunications fixe les critères de qualification des certificats.

Chapitre VII

Des certificats et signatures électroniques délivrés par les autorités de certification

Art. 19 - L'autorité de certification ayant conféré la validité à un certificat électronique ne peut se renier.

Art. 20 – (1) Un certificat électronique émis hors du territoire national produit les mêmes effets juridiques qu'un certificat qualifié émis au Cameroun à condition qu'il existe un acte de reconnaissance de l'autorité émettrice signé par le ministre chargé des Télécommunications.

(2) L'interopérabilité des certificats électroniques qualifiés est règlementée par un texte du ministre chargé des Télécommunications ;

Chapitre VIII

Du document électronique

Art. 21 – Toute personne désirant apposer sa signature électronique sur un document peut créer cette signature par un dispositif fiable dont les caractéristiques techniques sont fixées par un texte du ministre chargé des Télécommunications.

Art. 22 – Toute personne utilisant un dispositif de signature électronique doit :

- prendre les précautions minimales qui sont fixées par le texte visé à l'article 21 ci-dessus, afin d'éviter toute utilisation illégale des éléments de cryptage ou des équipements personnels relatifs à sa signature ;

- informer l'autorité de certification de toute utilisation illégitime de sa signature ;

- veiller à la véracité de toutes les données qu'elle a déclarées au fournisseur de services de certification électronique et à toute personne à qui il a demandé de se fier à sa signature.

Art. 23. En cas de manquement aux engagements prévus à l'article 22 ci-dessus, le titulaire de la signature est responsable du préjudice causé à autrui.

Chapitre IX

De la protection des réseaux de communications électroniques, des Systems d'information et de la vie privée des personnes

Section I

De la protection des réseaux de communications électroniques

Art. 24 – Les opérateurs des réseaux de communications électroniques et les fournisseurs de services de communications électroniques doivent prendre toutes les mesures techniques et administratives nécessaires pour garantir la sécurité des services offerts. A cet effet, ils sont tenus d'informer les usagers :

- du danger encouru en cas d'utilisation de leurs réseaux ;

- des risques particuliers de violation de la sécurité notamment, les dénis de service distribués ; le re-routage anormal, les pointes de trafic, le trafic et les ports inhabituels, les écoutes passives et actives, les intrusions et tout autre risque ;

- de l'inexistence de moyens techniques permettant d'assurer la sécurité de leurs communi-

Loi n° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun

tions.

Art. 25 – (1) Les opérateurs de réseaux et les fournisseurs de service de communications électroniques ont obligation de conserver les données de connexion et de trafic pendant une période de dix (10) ans.

(2) Les opérateurs de réseaux et les fournisseurs de services de communications électroniques installent des mécanismes de surveillance de trafic des données de leurs réseaux. Ces données peuvent être accessibles lors des investigations judiciaires.

(3) La responsabilité des opérateurs de réseaux et celles des fournisseurs de services de communications électroniques est engagée si l'utilisation des données prévues à l'alinéa 2 ci-dessus porte atteinte aux libertés individuelles des usagers.

Section II

De la protection des systèmes d'information

Art. 26 – (1) Les exploitants des systèmes d'information prennent toutes les mesures techniques et administratives afin de garantir la sécurité des services offerts. A cet effet, ils se dotent de systèmes normalisés leur permettant d'identifier, d'évaluer, de traiter et de gérer continuellement les risques liés à la sécurité des systèmes d'information dans le cadre des services offerts directement ou indirectement.

(2) Les exploitants des systèmes d'information mettent en place des mécanismes techniques pour faire face aux atteintes préjudiciables à la disponibilité permanente des systèmes, à leur intégrité, à leur authentification, à leur non répudiation par des utilisateurs tiers, à la confidentialité des données et à la sécurité physique.

(3) Les mécanismes prévus à l'alinéa 2 ci-dessus, font l'objet d'approbation et visa conforme de l'Agence.

(4) Les plates-formes des systèmes d'information font l'objet de protection contre d'éventuels rayonnements et des intrusions qui pourraient compromettre l'intégrité des données transmises et contre toute attaque externe notamment par un système de détection d'intrusions.

Art. 27 – Les personnes morales dont l'activité est d'offrir un accès à des systèmes d'information sont tenues d'informer les usagers :

- du danger encouru dans l'utilisation des systèmes d'information non sécurisés notamment pour les particuliers ;

- de la nécessité d'installer des dispositifs de contrôle parental ;

- des risques particuliers de violations de sécurité, notamment la famille générique des virus ;

- de l'existence de moyens techniques permettant de restreindre l'accès à certains services et de leur proposer au moins l'un de ces moyens, notamment l'utilisation des systèmes d'exploitation les plus récents, les outils antivirus et contre les logiciels espions et trompeurs, l'activation des pare-feux personnels, de systèmes de détection d'intrusions et l'activation des mises à jour automatiques.

Art. 28 – (1) Les exploitants des systèmes d'information informent les utilisateurs de l'interdiction faite d'utiliser le réseau de communications électroniques pour diffuser des contenus illicites ou tout autre acte qui peut entamer la sécurité des réseaux ou des systèmes d'information.

(2) L'interdiction porte également sur la conception de logiciel trompeur, de logiciel espion, de logiciel potentiellement indésirable ou de tout autre outil conduisant à un comportement frauduleux.

Art. 29 (1) Les exploitants des systèmes d'information ont l'obligation de conserver les données de connexion et de trafic de leurs systèmes d'information pendant une période de dix (10) ans.

(2) Les exploitants des systèmes d'information sont tenus d'installer des mécanismes de surveillance de contrôle d'accès aux données de leurs systèmes d'information. Les données conservées peuvent être accessibles lors des investigations judiciaires.

(3) Les installations des exploitants des systèmes d'information peuvent faire l'objet de perquisition ou de saisie sur ordre d'une autorité judiciaire dans les conditions prévues par les lois et règlements en vigueur.

Art. 30 – (1) Les exploitants des systèmes d'information évaluent, révisent leurs systèmes de sécurité et introduisent en cas de nécessité les modifications appropriées dans leurs pratiques, mesures et techniques de sécurité en fonction de l'évolution des technologies.

(2) Les exploitants des systèmes d'information et leurs utilisateurs peuvent coopérer entre eux pour l'élaboration et la mise en œuvre des pratiques, mesures et techniques de sécurité de leurs systèmes.

Art. 31 (1) Les fournisseurs de contenus des réseaux de communication électronique et systèmes d'information sont tenus d'assurer la disponibilité des contenus, ainsi que celle des données stockées dans leurs installations.

(2) Ils ont l'obligation de mettre en place des filtres pour faire face aux atteintes préjudiciables aux données personnelles et à la vie privée des utilisateurs.

Art. 32 (1) Les réseaux de communications électroniques et les systèmes d'information sont soumis à un audit de sécurité obligatoire et périodique de leurs systèmes de sécurité par l'Agence.

(2) L'audit de sécurité et les mesures d'impact de gravité sont effectués chaque année ou lorsque les circonstances l'exigent.

(3) Les rapports d'audit sont confidentiels et adressés au ministre chargé des télécommunications.

(4) Un texte du ministre chargé des télécommunications fixe les conditions d'évaluation des niveaux d'impact de gravité.

Section III

Des obligations des fournisseurs d'accès, de services et des continus

Art. 33 – Les personnes dont l'activité est d'offrir un accès aux services de communications électroniques, informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposer au moins un de ces moyens.

Art. 34 – (1) La responsabilité des personnes qui assurent, même à titre gratuit, le stockage des signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par les destinataires de ces services, peut être engagée.

(2) Toutefois, la responsabilité prévue à l'alinéa 1 ci-dessus n'est point engagée dans les cas suivants :

- les personnes n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ; Si, dès le moment où elles ont eu connaissance des faits, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible.

Art. 35 (1) Les personnes mentionnées aux articles 33 et 34 ci-dessus, sont tenues de conserver, pendant une durée de dix (10) ans, les données permettant l'identification de toute personne ayant contribué à la création du contenu des services dont elles sont prestataires.

(2) Elles fournissent aux personnes qui éditent un service de communications électroniques des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues aux articles 37 et 38 ci-dessus.

(3) L'autorité judiciaire peut requérir communication auprès des prestataires mentionnés aux articles 33 et 34 ci-dessus des données prévues à l'alinéa 1 ci-dessus.

