REPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie

ASSEMBLEE NATIONALE
8ème Législature
Année Législative 2010
3ème **Session Ordinaire**
(Novembre)

LOI

RELATIVE A LA CYBERSECURITE ET A LA CYBERCRIMINALITE AU CAMEROUN

L'Assemblée Nationale a délibéré et adopté,
en sa séance plénière du lundi 06 décembre 2010
le projet de loi n°862/PJL/AN dont la teneur suit :

TITRE PREMIER

DISPOSITIONS GENERALES

Article 1er. – 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.

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

Article 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.

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

1) **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 ;
2) **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 ;
3) **Algorithme** : suite d'opérations mathématiques élémentaires à appliquer à des données pour aboutir à un résultat désiré ;

4) **Algorithme asymétrique** : algorithme de chiffrement utilisant une clé publique pour chiffrer et une clé privée (différente) pour déchiffrer les messages ;
5) **Algorithme symétrique** : algorithme de déchiffrement utilisant une même clé pour chiffrer et déchiffrer les messages ;
6) **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) ;
7) **Attaque passive** : acte n'altérant pas sa cible (écoute passive, atteinte à la confidentialité) ;
8) **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 ;
9) **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 ;
10) **Authentification** : critère de sécurité défini par un processus mis en œuvre notamment pour vérifier l'identité d'une personne physique ou morale et s'assurer que l'identité correspond à l'identité de cette personne préalablement enregistrée ;
11) **Autorité de certification** : autorité de confiance chargée de créer et d'attribuer des clés publiques et privées ainsi que des certificats électroniques ;
12) **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 ;
13) **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 ;
14) **Certificat électronique qualifié** : certificat électronique émis par une autorité de certification agréée ;
15) **Certification électronique** : émission de certificats électroniques ;

16) **Chiffrement** : procédé grâce auquel on transforme à l'aide d'une convention secrète appelée clé, des informations claires en informations inintelligibles par des tiers n'ayant pas la connaissance de la clé ;
17) **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 ;
18) **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 ;
19) **Clé publique** : clé servant au chiffrement d'un message dans un système asymétrique et donc librement diffusé ;
20) **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 ;
21) **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 ;
22) **Communication audiovisuelle** : communication au public de services de radiodiffusion télévisuelle et sonore ;
23) **Communication électronique** : émission, transmission ou réception de signes, signaux, d'écrits, d'images ou de sons, par voie électromagnétique ;
24) **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 ;
25) **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 ;
26) **Contenu illicite** : contenu portant atteinte à la dignité humaine, à la vie privée, à l'honneur ou à la sécurité nationale ;
27) **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 ;
28) **Cryptage** : utilisation de codes ou signaux non usuels permettant la conservation des informations à transmettre en des signaux incompréhensibles par les tiers ;

29) **Cryptanalyse** : ensemble des moyens qui permet d'analyser une information préalablement chiffrée en vue de la déchiffrer ;
30) **Cryptogramme** : message chiffré ou codé ;
31) **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 ;
32) **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 ;
33) **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 ;
34) **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 ;
35) **Déchiffrement** : opération inverse du chiffrement ;
36) **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 ;
37) **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 ;
38) **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) ;
39) **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 ;
40) **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 ;

41) **Données** : représentation de faits, d'informations ou de notions sous une forme susceptible d'être traitée par un équipement terminal, y compris un programme permettant à ce dernier d'exécuter une fonction ;
42) **Données de connexion** : ensemble de données relatives au processus d'accès dans une communication électronique ;
43) **Données de trafic** : données ayant trait à une communication électronique indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type du service sous-jacent ;
44) **Equipement 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 ;
45) **Fiabilité** : aptitude d'un système d'information ou d'un réseau de communications électroniques à fonctionner sans incident pendant un temps suffisamment long ;
46) **Fournisseur des services de communications électroniques** : personne physique ou morale fournissant les prestations consistant entièrement ou principalement en la fourniture de communications électroniques ;
47) **Gravité de l'impact** : appréciation du niveau de gravité d'un incident, pondéré par sa fréquence d'apparition ;
48) **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 ;
49) **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 ;
50) **Interception légale** : accès autorisé aux données d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal ;
51) **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 ;
52) **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 ;

53) **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 ;
54) **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 ;
55) **Logiciel potentiellement indésirable** : logiciel présentant des caractéristiques d'un logiciel trompeur ou d'un logiciel espion ;
56) **Message clair** : version intelligible d'un message et compréhensible par tous ;
57) **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 ;
58) **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 ;
59) **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 ;
60) **Politique de sécurité** : référentiel de sécurité établi par une organisation, reflétant sa stratégie de sécurité et spécifiant les moyens de la réaliser ;
61) **Prestation de cryptographie** : opération visant à la mise en œuvre, pour le compte d'autrui, de moyens de cryptographie ;
62) **Réseau de communications électroniques** : système de transmission, actif ou passif et, le cas échéant, les équipements de commutation et de 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 ;

63) **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 ;

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

65) **Service de certification** : prestation fournie par une autorité de certification ;

66) **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 ;

67) **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 ;

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

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

70) **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 ;

71) **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 ;

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

73) **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.

