PRESIDENCE DE LA REPUBLIQUE

Loi n° 2010-12 du 21 décembre 2010 relative à la cybersécurite 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 premier.- 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 Cámeroun.

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.

PRESIDENCY OF THE REPUBLIC

Law n° 2010-12 of 21 December relating to cybersecurity and cybercriminality 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 the security framework of electronic communication networks and information systems, defines and punishes offences related to the use of information and communication technologies in Cameroon.

Accordingly, it seeks notably to:

- build trust in electronic communication networks and information systems;

- establish the legal regime of digital evidence, security, cryptography and electronic certification activities;

- protect basic human rights, in particular the right to human dignity, honour and respect of privacy, as well as the legitimate interests of corporate bodies.

Section 2. This law shall not cover the specific applications used in national defence and security.

Section 3. The electronic communication networks targeted by this law shall include: satellite, ground and electronic networks when they are used to route electronic communications and audio-visual communication broadcast or distribution networks.

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 desiré ;

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 sécu-

Section 4. Within the meaning of this law and its implementing instruments, the following definitions shall be accepted:

(1) Illegal access: unauthorized intentional access to all or part of an electronic communication network, an information system or terminal equipment;

(2) Administration in charge of telecommunications: ministry or minister, as the case may be, invested with general powers over telecommunications and information and communication technologies by the Government;

(3) Algorithm: series of basic mathematical operations to be applied to data to achieve a desired result;

(4) Asymmetric algorithm: cipher algorithm using a public key to cipher and a private key (different) to decipher messages;

(5) Symmetric algorithm: cipher algorithm using the same key to cipher and decipher messages;

(6) Active attack: action modifying or altering the resources targeted by the attack (violation of the integrity and confidentiality of data);

(7) Passive attack: action that does not alter its target (eavesdropping, invasion of privacy);

(8) Integrity violation: action carried out intentionally to substantially disrupt or disable an information system, electronic communication network or terminal equipment by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or making data inaccessible;

(9) Security audit: systematic examination of components and security actors, policies,

rité, 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 ;

actions, procedures and resources used by an organization to protect its environment, conduct compliance tests, controls to assess the adequacy of (organizational, technical, human and financial) resources allocated for risks, optimization, efficiency and 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 ;

(10) Authentication: safety criteria defined using a specific process to verify the identity of a person or entity and ensure that the identification given corresponds to the identity of the person initially registered;

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

(11) Certification Authority: trusted authority responsible for the creation and assignment of public and private keys and electronic certificates;

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 ;

(12) Root Certification Authority: structure put in place in charge of the mission of accreditation of certification authorities, validating certification policy of certification authorities accredited, validating and signing certification authorities accredited certificates.

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 ;

(13) Digital certificate: electronic record secured by the electronic signature of the person who issued it after ensuring that it certifies the authenticity of its contents;

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

(14) Qualified electronic certificate: digital certificate issued by a licensed Certification Authority;

15) Certification électronique : émission de certificats électroniques ;

(15) Electronic certification: issuance of electronic certificates;

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 ;

(16) Cipher: the transformation of information using a secret key to make it illegible to anyone except those possessing special knowledge of the key;

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

(17) Key: in a cipher system, it corresponds to a mathematical value, a word, or a phrase which enables the ciphering or deciphering of a message with the help of the encryption

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,

algorithm;

(18) Private key: key used in asymmetric cipher mechanism (or public key cipher) which belongs to an entity and kept secret;

(19) Public key: used to cipher a message in an asymmetric system distributed freely;

(20) Secret key: key known to the sender and recipient used to cipher and decrypt messages using the symmetric cipher mechanism;

(21) Source code: all technical specifications, with no restrictions on access or implementation of a software or communication protocol, interconnection, interchange, or data format;

(22) Audiovisual communication: public communication by television and radio broadcasting services;

(23) Electronic communication: electromagnetic emission, transmission or reception of signs, signais, writings, images or sounds;

(24) Confidentiality: maintenance of the confidentiality of information and transactions to prevent unauthorized disclosure of information to non-recipients enabling the reading, listening, intentional or accidental, illegal copying during storage, processing or transfer;

(25) Content: all information relating to data belonging to individuals or legal entities, transmitted or received through electronic communication networks and information systems;

(26) Illegal content: content that infringes on human dignity, privacy, honour or national security;

(27) Electronic mail: message in the form of text, voice, sound or image transmitted

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 appliqué 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

through a public communication network, stored in a network server or the recipient's terminal equipment until he retrieves it;

(28) Encryption: use of codes or signals to convert information to be transmitted in the form of signals that are not understood by others;

(29) Cryptanalysis: all resources used to analyze initially encrypted information to be decrypted;

(30) Encrypted text: encrypted or encoded message;

(31) Cryptography: use of mathematical algorithm to encrypt information in an attempt to make it unintelligible to those who are not authorized to access it;

(32) Cybercriminality: infraction of the law carried out through cyberspace using means other than those habitually used to commit conventional crimes;

(33) Cybersecurity: technical, organizational, legal, financial, human, procedural measures for prevention and deterrence and other actions carried out to attain set security objectives through electronic communication networks and information systems, and to protect privacy;

(34) Certification practice statement: practices (organization, operational procedures, technical and human resources) that the competent Certification Authority applies within the framework of the provision of this service in accordance with the certification of a policy or policies it undertook to comply with;

(35) Decryption: reverse of encryption;

(36) Denial of service: attack by saturation of a resource of the information system or elec-

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 traffic : 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 ;

tronic communication network to make it collapse and unable to provide expected services;