Art. 36 – La juridiction compétente saisie statue dans un délai maximum de trente (30) jours sur toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication électronique.

Art. 37 – Les personnes dont l'activité consiste à éditer un service de communications électroniques, mettent à la disposition du public :

- leurs nom, prénoms, domicile et numéro de téléphone et, si elles sont assujetties aux formalités d'inscription au registre de commerce et du crédit mobilier, le numéro de leur inscription, s'il s'agit des personnes physiques ;

- leur dénomination ou leur raison sociale et leur siège social, leur numéro de téléphone et, s'il

s'agit des personnes morales assujetties aux formalités d'inscription au registre de commerce et du crédit mobilier, le numéro de leur inscription, leur capital social, l'adresse de leur siège social, s'il s'agit des personnes morales ;

- le nom du directeur ou du codirecteur de la publication et, le cas échéant, celui du responsable de la rédaction ;

- le nom, la dénomination ou la raison sociale, l'adresse et le numéro de téléphone du prestataire mentionné aux articles 33 et 34.

Art. 38 (1) Les personnes éditant à titre non professionnel un service de communications électroniques peuvent ne tenir à la disposition du public que le nom, la dénomination ou la raison sociale et l'adresse du prestataire.

(2) Les personnes mentionnées aux articles 33 et 34 ci-dessus, sont assujetties au secret professionnel.

Art. 39 (1) Toute personne victime d'une diffamation au moyen d'un service de communications électroniques, dispose d'un droit de réponse et peut en exiger la rectification.

(2) Les conditions d'insertion du droit de réponse sont celles prévues par les textes en vigueur.

Art. 40 (1) Toute personne assurant une activité de transmission de contenus sur un réseau de communications électroniques ou de fourniture d'accès à un réseau de communications électroniques ne peut voir sa responsabilité engagée que lorsque :

- elle est à l'origine de la demande de transmission litigieuse ;

- elle sélectionne ou modifie les contenus faisant l'objet de la transmission.

(2) Toute personne assurant dans le seul but de rendre plus efficace leur transmission ultérieure, une activité de stockage automatique, intermédiaire et temporaire des contenus qu'un prestataire transmet, ne peut voir sa responsabilité civile ou pénale engagée en raison de ces contenus que dans le cas où elle a modifié ces contenus, ne s'est pas conformée à leur conditions d'accès et aux règles usuelles concernant leur mise à jour ou a entravé l'utilisation licite et usuelle de la technologie utilisée pour obtenir les données.

Section IV

De la protection de la vie privée des personnes

Art. 41 – Toute personne a droit au respect de sa vie privée. Les juges peuvent prendre les mesures conservatoires, notamment le séquestre et la saisie pour empêcher ou faire cesser une atteinte à la vie privée.

Art. 42 – La confidentialité des communications acheminées à travers les réseaux de communications électroniques et les systèmes d'information y compris les données relatives au trafic, est assurée par les opérateurs et exploitants des réseaux de communications électroniques et des systèmes d'information.

Art. 43 – Le fournisseur de contenus est responsable des contenus véhiculés par son système d'information, notamment lorsque ces contenus portent atteinte à la dignité humaine, à l'honneur et à la vie privée.

Art. 44 (1) Interdiction est faite à toute personne physique ou morale d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférent, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés, sauf lorsque cette personne y est légalement autorisée.

(2) Toutefois, le stockage technique préalable à l'acheminement de toute communication est autorisé aux opérateurs et exploitants des réseaux de communications électroniques, sans préjudice du principe de confidentialité.

Art. 45 – L'enregistrement des communications et des données de trafic y afférentes, effectué dans le cadre professionnel en vue de fournir la preuve numérique d'une communication électronique est autorisé.

Art. 46 (1) Les fournisseurs de contenus des réseaux de communications électroniques et systèmes d'information, sont tenus de conserver les contenus ainsi que les données stockées dans leurs installations pendant une durée de dix (10) ans.

(2) Les fournisseurs de contenus des réseaux de communications électroniques et systèmes d'information, ont l'obligation de mettre en place des filtres pour faire face aux atteintes préjudiciables aux données personnelles et à la vie privée des utilisateurs.

Art. 47 – L'utilisation des réseaux de communications électroniques et des systèmes d'information aux fins de stocker les informations ou d'accéder à des informations stockées dans un équipement terminal d'une personne physique ou morale, ne peut se faire qu'avec son consentement préalable.

Art. 48 (1) L'émission des messages électroniques à des fins de prospection en dissimulant l'identité de l'émetteur au nom duquel la communication est faite, ou sans indiquer une adresse valide à laquelle le destinataire peut transmettre une demande visant à obtenir l'arrêt de ces informations est interdite.

(2) L'émission des messages électroniques en usurpant l'identité d'autrui est interdite.

Section V - De l'interception des communications électroniques

Art. 49 – Nonobstant les dispositions du Code de Procédure Pénale, en cas de crimes ou délits prévus dans la présente loi, l'officier de police judiciaire peut intercepter, enregistrer ou transcrire toute communication électronique.

Art. 50 – Si les opérateurs de réseaux de communications électroniques ou les fournisseurs de services de communications électroniques procèdent au codage, à la compression ou au chiffrement des données transmises, les interceptions correspondantes sont fournies en clair aux services qui les ont requis.

Art. 51 – Les personnels des opérateurs des réseaux de communications électroniques ou des fournisseurs de services de communications électroniques sont astreints au secret professionnel quant aux réquisitions reçues.

Titre III

De la cybercriminalité

Chapitre I

Des dispositions du droit processuel

Art. 52 (1) En cas d'infraction cybernétique, les officiers de police judiciaire à compétence générale et les agents habilités de l'agence, procèdent aux enquêtes conformément aux dispositions du code de procédure pénale.

(2) Avant leur entrée en fonction, les agents habilités de l'Agence prêtent serment, devant le Tribunal de Première Instance compétent selon la formule suivante : « Je jure de remplir loyalement mes fonctions et d'observer en tout les devoirs qu'elles m'imposent, de garder secrètement les informations dont j'ai eu connaissance à l'occasion ou dans l'exercice de mes fonctions. »

(3) Les officiers de police judiciaire et les agents habilités de l'Agence peuvent, lors des investigations, accéder aux moyens de transport, à tout local à usage professionnel, à l'exclusion des domiciles privés, en vue de rechercher, de constater les infractions, de demander la communication de tous les documents professionnels et en prendre copie, recueillir, sur convocation ou sur place, les renseignements et justifications.

Art. 53 (1) Les perquisitions en matière de cybercriminalité sont susceptibles de porter sur les données qui peuvent être des supports physiques ou des copies réalisées en présence des personnes qui assistent à la perquisition.

(2) Lorsqu'une copie des données saisies a été faite, celle-ci peut être détruite sur instruction du Procureur de la République pour des raisons de sécurité.

(3) Sur accord du Procureur de la République, seuls seront gardés sous scellé par l'officier de police judiciaire, les objets, documents et données utilisées à la manifestation de la vérité.

(4) Les personnes présentes lors de la perquisition peuvent être réquisitionnées de fournir les renseignements sur les objets, documents et données saisis.

Art. 54 – Les perquisitions et les saisies sont effectuées conformément aux dispositions du Code de procédure pénale en tenant compte du dépe-

Loi n° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun

risement des preuves.

Art. 55 (1) Lorsqu'il apparaît que les données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait l'objet d'opérations de transformation empêchant d'accéder en clair ou sont de nature à compromettre les informations qu'elles contiennent, le procureur de la République, le juge d'instruction ou la juridiction de jugement peuvent réquisitionner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair desdites données.

(2) Lorsqu'un moyen de cryptographie a été utilisé, les autorités judiciaires peuvent exiger la convention secrète de déchiffrement du cryptogramme.

Art. 56 – La réquisition prévue à l'article 50 ci-dessus peut être faite à tout expert. Dans ce cas, son exécution est faite conformément aux dispositions du Code de procédure pénale relative à la commission d'expert.

Art. 57 (1) Les autorités judiciaires camerounaises peuvent donner commission rogatoire tant nationale qu'internationale, à toute personne morale ou physique pour rechercher les éléments constitutifs des infractions de cybercriminalité, dont au moins l'un des éléments constitutifs a été commis sur le territoire camerounais ou dont l'un des auteurs ou complices se trouve dans ledit territoire.