Article 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 CYBERSECURITE

CHAPITRE I
DE LA POLITIQUE GENERALE DE SECURITE ELECTRONIQUE

Article 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 REGULATION ET SUIVI DES ACTIVITES DE SECURITE ELECTRONIQUE

Article 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.

Article 8. – (1) L’Agence est l’Autorité de Certification Racine.

(2) L’Agence est l’autorité de certification de l’Administration Publique.

Article 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 Electronique** », 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 développement, 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 REGIME JURIDIQUE DES ACTIVITES DE CERTIFICATION

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

Article 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.

Article 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 ACTIVITES DE SECURITE

Article 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 prévu à l'alinéa 1 ci-dessus sont définies par voie réglementaire.

Article 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 ELECTRONIQUE

Article 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.

Article 16. – (1) Les autorités de certification sont responsables du préjudice causé aux personnes qui se sont fiées aux certificats présentés par elles comme qualifiées 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 ELECTRONIQUE

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

Article 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 ELECTRONIQUES DELIVRES PAR LES AUTORITES DE CERTIFICATION

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

Article 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 ELECTRONIQUE

Article 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.

Article 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.

Article 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 RESEAUX DE COMMUNICATIONS ELECTRONIQUES, DES SYSTEMES D'INFORMATION ET DE LA VIE PRIVEE DES PERSONNES

SECTION I
DE LA PROTECTION DES RESEAUX DE COMMUNICATION ELECTRONIQUES

Article 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 communications.

Article 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 SYSTEMES D'INFORMATION

Article 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 continûment 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.

Article 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.

Article 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.

Article 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.

Article 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.

Article 31.- (1) Les fournisseurs de contenus des réseaux de communication électroniques 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.

Article 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'ACCES, DE SERVICES ET DES CONTENUS

Article 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.

Article 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.

Article 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-dessous.

(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.

Article 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.

Article 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.

Article 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.

Article 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.

Article 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 PRIVEE DES PERSONNES

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

Article 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.

Article 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.

Article 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.

Article 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.

Article 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.

Article 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.

Article 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 ELETRONIQUES

Article 49.- Nonobstant les dispositions du Code de Procédure Pénale, en cas de crimes ou délits prévus dans la présente loi, l'Officier de Police Judiciaire peut intercepter, enregistrer ou transcrire toute communication électronique.

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

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

TITRE III
DE LA CYBERCRIMINALITE

CHAPITRE I
DES DISPOSITIONS DU DROIT PROCESSUEL

Article 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.

Article 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.

Articles 54.- Les perquisitions et les saisies sont effectuées conformément aux dispositions du Code de Procédure Pénale en tenant compte du dépérissement des preuves.

Article 55.- (1) Lorsqu'il apparaît que les données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait l'objet d'opérations de transformation empêchant d'accéder en clair ou sont de nature à compromettre les informations qu'elles contiennent, le Procureur de la République, le Juge d'Instruction ou la juridiction de jugement peuvent réquisitionner toute personne physique ou morale qualifiée, en vue

d’effectuer les opérations techniques permettant d’obtenir la version en clair desdites données.

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

Article 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.

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

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

Article 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 oeuvre ces conventions, sauf si ceux-ci démontrent qu’ils ne sont pas en mesure de satisfaire à de telles réquisitions.

Article 59.- (1) Lorsque les nécessités de l’enquête ou de l’instruction le justifient, l’audition ou l’interrogatoire d’une personne et/ou la confrontation entre plusieurs personnes, peuvent être effectuées en plusieurs points du territoire national se trouvant reliés par des moyens de communications électroniques garantissant la confidentialité de la transmission. Il est dressé, dans chacun des lieux, un Procès-verbal des

opérations qui y ont été effectuées. Ces opérations peuvent faire l'objet d'enregistrement audiovisuel et/ou sonore.

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

(3) Les dispositions du 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

Article 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 commerciaux ;
- 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 concerné pourra être remis en circulation dès que les obligations antérieurement non respectées auront été satisfaites et dûment constatées par l'Agence.

Article 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) F CFA, les personnels de l'Agence et les experts des personnes

morales chargés des audits qui révèlent 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 de ces 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.

Article 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.

Article 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.

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

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

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

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

- la dissolution lorsqu'il s'agit d'un crime ou d'un délit puni en ce qui concerne les personnes physiques d'une peine d'emprisonnement supérieure ou égale à trois (03) ans et que la personne morale a été détournée de son objet pour servir de support à la commission des faits incriminés ;
- l'interdiction, à titre définitif ou pour une durée de cinq ans au moins, d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ;
- la fermeture temporaire pour une durée de cinq (05) ans au moins, dans les conditions prévues par l'article 34 du Code Pénal, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
- l'exclusion des marchés publics à titre définitif ou pour une durée de cinq (05) ans au moins ;
- l'interdiction, à titre définitif ou pour une durée de cinq (05) ans au moins, de faire appel public à l'épargne ;
- l'interdiction, pour une durée de cinq (05) ans au moins, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ou d'utiliser des cartes de paiement ;
- la confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit ;
- la publication ou la diffusion de la décision prononcée soit par la presse écrite, soit par tout moyen de communication au public par voie électronique.