(2) Sous réserve des règles de réciprocité entre le Cameroun et les pays étrangers liés par un accord de coopération judiciaire, les commissions rogatoires sont exécutées conformément aux dispositions du Code de procédure pénale.

Art. 58 (1) Les personnes physiques ou morales qui fournissent des prestations de cryptographie visant à assurer une fonction de confidentialité, sont tenues de remettre aux officiers de police judiciaire ou aux agents habilités de l'Agence, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies ;

(2) Les officiers de police judiciaire et agents habilités de l'Agence peuvent demander aux fournisseurs des prestations visés à l'alinéa 1 ci-dessus de mettre eux-mêmes en œuvre ces conventions, sauf si ceux-ci démontrent qu'ils ne sont pas en mesure de satisfaire à de telles réquisitions.

Art. 59 (1) Lorsque les nécessités de l'enquête ou de l'instruction le justifient, l'audition ou l'interrogatoire d'une personne et/ou la confrontation entre plusieurs personnes, peuvent être effectuées en plusieurs points du territoire national se trouvant reliés par des moyens de communications électroniques garantissant la confidentialité de la transmission. Il est dressé, dans chacun des lieux, un procès-verbal des opérations qui y ont été effectuées. Ces opérations peuvent faire l'objet d'enregistrement audiovisuel et/ou sonore.

(2) Lorsque les circonstances l'exigent, l'interprétation peut être faite au cours d'une audition, d'un interrogatoire ou d'une confrontation par des moyens de communications électroniques.

(3) Les dispositions du présent article sont également applicables pour l'exécution simultanée, sur un point du territoire national et sur un point situé à l'extérieur, des demandes d'entraide émanant des autorités judiciaires étrangères ou des actes d'entraide réalisés à l'étranger sur demande des autorités judiciaires camerounaises.

(4) Les modalités d'application du présent article sont définies par voie réglementaire.

Chapitre II

Des infractions et des sanctions

Art. 60 (1) Lorsqu'une autorité de certification ne respecte pas les obligations auxquelles elle est assujettie, l'Agence peut, après avoir mis la structure en demeure de présenter ses observations, prononcer l'interdiction de mise en circulation du moyen de cryptographie concerné.

(2) L'interdiction de mise en circulation est applicable sur l'ensemble du territoire national. Elle emporte en outre pour le fournisseur, l'obligation de procéder au retrait des :

- moyens de cryptographie dont la mise en circulation a été interdite auprès des diffuseurs com-

merciaux ;

- matériels constituant des moyens de cryptographie dont la mise en circulation a été interdite et qui ont été acquis à titre onéreux, directement ou par l'intermédiaire de diffuseurs commerciaux.

(3) Le moyen de cryptographie concernée pourra être remis en circulation dès que les obligations antérieurement non respectées auront été satisfaites et dûment constatée par l'Agence.

Art. 61 (1) Sont punis d'un emprisonnement de trois (03) mois à trois (03) ans et d'une amende de 20.000 (vingt mille) à 100.000 (cent mille) FCFA, les personnels de l'Agence et les experts des personnes Morales chargés des audits qui révoquent sans autorisation, des informations confidentielles dont ils ont eu connaissance à l'occasion d'un audit de sécurité.

(2) Est puni d'un emprisonnement de trois (03) mois à quatre (04) ans, le refus de déférer aux convocations des agents habilités de l'Agence.

(3) Est puni d'un emprisonnement de un (01) à cinq (05) ans et d'une amende de 100.000 (cent mille) à 1.000.000 (un million) f cfa ou de l'une des deux peines seulement, celui qui, par quelque moyen que ce soit, fait obstacle, incite à résister ou à empêcher le déroulement des audits de sécurité prévus au présent article ou refuse de fournir les informations ou documents y afférents.

Art. 62.-(1) Est puni d'un emprisonnement de un (01) à cinq (05) ans et d'une amende de 200.000 (deux cent mille) à 2.000.000 (deux millions) f cfa celui qui présente aux personnes mentionnées aux articles 33 et 34 ci-dessus, un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion, alors qu'elle sait cette information inexacte.

(2) Le directeur de la publication est tenu d'insérer, sous peine d'une amende de 100.000 (cent mille) à 2.000.000 (deux millions) f cfa, dans les quarante huit (48) heures de leur réception, les réponses de toute personne désignée dans le service de communications électroniques.

Art. 63.-(1) Est puni d'un emprisonnement de un (01) à cinq (05) ans et d'une amende de 40.000 (quarante mille) à 4.000.000 (quatre millions) f cfa, le dirigeant de droit ou de fait d'une personne morale exerçant l'activité définie aux articles 33 et 34 de la présente loi, qui n'a pas conservé les éléments d'information visés aux articles 25 et 29 ci-dessus.

(2) Est passible des mêmes peines, le dirigeant de droit ou de fait d'une personne morale exerçant l'activité définie aux articles 37 et 38 qui ne respecte pas les prescriptions prévues auxdits articles.

Art. 64. - (1) Les personnes morales sont pénalement responsables des infractions commises, pour leur compte, par leurs organes dirigeants.

(2) La responsabilité pénale des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits.

(3) Les peines encourues par les personnes morales sont des amendes de 5.000.000 (cinq millions) à 50.000.000 (cinquante millions) f cfa.

(4) Nonobstant la peine prévue à l'alinéa 3 ci-dessus, l'une des peines accessoires suivantes peut également être prononcée à l'encontre des personnes morales :

- la dissolution lorsqu'il s'agit d'un crime ou d'un délit puni en ce qui concerne les personnes physiques d'une peine d'emprisonnement supérieure ou égale à trois (03) ans et que la personne morale a été détournée de son objet pour servir de support à la commission des faits incriminés ;

- l'interdiction, à titre définitif ou pour une durée de cinq ans au moins, d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ;

- la fermeture temporaire pour une durée de cinq (05) ans au moins, dans les conditions prévues par l'article 34 du Code pénale, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

- l'exclusion des marchés publics à titre définitif ou pour une durée de cinq (05) ans au moins ;

- l'interdiction, à titre définitif ou pour une durée du cinq (05) ans au moins, de faire appel public à l'épargne ;

- l'interdiction, pour une durée de cinq (05) ans au moins, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ou d'utiliser des cartes de paiement ;

- la confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit ;

- la publication ou la diffusion de la décision prononcée soit par la presse écrite, soit par tout moyen de communication au public par voie électronique.

Art. 65. – (1) Est puni d'un emprisonnement de cinq (05) à dix (10) ans et d'une amende de 5.000.000 (cinq millions) à 10.000.000 (dix millions) f cfa ou de l'une de ces deux peines seulement, celui que effectue, sans droit ni autorisation, l'interception par des moyens techniques, de données lors des transmissions ou non, à destination, en provenance ou à l'intérieur ou non d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal ;

(2) Est puni des peines prévues à l'alinéa 1 ci-dessus, tout accès non autorisé, à l'ensemble ou à une partie d'un réseau de communications électroniques ou d'un système d'information ou d'un équipement terminal.

(3) Les peines prévues à l'alinéa 1 ci-dessus sont doublées, en cas d'accès illicite portant atteinte à l'intégrité, la confidentialité, la disponibilité du réseau de communications électroniques ou du système d'information.

(4) Est puni des mêmes peines prévues à l'alinéa 1 ci-dessus, celui qui, sans droit, permet l'accès dans un réseau de communications électroniques ou dans un système d'information par défi intellectuel.

Art. 66. (1) Est puni d'un emprisonnement de deux (02) à cinq (05) ans et d'une amende de 1.000.000 (un million) à 2.000.000 (deux millions) f cfa ou de l'une de ces deux peines seulement, celui qui entraîne la perturbation ou l'interruption du fonctionnement d'un réseau de communications électroniques ou d'un équipement terminal, en introduisant, transmettant, endommageant, effaçant, détériorant, modifiant, supprimant ou rendant inaccessible les données.

(2) Sont passibles des mêmes peines prévues à l'alinéa 1 ci-dessus, les personnes qui font usage d'un logiciel trompeur ou indésirable en vue d'effectuer des opérations sur un équipement terminal d'un utilisateur sans en informer au préalable celui-ci de la nature exacte des opérations que ledit logiciel est susceptible d'endommager.

(3) Est puni des mêmes peines prévues à l'alinéa 1 ci-dessus, celui qui, à l'aide d'un logiciel potentiellement indésirable collecte, tente de collecter ou facilite l'une de ces opérations pour accéder aux informations de l'opérateur ou du fournisseur d'un réseau ou de service électronique afin de commettre des infractions.

Art. 67.- Constitue une atteinte à l'intégrité d'un réseau de communications électroniques ou d'un système d'information et punie des peines prévues à l'article 66, alinéa 1 ci-dessus, le fait de provoquer une perturbation grave ou une interruption de fonctionnement d'un réseau de communications électroniques d'un équipement terminal par l'introduction, la transmission, la modification, la suppression, l'altération des données.

Art. 68. – (1) Est puni d'un emprisonnement de cinq (05) à dix (10) ans et d'une amende de 10.000.000 (dix millions) à 50.000.000 (cinquante millions) f cfa ou de l'une de ces deux peines seulement, celui qui accède ou se maintient, frauduleusement, dans tout ou partie d'un réseau de communications électroniques ou d'un système d'information en transmettant, endommageant, provoquant une perturbation grave ou un interruption du fonctionnement dudit système ou dudit réseau.

(2) Les peines prévues à l'alinéa 1 ci-dessus sont doublées s'il en est résulté, soit la suppression ou la modification des données contenues dans le système d'information, soit une altération de son fonctionnement.

Art. 69. – Est puni d'un emprisonnement de cinq (05) à dix (10) ans et d'une amende de

10.000.000 (dix millions) à 100.000.000 (cent millions) f cfa ou de l'une de ces deux peines seulement, celui qui accède sans droit, et en violation des mesures de sécurité, à l'ensemble ou à une partie d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal, afin d'obtenir des informations ou des données, en relation avec un système d'information connecté à un autre système d'information.

Art. 70 – Est puni d'une amende de 1.000.000 (un million) à 5.000.000 (cinq millions) f cfa, celui qui provoque par saturation, l'attaque d'une ressource de réseau de communications électroniques ou d'un système dans le but de l'effondrer en empêchant la réalisation des services attendus.

Art. 71. – Est puni d'un emprisonnement de deux (02) à cinq (05) ans et d'une amende de 1.000.000 (un million) à 25.000.000 (vingt cinq millions) f cfa, celui qui introduit sans droit, des données dans un système d'information ou dans un réseau de communications électroniques en vue de supprimer ou de modifier les données qui en sont contenues.

Art. 72. – Est puni des peines prévues par l'article 66 ci-dessus celui qui, de quelque manière que ce soit, sans droit, introduit, altère, efface, ou supprime, afin d'obtenir un bénéfice économique, les données électroniques, de manières à causer un préjudice patrimonial à autrui.

Art. 73. – (1) Est puni d'un emprisonnement de deux (02) à dix (10) ans et d'une amende de 25.000.000 (vingt cinq millions) à 50.000.000 (cinquante millions) f cfa, ou de l'une de ces deux peines seulement, celui qui, par la voie d'un système d'information ou dans un réseau de communications contrefait, falsifie une carte de paiement, de crédit, ou de retrait ou fait usage en tente de faire usage en connaissance de cause, d'une carte de paiement, de crédit ou de retrait contrefaite ou falsifiée.

(2) Est puni des peines prévues à l'alinéa 1 ci-dessus, quiconque, en connaissance de cause, accepte de recevoir par voie de communications électroniques, un règlement au moyen d'une carte de paiement, de crédit ou de retrait contrefaite ou falsifiée.

Art. 74 (1) Est puni d'un emprisonnement de un (01) à deux (02) ans et d'une amende de 1.000.000 (un million) à 5.000.000 (cinq millions) f cfa, quiconque, au moyen d'un procédé quelconque porte atteinte à l'intimité de la vie privée d'autrui en fixant, enregistrant ou transmettant, sans le consentement de leur auteur, les données électroniques ayant un caractère privé ou confidentiel.

(2) Sont passibles des peines prévues à l'alinéa 1 ci-dessus les personnes qui, sans droit, interceptent des données personnelles lors de leur transmission d'un système d'information à un autre ;

(3) Est puni d'un emprisonnement d'un (01) à trois (03) ans et d'une amende de 1.000.000 (un million) à 5.000.000 (cinq millions) f cfa ou de l'une de ces deux peines seulement, quiconque procède ou fait procéder, même par négligence au traitement des données à caractère personnel en violation des formalités préalables à leur mise en œuvre.

(4) Est puni d'un emprisonnement de six (06) mois à deux (02) ans et d'une amende de 1.000.000 (un million) à 5.000.000 (cinq millions) f cfa ou de l'une de ces deux peines seulement, le fait de collecter par des moyens illicites, des données nominatives d'une personne en vue de porter atteinte à son intimité et à sa considération.

(5) Les peines prévues à l'alinéa 4 ci-dessus sont doublées, à l'encontre de celui qui met, fait mettre en ligne, conserve ou fait conserver en mémoire informatisée, sans l'accord exprès de l'intéressé, des données nominatives qui, directement ou indirectement, font apparaître ses origines tribales, ses opinions politiques, religieuses, ses appartenances syndicales ou ses mœurs.

(6) Les peines prévues à l'alinéa 5 ci-dessus, s'appliquent aux personnes qui détournent les informations, notamment, à l'occasion de leur enregistrement, de leur classement, de leur transmission.

Loi n° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun

(7) Est puni d'un emprisonnement de six (06) mois à deux (02) ans et d'une amende de 5.000.000 (cinq millions) à 50.000.000 (cinquante millions) fca ou de l'une de ces deux peines seulement, celui qui conserve des informations sous une forme nominative ou chiffrée au-delà de la durée légale indiquée dans la demande d'avis ou la déclaration préalable à la mise en œuvre du traitement automatisé.

(8) Est puni des peines prévues à l'alinéa 7 ci-dessus, le fait de divulguer des données nominatives portant atteinte à la considération de la victime.

Art. 75 (1) - Est puni d'un emprisonnement de deux (02) à cinq (05) ans et d'une amende de 1.000.000 (un million) à 5.000.000 (cinq millions) fca ou de l'une de ces deux peines seulement, celui qui enregistre et diffuse à but lucratif, par la voie de communications électroniques ou d'un système d'information sans le consentement de l'intéressé, des images portant atteinte à l'intégrité corporelle.

(2) Le présent article n'est pas applicable lorsque l'enregistrement et la diffusion résultent de l'exercice normal d'une profession ayant pour objet d'informer le public ou sont réalisés afin de servir de preuve en justice conformément aux dispositions du Code de procédure pénale.

Art. 76. - Est puni d'un emprisonnement de cinq (05) à dix (10) ans et d'une amende de 5.000.000 (cinq millions) à 10.000.000 (dix millions) fca ou de l'une de ces deux peines seulement, celui qui confectionne, transporte, diffuse, par voie de communications électroniques ou d'un système d'information, un message à caractère pornographique infantile, ou de nature à porter gravement atteinte à la dignité d'un enfant.

Art. 77. - Est puni d'un emprisonnement de deux (02) à cinq (05) ans et d'une amende de 2.000.000 (deux millions) à 5.000.000 (cinq millions) fca ou de l'une de ces deux peines seulement, celui qui, par la voie de communications électroniques ou d'un système d'information, commet un outrage à l'encontre d'une race ou d'une religion.

(2) Les peines prévues à l'alinéa 1 ci-dessus sont doublées lorsque l'infraction est commise dans le but de susciter la haine ou le mépris entre les citoyens.

Art. 78. (1) Est puni d'un emprisonnement de six (06) mois à deux (02) ans et d'une amende de 5.000.000 (cinq millions) à 10.000.000 (dix millions) fca ou de l'une de ces deux peines seulement, celui qui publie ou propage par voie de communications électroniques ou d'un système d'information, une nouvelle sans pouvoir en rapporter la preuve de véracité ou justifier qu'il avait de bonnes raisons de croire à la vérité de ladite nouvelle.

(2) Les peines prévues à l'alinéa 1 ci-dessus sont doublées lorsque l'infraction est commise dans le but de porter atteinte à la paix publique.