Article 65.- (1) Est puni d'un emprisonnement de cinq (05) à dix (10) ans et d'une amende de 5.000.000 (cinq millions) à 10.000.000 (dix millions) F CFA ou de l'une de ces deux peines seulement, celui qui effectue, sans droit ni autorisation, l'interception par des moyens techniques, de

données lors des transmissions ou non, à destination, en provenance ou à l'intérieur ou non d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal.

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

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

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

Article 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 inaccessibles 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 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.

Article 67.- Constitue une atteinte à l'intégrité d'un réseau de communications électroniques ou d'un système d'information et punie des peines prévues à l'article 66, alinéa 1 ci-dessus, le fait de provoquer une perturbation grave ou une interruption de fonctionnement d'un

réseau de communications électroniques d'un équipement terminal par l'introduction, la transmission, la modification, la suppression, l'altération des données.

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

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

Article 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.

Article 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 d'information dans le but de l'effondrer en empêchant la réalisation des services attendus.

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

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

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

(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.

Article 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.

(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) F CFA, 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.

Article 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) F CFA 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.

Article 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) F CFA ou de l'une de ces deux peines seulement, celui qui confectionne, transporte, diffuse, par voie de communications électroniques ou d'un système d'information, un message à caractère pornographique enfantine, ou de nature à porter gravement atteinte à la dignité d'un enfant.

Article 77.- (1) 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) F CFA 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.

Article 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) F CFA 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.

Article 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 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, 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.

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

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

(3) Est puni d'un emprisonnement de un (01) à cinq (05) ans et d'une amende de 5.000.000 (cinq millions) à 10.000.000 (dix millions) F CFA ou de l'une de ces deux peines seulement, celui qui détient dans un réseau de communications électroniques ou dans un

système d'informations, une image ou une représentation à caractère pédophile.

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

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

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

- l'offre, la production, la mise à disposition de pornographie enfantine en vue de sa diffusion ;
- le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système d'information ;
- le fait pour les personnes majeures de faire des propositions sexuelles à des mineurs de moins de quinze (15) ans ou une personne se présentant comme telle ;
- la diffusion ou la transmission de pornographie enfantine par le biais d'un système d'information.

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

- un mineur se livrant à un comportement sexuellement explicite ;
- une personne qui apparaît comme mineur se livrant à un comportement sexuellement explicite ;
- des images réalistes présentant un mineur se livrant à un comportement sexuellement explicite.

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

Article 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) F

CFA 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.

Article 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 F CFA 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.

Article 85.- Est punie des peines prévues à l'article 84 ci-dessus, celui qui, chargé d'une mission de service public, agissant dans l'exercice ou à 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.

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

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

Article 87.- Les auteurs de l'une des infractions prévues à l'article 86 ci-dessus encourent également les peines complémentaires suivantes :

- la confiscation selon les modalités prévues par l'article 35 du Code Pénal, de tout objet ayant servi ou destiné à commettre

l'infraction ou considéré comme en étant le produit, à l'exception des objets susceptibles de restitution ;

- l'interdiction dans les conditions prévues par l'article 36 du Code Pénal, pour une durée de cinq (05) ans au moins, d'exercer une fonction publique ou une activité socioprofessionnelle, lorsque les faits ont été commis dans l'exercice ou à l'occasion de l'exercice des fonctions ;
- la fermeture, dans les conditions prévues par l'article 34 du Code Pénal pour une durée de cinq (05) ans au moins, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
- l'exclusion, pour une durée de cinq (05) ans au moins, des marchés publics.

Article 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) F CFA 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) F CFA.

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

TITRE IV
DE LA COOPERATION ET DE L'ENTRAIDE JUDICIAIRE INTERNATIONALES

CHAPITRE I
DE LA COOPERATION INTERNATIONALE

Article 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 règlementaire.

CHAPITRE II
DE L'ENTRAIDE JUDICIAIRE INTERNATIONALE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Article 94.- (1) Si l'exécution d'une demande d'entraide émanant d'une autorité judiciaire étrangère est de nature à porter atteinte à l'ordre public ou aux intérêts essentiels de la Nation, le Procureur de la République saisi ou

avisé de cette demande, la transmet au Procureur Général qui en saisit le Ministre chargé de la Justice et donne, le cas échéant, avis de cette transmission au Procureur de la République.

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

TITRE V
DISPOSITIONS TRANSITOIRES ET FINALES

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

Article 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 prévu par celles-ci.

Article 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

LE PRESIDENT DE L'ASSEMBLEE NATIONALE

CAVAYE YEGUIE DJIBRIL