Art. 79. - Les peines réprimant les faits d'outrage privé à la pudeur prévus à l'article 295 du Code pénal, sont un emprisonnement de cinq (05) à dix (10) ans et d'une amende de 5.000.000 (cinq millions) à 10.000.000 (dix millions) fca ou de l'une de ces deux peines seulement, lorsque la victime a été mise en contact avec l'auteur desdits faits, grâce à l'utilisation des communications électroniques ou des systèmes d'information.

Art. 80. (1) Est puni d'un emprisonnement de trois (03) à six (06) ans et d'une amende de 5.000.000 (cinq millions) à 10.000.000 (dix millions) fca ou de l'une de ces deux peines seulement, celui qui diffuse, fixe, enregistre ou transmet à titre onéreux ou gratuit l'image présentant les actes de pédophilie sur un mineur par voie de communications électroniques ou d'un système d'information.

(2) Est puni des mêmes peines prévues à l'alinéa 1 ci-dessus, quiconque offre, rend disponible ou diffuse, importe ou exporte, par quelque moyen électronique que ce soit, une image ou une représentation à caractère pédophile.

(3) Est puni d'un emprisonnement de un (01) à cinq (05) ans et d'une amende de 5.000.000 (cinq millions) à 10.000.000 (dix millions) fca ou de l'une de ces deux peines seulement, celui

qui détient dans un réseau de communications électroniques ou dans un système d'informations, une image ou une représentation à caractère pédophile.

(4) Les peines prévues à l'alinéa 3 ci-dessus sont doublées lorsqu'il a été utilisé un réseau de communications électroniques pour la diffusion de l'image ou la représentation du mineur à destination du public.

(5) Les dispositions du présent article sont également applicables aux images pornographiques mettant en scène les mineurs.

Art. 81. (1) Sont punis des peines prévues à l'article 82 ci-dessous, les faits ci-dessous, lorsqu'ils sont commis en utilisant un réseau de communication électroniques ou un système d'information :

- l'offre, la production, la mise à disposition de pornographie infantile en vue de sa diffusion ;

- le fait de se procurer ou de procurer à autrui de la pornographie infantile par le biais d'un système d'information ;

- le fait pour les personnes majeures de faire des propositions sexuelles à des mineurs de moins de quinze (15) ans ou une personne se présentant comme telle ;

- la diffusion ou la transmission de pornographie infantile par le biais d'un système d'information.

(2) Est considéré comme pornographie infantile, tout acte présentant de manière visuelle :

- un mineur se livrant à un comportement sexuellement explicite ;

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

- des images réalistes présentant un mineur se livrant à un comportement sexuellement explicite.

Art. 82. - Est puni du double des peines prévues à l'article 79 de la présente loi celui qui commet ou tente de commettre par voie de communications électroniques un outrage à la pudeur sur un mineur de moins de quinze (15) ans.

Art. 83. - (1) Est puni d'un emprisonnement d'un (01) à deux (02) ans et d'une amende de 500.000 (cinq cent mille) à 1.000.000 (un million) fca ou de l'une de ces deux peines seulement, celui qui par voie de communications électroniques, fait des propositions sexuelles à une personne de son sexe.

(2) Les peines prévues à l'alinéa 1 ci-dessus, sont doublées lorsque les propositions ont été suivies de rapports sexuels.

Art. 84. - (1) Est puni d'un emprisonnement de six mois (06) à deux (02) ans et d'une amende de 500.000 à 1.000.000 fca ou de l'une de ces deux peines seulement, celui qui accède, prend frauduleusement connaissance, retarde l'accès ou supprime les communications électroniques adressées à autrui.

(2) Est puni des mêmes peines prévues à l'alinéa 1 ci-dessus, celui qui intercepte sans autorisation, détourne, utilise ou divulgue les communications électroniques émises, ou reçues par des voies électroniques ou procède à l'installation d'appareils conçus pour réaliser de telles interceptions.

Art. 85. - Est puni des peines prévues à l'article 84 ci-dessus, celui qui, chargé d'une mission de service public, agissant dans l'exercice ou l'occasion de l'exercice de ses fonctions, détourne ou facilite le détournement, la suppression ou l'accès aux communications électroniques ou la révélation du contenu de ces communications.

Art. 86. - (1) Est puni des peines prévues l'article 71 ci-dessus, celui qui importe, détient, offre, cède, vend ou met à disposition, sous quelque forme que ce soit, un programme informatique, un mot de passe, un code d'accès ou toutes données informatiques similaires conçus et ou spécialement adaptés, pour permettre d'accéder, à tout ou partie d'un réseau de communication électroniques ou d'un système d'information.

(2) Est également puni des mêmes peines prévues à l'alinéa 1 ci-dessus, quiconque provoque une perturbation grave ou une interruption d'un réseau de communications électroniques ou d'un système d'information dans l'intention de porter atteinte à l'intégrité des données.

Art. 87. - Les auteurs de l'une des infractions prévues à l'article 86 ci-dessus encourrent égale-

ment les peines complémentaires suivantes :

- la confiscation selon les modalités prévues par l'article 35 du Code pénal, de tout objet ayant servi ou destiné à commettre l'infraction ou considéré comme un étant le produit, à l'exception des objets susceptibles de restitution ;

- l'interdiction dans les conditions prévues par l'article 36 au Code pénal, pour une durée de cinq (05) ans au moins, d'exercer une fonction publique ou une activité socioprofessionnelle, lorsque les faits ont été commis dans l'exercice ou à l'occasion de l'exercice des fonctions ;

- la fermeture, dans les conditions prévues par l'article 34 du Code pénal pour une durée de cinq (05) ans au moins, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

- l'exclusion ; pour une durée de cinq (05) ans au moins, des marchés publics ;

Art. 88. - (1) Est puni d'un emprisonnement de (01) à cinq (05) ans et d'une amende de 100.000 (cent mille) à 1.000.000 (un million) fca ou de l'une de ces deux peines seulement, celui qui, ayant connaissance de la convention secrète de déchiffrement, d'un moyen de cryptographie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, refuse de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités.

(2) Si le refus est opposé alors que la remise ou la mise en œuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, les peines prévues à l'alinéa 1 ci-dessus, sont portées de trois (03) à cinq (05) ans d'emprisonnement et l'amende de 1.000.000 (un million) à 5.000.000 (cinq millions) fca.

Art. 89. - Le sursis ne peut être accordé pour les infractions prévues dans la présente loi.

Titre IV

De la coopération et de l'entraide judiciaire internationales

Chapitre I

De la coopération internationale

Art. 90. - (1) Dans le cadre de l'exercice de leurs activités, les autorités de certification camerounaises peuvent, sous le contrôle de l'agence, établir des conventions, avec les autorités de certification étrangères.

(2) Les modalités d'établissement des conventions prévues à l'alinéa 1 ci-dessus sont déterminées par voie réglementaire.

Chapitre II

De l'entraide judiciaire internationale

Art. 91. (1) A moins qu'une convention internationale à laquelle le Cameroun est partie n'en dispose autrement, les demandes d'entraide émanant des autorités judiciaires camerounaises et destinées aux autorités judiciaires étrangères sont transmises par l'intermédiaire du ministère chargé des relations extérieures. Les pièces d'exécution sont renvoyées aux autorités de l'Etat requérant par la même voie.

(2) Les demandes d'entraide émanant des autorités judiciaires étrangères et destinées aux autorités judiciaires camerounaises doivent être présentées par la voie diplomatique par le gouvernement étranger intéressé. Les pièces d'exécution sont renvoyées aux autorités de l'Etat requérant par la même voie.

(3) En cas d'urgence, les demandes d'entraide demandées par les autorités camerounaises ou étrangères peuvent être transmises directement aux autorités de l'Etat requis pour leur exécution. Le renvoi des pièces d'exécution aux autorités compétentes de l'Etat requérant est effectué selon les mêmes modalités.

(4) Sous réserve des conventions internationales, les demandes d'entraide émanant des autorités judiciaires étrangères et destinées aux autorités judiciaires camerounaises doivent faire l'objet d'un avis de la part du gouvernement étranger intéressé. Cet avis est transmis aux autorités ju-

diciaires compétentes par voie diplomatique.

(5) En cas d'urgence, les demandes d'entraide émanant des autorités judiciaires étrangères sont transmises au procureur de la République ou au juge d'instruction territorialement compétent.

(6) Si le procureur de la République reçoit directement d'une autorité étrangère, une demande d'entraide qui ne peut être exécutée que par le juge d'instruction, il la transmet pour exécution à ce dernier ou saisit le procureur général dans le cas prévu à l'article 94 de la présente loi.

(7) Avant de procéder à l'exécution d'une demande d'entraide dont il a été directement saisi, le juge d'instruction la communique immédiatement pour avis au procureur de la République.

Art. 92 (1) Les demandes d'entraide émanant des autorités judiciaires étrangères sont exécutées par le Procureur de la République ou par les officiers ou agents de police judiciaire requis à cette fin par ce magistrat.

(2) Elles sont exécutées par le juge d'instruction ou par des officiers de police judiciaire agissant sur commission rogatoire de ce magistrat lorsqu'elles nécessitent certains actes de procédure qui ne peuvent être ordonnés ou exécutés qu'au cours d'une instruction préparatoire.

Art. 93 (1) Les demandes d'entraide émanant des autorités judiciaires étrangères sont exécutées selon les règles de procédure prévues par le Code de procédure pénale.

(2) Toutefois, si la demande d'entraide le précise, elle est exécutée selon les règles de procédure expressément indiquées par les autorités compétentes de l'Etat requérant, sans que ces règles ne réduisent les droits des parties ou les garanties procédurales prévues par le Code de Procédure Pénale.

(3) Lorsque la demande d'entraide ne peut être exécutée conformément aux exigences de l'Etat requérant, les autorités compétentes camerounaises en informent sans délai les autorités de l'Etat requérant et indiquent dans quelles conditions la demande pourrait être exécutée.

(4) Les autorités camerounaises compétentes et celles de l'Etat requérant peuvent ultérieurement s'accorder sur la suite à réserver à la demande, le cas échéant, en la subordonnant au respect desdites conditions.

(5) L'irrégularité de la transmission de la demande d'entraide ne peut constituer une cause de nullité des actes accomplis en exécution de cette demande.

Art. 94 (1) Si l'exécution d'une demande d'entraide émanant d'une autorité judiciaire étrangère est de nature à porter atteinte à l'ordre public ou aux intérêts essentiels de la Nation, le Procureur de la République saisi ou avisé de cette demande, la transmet au Procureur général en saisit le ministre chargé de la Justice et donne, le cas échéant, avis de cette transmission au Procureur de la République.

(2) S'il est saisi, le ministre chargé de la Justice informe l'autorité requérante, le cas échéant, de ce qu'il ne peut être donné suite, totalement ou partiellement, à sa demande. Cette information est notifiée à l'autorité judiciaire concernée et fait obstacle à l'exécution de la demande d'entraide ou au retour des pièces d'exécution.

Titre V

Dispositions transitoires et finales

Art. 95. Des textes d'application fixent, en tant que de besoin, les modalités d'application de la présente loi.

Art. 96. Les autorisations et les déclarations de fourniture, d'importation et d'exportation de moyens de cryptographie délivrées par les autorités compétentes demeurent valables jusqu'à l'expiration du délai prévus par celles-ci.

Art. 97. La présente loi sera enregistrée et publiée suivant la procédure d'urgence, puis insérée au Journal officiel en français et en anglais.

Yaounde, le 21 Décembre 2010
Le président de la République,
(é) Paul BIYA

Law N° 2010/021 of 21 December 2010 on Electronic Commerce in Cameroon

The National Assembly deliberated and adopted, the President of the Republic hereby enacts the law set out below:

Part I – General Provisions

Section 1: This law governs electronic commerce in Cameroon.

Section 2: For the purposes of this law and its implementing instruments, the following terms shall mean:

Commercial Activity: Any activity for the production and exchange of goods and services carried out using electronic or material media, by any natural person or corporate body in accordance with the provisions of the laws, regulations and conventions governing trade;

Certification Authority: The body entrusted with the mission of generating and allocating public and private electronic keys and certificates;

Electronic Certificate: An electronic document protected by the electronic signature of the person who issued it and which attests, upon verification, to the authenticity of its content;

Qualified electronic Certificate: An electronic certificate issued by an authorized certification structure;

Client: Any natural person or corporate body using electronic means to conduct business with a trader;

Electronic Commerce: A commercial activity whereby a person uses electronic means to supply or ensure the supply of goods or services;

Commercial Communication: Any form of communication intended to directly or indirectly promote the goods, services or image of a company, an organization or an individual having a commercial, industrial, artisanal activity or engaged in a regulated profession;

Consumer: Any natural person or corporate body benefiting from the services or using commercial products to satisfy his personal needs or those of his dependants;

Electronic Mail: Any text, voice, audio or video message sent through a communication network, stored in a server of the network or in the terminal equipment of the addressee until the latter retrieves it;

Service Addressee: Any natural person or corporate body who, for professional purposes or otherwise, uses electronic means, in particular, to search for information or make it accessible;

Electronic signature generating system: All the equipment and/or private encrypting software approved by a competent authority, intended for the creation of electronic signatures;

Electronic signature verification system: All the equipment and/or public encrypting software authorized by a competent authority, which a certification authority uses to ascertain an electronic signature.

Electronic Document: All the data stored or saved in the memory of any media by a computer system or similar mechanism and which may be read or seen by a person or such a system or mechanism. This shall also include bill-posting and print-outs or any other such data;

Data relating to the creation of signatures: Unique data such as codes or private cryptographic keys, which the signatory uses to generate an electronic signature;

Electronic Correspondence: Exchanges conducted through electronic documents;

Electronic Data Interchange (EDI): Electronic transmission of information from computer to computer according to agreed standard rules for structuring information;

Data Message: Information created, sent, received or stored using electronic, optical or analog means, in particular, but not exclusively, the electronic data interchange (EDI), electronic messaging, telegraphy, telex and telecopy;

Electronic means of payment: Means enabling its holder to carry out distance payments through telecommunications networks;

Electronic signature product: Any material product, software or specific element of the said product, intended to be used by a certification service provider to deliver electronic signature services, or intended to be used in creating or

verifying electronic signatures;

Commercial Advertising: Information published using various media to make a product or service known, with a view to encouraging the public to buy or use it;

Electronic Signatory: The person who owns a signature generating device and who acts either in his personal name or as a representative of a natural person or corporate body;

Electronic Signature: Signature obtained by an asymmetrical encryption algorithm that helps to authenticate the sender of a message and verify the integrity thereof;

Information System: Any isolated device or group of interconnected or linked devices, which ensure or one or more of whose elements ensure automated data processing according to a programme.

Part II – Principles Governing the Exercise of Electronic Commerce-Related Activities

Chapter I – Restrictions and Exceptions

Section 3 (1): The exercise of electronic commerce shall be free, to the exclusion:

- legally authorized money games, betting and lotteries;
- activities concerning legal representation and aid;
- activities carried out by notaries public.

(2) The exercise of electronic commerce shall be subject to compliance with the provisions relating to:

- conditions for setting up and operating an insurance business, as provided for under relevant international and national instruments;
- anti-trust practices and economic concentration;
- the prohibition or authorization of unsolicited advertising sent by electronic mail;
- the Customs Code of the Central African Economic and Monetary Community;
- the General Tax Code;
- rights protected by intellectual property laws and regulations.

Section 4: Under the conditions laid down by regulation, the administrative authority may, on a case by case basis, take restrictive measures on the free exercise of electronic commerce activities in case of disturbance or serious and great risk of undermining public order and security, the protection of minors, public health, defence of national interest or the protection of natural persons.

Chapter II – Electronic Advertising

Section 5(1): Any advertisement that is accessible through an online service shall clearly identify:

- the said advertisement;
- the natural person or corporate body for whom the advertisement is made;
- the promotional offers such as discounts, premiums or gifts, as well as competitions or promotional games, the conditions for participation of which shall be easily accessible, precise and unambiguous.

(2) The provisions of Section 5(1) shall apply without prejudice to the provisions that punish misleading advertising.

Section 6: Unsolicited advertising material made by a service provider by electronic mail shall be clearly and unequivocally identified once the addressee receives it.

Section 7(1): It shall be forbidden to engage in direct prospecting through a call processor, fax machine or an electronic mail using the address, in any form whatsoever, of a natural person or corporate body that has not expressed prior consent to receive direct prospecting by such means.

(2) Direct prospecting shall mean sending any message intended to directly or indirectly promote goods, services or the image of a person selling goods or providing services.

Section 8 (1): Members of regulated professions shall be authorized to use advertising in the exercise of their activities, subject to compliance

with professional rules of independence, dignity and honour of the profession as well as confidentiality and loyalty to customers and the other members of the profession.

(2) Professional organizations and associations shall prepare the codes of conduct to specify the information which may be provided for advertising purposes in compliance with the rules referred to in Section 8(1) above.

Chapter III – Contracts Signed by Electronic Means

Section 9: The signing of contracts by electronic means shall be allowed subject to the conditions laid down by the laws and regulations in force.

Section 10: The regime of written contracts shall apply to electronic contracts in terms of consent, their legal effect, validity and implementation, except for the following contracts:

- contracts which create or transfer rights over immovable property, except for renting rights ;
- contracts for which the law requires the intervention of courts, public authorities or professionals exercising public authority;
- surety and guarantee contracts produced by persons acting for purposes not coming under their professional or commercial activity;
- contracts governed by family law and succession law.

Section 11 (1): Bids made electronically concerning the supply of goods and services shall be accompanied by the contractual conditions applicable thereto such that they can be stored and reproduced. Without prejudice to the conditions of validity mentioned in the said bids, the authors of the bids shall remain bound as long as remaining accessible online is their own doing.

(2) The bids referred to in Section 11 (1) above shall clearly specify:

- the various steps to follow in concluding an electronic contract;
- the technical means that helps the user to spot any errors made in keying in data and to correct them before concluding the contract;
- the proposed language(s) for concluding the contract;
- in case of archiving the contract, the conditions for such archiving by the author of the bid and the conditions for accessing the contracts in the archives;
- the means for electronically consulting the professional and commercial rules which the author of the bid undertakes, where necessary, to abide by.

(3) The general contractual terms and conditions must be provided to the addressee such that it can keep and reproduce them.

(4) Sub-sections (1) and (2) of Section 11 above shall not apply to contracts signed exclusively through the exchange of electronic mail or through equivalent individual messages. There may also be exceptions to the provisions of the said sub-sections in agreements signed between professionals.

Section 12 (1): A contract may be deemed to be validly concluded only if the addressee of the bid previously had the possibility of verifying the details and total price of its order, and correcting any errors before confirming the bid to express acceptance.

(2) The author of the bid shall, within a period of no more than 5(five) days, acknowledge online receipt of the order addressed to it.

(3) The order, confirmation of acceptance of the bid and acknowledgement of receipt shall be deemed to have been received when the parties to which they are addressed can access them.

(4) Sub-sections (1) and (2) of Section 11 above shall not apply to contracts concluded exclusively through the exchange of electronic mail or through equivalent individual messages. There may also be exceptions to the provisions of the said sub-sections in agreements signed between professionals.

Section 13 (1): Where a paper document is required for the validity of a legal act, it may be issued and kept in an electronic form under the

conditions stipulated in Sections 1317 et seq. of the Civil Code, relating to written proof.

(2) Where a handwritten note is required, even by the person making the undertaking, the latter may append the note electronically where the conditions for appending the note are such as to guarantee that it can be done solely by such person, except for the provisions of Section 13 (1) above for :

- private agreements relating to family law and succession law;
- private agreements relating to personal or real sureties, civil or commercial, save where they are signed by an individual for the purposes of its profession.

Section 14: Where the contract is concluded electronically and concerns an amount equal to or exceeding that fixed by regulation, the professional contracting party shall keep the ascertaining paper version for a period equally specified by regulation and ensure access thereto at all times by its contracting party if the latter so requests.

Chapter IV – Electronic Commercial Transactions

Section 15 (1): Prior to the conclusion of a contract, the seller shall be bound, during electronic commercial transactions, to provide the consumer with the following information in a clear and intelligible manner:

- the identity, address and telephone number of the seller or service provider;
- a complete description of the states for the conduct of the transaction;
- the nature, characteristic and price of the product;
- the cost of delivery and, where applicable, the insurance rates of the product and the required taxes;
- the duration of validation of the supply of the product at fixed prices;
- the conditions of commercial guarantees and after sales service;
- the payment conditions and procedures and, where applicable, the proposed credit conditions;
- the conditions and deadlines for delivery, execution of the contract and the consequences of failure to honour the commitments;
- the possibility of revocation and its timeframe;
- the procedure for confirming the order;
- the procedure for returning the product, change of product or refund;
- the cost of using telecommunication means where they are assessed using a reference other than the applicable rate;
- the conditions for terminating the contract where it is signed for an unspecified period or for a period of over 1 (one) year;
- the minimum contract period for contracts relating to long-term or periodic supply of a product or service.

(2) The information under sub-section (1) above must be provided electronically and put at the disposal of the consumer for consultation at all stages of the transaction.

Section 16 (1): It shall be prohibited for the seller to deliver a product not ordered by the consumer where it is accompanied by a request for payment.

(2) In case of delivery of a product not ordered by the consumer, the latter may not be requested to pay its price or the cost of its delivery.

(3) The cost of returning products delivered without any order shall be borne by the seller.

Section 17: Before concluding a contract, the seller shall allow the consumer to make a final statement of all its choices, confirm or modify the order as it may desire and consult the electronic certificate relating to its signing.

Section 18: Unless otherwise agreed by the parties, the contract shall be concluded at the address of the seller and on the date of acceptance of the order by the latter through an electronic document signed and addressed to the consumer.

Section 19: The seller shall have a period of 10

Law N° 2010/021 of 21 December 2010 on Electronic Commerce in Cameroon

(ten) days with effect from the date of signature of the contract to provide the consumer, at the request of the latter, with a paper or electronic document containing all the information relating to the sales operation.

Section 20 (1): Subject to the provisions of section 15 above, the consumer may revoke its order within a period of 15 (fifteen) days :

- for goods, with effect from the day following the date the consumer receives them;
- for services, with effect from the date of conclusion of the contract.

(2) The revocation notice shall be transmitted electronically or by any other relevant means.

(3) Where the goods have not been damaged by the consumer, the seller shall be bound to refund the amount received within 15 (fifteen) days from the date of return of the goods or the revocation of the service.

(4) The consumer shall bear the cost of returning the goods.

Section 21: Subject to payment of damages to the consumer, the latter may, within 15 (fifteen) days of the date of delivery, return the product as it is where it does not meet the conditions of the order or where the seller has failed to deliver on schedule.

In such a case, the seller must refund the amounts received to the consumer within 15 (fifteen) clear days of the date of return of the product.

Section 22: Subject to Section 15 of this law and save in cases where the sales contract or the goods and services arising there from may contain obvious or hidden defects, the consumer may not renounce the order where it:

- requests the service to be delivered prior to the expiry of the deadline for revocation and the seller acted accordingly;
- receives products manufactured accordingly to personalized deteriorated or expired due to the expiry of the validity periods;
- detects delivered or downloaded audio or video recordings or computer software;
- buys newspapers and magazines.

Section 23: Where the sales operation is wholly or partially covered by a loan granted to the consumer by the seller or by a third party under a contract concluded between the seller and the third party, revocation by the consumer shall be tantamount to termination, without penalty, of the loan agreement.

Section 24: Save in cases of improper use, the seller shall bear, in case of sale after testing, the risks to which the product may be exposed and this, up to the end of the testing period of the product.

All disclaimer clauses repugnant to the provisions of this section shall be null and void.

Section 25 (1): Where the product or service ordered is unavailable, the seller shall inform the customer or consumer at least 24 (twenty-four) hours before the delivery date set in the purchase or service contract. Where applicable, the seller or service provider shall refund to the customer

the total of amounts received for the delivery of the product or provision of the service.

(2) In case of force majeure, the contract shall be terminated where the seller fails to honour its commitments and the consumer shall be reimbursed all amounts paid, without prejudice to damages.

Section 26: The seller must prove the existence of prior information, confirmation of the information listed in Section 15 above, compliance with timeframes and the consent of the consumer. Any agreement repugnant hereto shall be null and void.

Section 27: Payment operations may be carried out in public services electronically under the conditions laid down by the laws and regulations in force.

Section 28 (1) : The holder of the electronic means of payment shall notify the issuer of the loss or theft of the said means or instruments used to operate it, as well as any fraudulent use it is aware of.

(2) The issuer of an electronic means of payment shall include the appropriate means for such notification in the contract concluded with its holder.

Section 29(1): Cases of fraud notwithstanding, the holder of the electronic means of payment shall :

- until notifies the issuer, assume responsibility for the loss or theft of the means of payment or the fraudulent use thereof by a third party;
- be released from all responsibility for the use of the electronic means of payment after notifying the issuer.

(2) The use of the electronic means of payment without presentation of the said means of payment and identification by electronic means shall not commit its holder.

Part III – Responsibility of Service Providers and Intermediaries

Chapter I – Obligation to Inform

Section 30 (1) : Without prejudice to other obligations to inform provided for by the laws and regulations in force, any person operating as a service provider in the domain of electronic commerce shall be bound to ensure that the end-users of the said service and the authorities have easy, direct and permanent access to the following minimum information:

- in case of a natural person, his/her full name and, in case of a corporate body, its company name, physical address, email address and its telephone number;
- where it is subject to the formalities for registration in the trade and personal property credit register, its registration number, its registered capital and head office address;
- where it is subject to the value added tax and identified by an individual number in keeping with Book I of the General Tax Code, its taxpayer's number;
- where its activity is subject to an authorization regime, the name and address of the authority

that issued the authorization;

- where he/she is a member of a regulated profession, reference to the applicable professional rules, his/her professional title, the name and order or the professional organization to which he/she belongs.

(2) The obligations to inform and forward the contractual conditions referred to in Section 11 and Section 30 (1) above shall be fulfilled electronically in accordance with the conditions laid down by regulation.

Section 31: Subject to the conditions for setting rates and taxes under the laws and regulations in force, any person operating as a service provider in the domain of electronic commerce shall, even in the absence of an offer of contract, as long as he/she indicates a price, do so clearly and unequivocally and, in particular, where the delivery taxes and fees are included.

Section 32: Every service provider shall be bound to store and keep data relating to any commercial transaction carried out by electronic means in accordance with the laws and regulations in force.

Chapter II – Storage, conservation and Transmission of Data

Section 33: Any natural person or corporate body engaged in automatic, intermediate and temporary storage for the sole purpose of making subsequent transmission of contents more efficiently shall not be criminally or vicariously liable for such contents, except in the following cases:

- it has modified the contents, failed to keep to their conditions for access and the usual rules for updating them or has obstructed the authorized and ordinary use of the technology used to obtain data;
- it has failed to act promptly to remove the contents he/she stored or make access thereto impossible, once it effectively became aware either of the fact that the contents transmitted initially have been removed from the network or due to the fact that it has become impossible to access the contents transmitted initially, either on account of the judicial authorities having ordered removal from the network of the contents transmitted initially or denial of access thereto.

Section 34(1): The electronic document shall be stored on an electronic medium making it possible to:

- consult its content throughout its validity period;
 - keep it in its final form in order to ensure the integrity of its content, conserve the information relating to its provenance and destination as well as the date and place of its issuance or reception.
- (2) The conservation of the electronic document as well as that of the paper document shall be authentic.

(3) The issuer shall undertake to keep the electronic document in the format in which it was issued. The addressee shall undertake to keep the electronic document in the format in which it is received.

Part IV – Securing and Authentication of Data and Information

Chapter I – Electronic Certificate and Signature

Section 35 (1): Any natural person or corporate body shall be authorized to use the electronic certificate and signature in electronic commerce under the conditions laid down by a separate instrument.

(2) Official documents may be authenticated in government services using electronic certificates and signatures under conditions laid down in separate instruments.

Section 36: Anyone using an electronic signature device shall:

- take the minimum precautionary measures set forth in the instruments in force to avoid any unauthorized use of the personal equipment concerning its signature;
- report any unauthorized use of its signature to the certification authority;
- ensure the accuracy of all the information it provides to the said authority;
- ensure the veracity of all the information it pro-

vided to any person whom it has asked to rely on its signature.

Section 37 : In case of violation of the provisions of Section 36 above, the holder of the signature shall be held responsible for the tort caused another person.

Section 38: The conditions for exercising the activities of certification authority shall be laid down in a separate instrument.

Section 39: The certification authority shall keep an electronic register of certificates at the disposal of users.

Chapter II – Equivalences

Section 40 (1): The certificates and signatures issued by a certification authority based abroad shall have the same value as those issued by a certification authority based in Cameroon, where such an authority is recognized under a mutual recognition agreement signed by the competent authorities of the States concerned.

(2) The conditions for the legal recognition of electronic certificates and signatures issued from third countries shall be defined in a separate instrument by default.

Part V – Establishing Offences and Penalties

Section 41 (1): All violations of the provisions of this law and its implementing instruments shall be established by criminal investigation officers with general jurisdiction, sworn officers of the Ministries in charge of telecommunications and advertising, the electronic regulation and certification authority, as well as those of economic control, in accordance with the conditions set forth in the laws and regulations in force.

(2) Reports establishing offences as well as objects and documents seized shall be transmitted to the State Counsel with territorial jurisdiction.

Section 42: Whoever illegally uses the electronic signature of another shall be punished with the penalties provided in Section 219 of the Penal Code.

Section 43: Whoever is found guilty of breaching the provisions of Section 15, 17, 19, 21, 24 and 25 of this law shall be punished with a fine of from 250 000 to 2 500 000 FCFA francs.

Section 44 : Whoever takes advantage of the weakness or ignorance of another to make him/her enter, through an electronic sale, into commitments in cash or on credit in any form whatsoever, where it is proven that such a person is not capable of appreciating the extent of the commitments he/she is making or detecting the trick or tactics being used to convince him/her to subscribe thereto or that he/she was under duress shall be punished with the penalties set forth in Section 349 of the Penal Code.

Section 45 : The certification authority and/or its officers who disclose, cause or participate in the disclosure of information entrusted to them within the framework of the exercise of their activities shall be punished with the penalties provided in Section 310 of the Penal Code, except for those whose publication or communication are authorized by the older of the certificate either in writing, by electronic means or in the cases provided by the law in force.

Section 46: Any violation of the provisions of Sections 9 and 10 of this law shall be punished with the penalties set forth in Sections 37 and 38 of Law No. 90/31 of 10 August 1990 governing commercial activity.

Part VI – Transitional and Final Provisions

Section 47: Any natural person or corporate body engaged in electronic commerce on the date of enactment of this law shall have a period of 6 (six) months within which to comply with provisions.

Section 48: This law shall be registered, published according to the procedure of urgency and inserted in the Official Gazette in English and French.

Yaounde, 21 December 2010

Paul BIYA

President of the Republic

Un enfant retrouvé et pris en charge par le MINAS

Le communiqué parvenu à notre Rédaction

Le ministre des Affaires sociales a l'honneur de porter à la connaissance de l'opinion publique, que dans le cadre de La protection sociale de l'enfant, un enfant en détresse retrouvé abandonné, a été conduit dans les services opérationnels du MINAS.

Cet enfant qui continue de faire l'objet de recherche de sa famille sur l'ensemble du territoire national, est actuellement pris en charge nutritionnelle, sanitaire et psychosociale dans les structures spécialisées de son département ministériel.

Il s'agit :

- d'un enfant de sexe masculin, âgé aujourd'hui d'environ 5 ans, répondant au nom de Nyobe Alain Joël, retrouvé le 9 décembre 2010.

Les parents ou famille de cet enfant, et toute

personne qui se sentirait concernée sont invités à prendre attache avec les services déconcentrés locaux et/ou centraux du ministère des Affaires sociales sis derrière l'ancien palais présidentiel ou appeler au 22 22 29 58, 22 23 05 35 ou 74 88 69 04 ou écrire à minascab@yahoo.fr.

Le ministre des Affaires sociales prie par ailleurs lesdits parents ou relatifs de bien vouloir se munir de tout document permettant d'établir l'existence d'un lien de filiation ou de toute autre relation avec l'enfant afin de procéder à son retour en famille.

Pour le ministre des Affaires sociales et par délégation, le secrétaire général, (é) MOUHTAR OUSMANE Administrateur civil principal