(37) Distributed Denial of Service: simultaneous attack of the resources of an information system or electronic communication network in order to saturate and amplify the effects of interference;

(38) Availability: security criterion of resources of electronic communication networks, information systems and terminal equipment being accessible and usable as required (time factor);

(39) Device for electronic signature creation: equipment and / or private encryption software certified by a competent authority, configured to create an electronic signature;

(40) Device for electronic signature verification: equipment and / or public encryption software certified by a competent authority used by a certifying authority to verify electronic signatures;

(41) Data: representation of facts, information or concepts in a form suitable for processing by terminal equipment, including a program allowing it to perform a function;

(42) Connection data: data relating to the access process in an electronic communication;

(43) Traffic data: data relating to an electronic communication indicating the origin, destination, route, time, date, size and duration or type of underlying service;

(44) Terminal equipment: equipment, installation or facilities to be connected to the end point of an information system which broadcasts, receives, processes and stores information data;

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 ;

(45) Reliability: ability of an information system or electronic communication's network to operate without any incident for a very long time;

(46) Provider of electronic communication services : natural person or corporate body providing services consisting entirely or . mainly in the provision of electronic communications;

(47) Impact severity: assessment of the gravit y of an incident, weighted by its frequency of occurrence;

(48) Data integrity: safety criterion defining the status of an electronic communication's network, an information system or terminal equipment that remains intact and helps ensure that resources have not been altered (modified or destroyed) intentionally and accidentally to ensure their accuracy, reliability and durability;

(49) Unlawful interception: illegal or unauthorized access to the data of an electronic communication's network, an information system or a terminal equipment;

(50) Lawful interception: authorized access to the data of an electronic communication's network, an information system or terminal equipment without right or authorization;

(51) Intentional intrusion: intentional and unauthorized access to an electronic communication's network or an information system with the intent of causing harm or deriving economic, financial, industrial, or security benefit or sovereignty;

(52) Intrusion by intellectual challenge: intentional access without right to an electronic communication's network or an information system with the intent of taking up an intellectual challenge that can help improve the performance of the organization's security system;

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

(53) Deceptive software: software that performs operations on a user's terminal equipment without initially informing him of the exact nature of the operations to be performed on his terminal equipment by the software or without asking his approval for the software to perform the operations;

(54) Spyware: specific deceptive software that collects personal information (most visited websites, passwords, etc.) from a user's electronic communication's network;

(55) Potentially unwanted software: software having the features of a deceptive software or spyware;

(56) Plain text: version of a message that is intelligible to and understandable by all;

(57) Cryptographic means: equipment or software designed or modified used in transforming data, be it information or signals, using secret codes or to perform an inverse operation with or without a secret code to guarantee the safe storage or transmission of data and ensure the confidentiality and control of their integrity;

(58) Non-repudiation: security criterion that ensures the availability of evidence that can be used to prove the traceability of an electronic communication that has taken place;

(59) Certificate policy: set of rules that define standards to be respected by Certification Authorities when providing their services, indicating the applicability of a certificate to a particular community and/or class of application with common security requirements;

(60) Security policy: security benchmark established by an organization which reflects its security strategy and specifies the means to achieve it;

(61) Provision of cryptographic service: ope-

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 obte-

ration aimed at implementing cryptographie solutions on behalf of others;

(62) Electronic communication's network: active or inactive transmission systems and, where applicable, switching and routing equipment and other resources that enable signal routing by wire, radio, optical means or other electromagnetic means, including satellite, terrestrial networks, fixed (circuits or packets switching, including the Internet) and mobile networks, systems using electrical network, provided they are used to transmit signals, networks used for radio and television and cable television networks, irrespective of the type of information transmitted;

(63) Telecommunication network: installation or group of installations used in the transmission and routing of telecommunications signais, or exchange of command and management information associated with these signals between network points;

(64) Security: situation in which someone or something is not exposed to any danger. Mechanism to prevent any havoc or their attendant effects;

(65) Certification service: service provided by a Certification Authority;

(66) Electronic communication's service: service consisting wholly or mainly in the provision of electronic communications, except the content of audiovisual communication services;

(67) Representative: individual acting on his own behalf or on behalf of the person or entity he represents, which involves a device for creating an electronic signature;

(68) Electronic signature: signature obtained

nue 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 detection : 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.

by an asymmetric encryption algorithm to authenticate the sender of a message and verify its integrity;

(69) Advanced electronic signature: electronic signature obtained using a qualified electronic certificate;

(70) Open standard: communication, interconnection or exchange and interoperable data format protocol whose technical specifications and access are public and have no restriction or implementation;

(71) Detection system: system that helps detect incidents that could lead to security policy violation and help diagnose potential intrusions;

(72) Information system: devices or group of interconnected or related devices performing, by itself or by one or many of its components, automatic data processing, in line with a program;

(73) Vulnerability: security breach resulting either intentionally or accidentally by a violation of security policy in the architecture of an electronic communication's network, in designing an information system.

Section 5. The terms and expressions not defined under this law shall maintain their definitions or meanings as provided for in international legal instruments to which Cameroon adheres, notably the Constitution and the Convention of the International Telecommunications Union, the Radiocommunications Regulation and the International Telecommunications Regulation.

Titre II

De la cybersécurité

Chapitre I

De la politique générale de sécurité électronique

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 régulation et du suivi des activités de sécurité électronique

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,

Part II

Cybersecurity

Chapter I

Electronic Security and general policy

Section 6. The Administration in charge of Telecommunications shall formulate and implement the electronic communication's security policy by taking into account technological developments and Government priorities in this domain.

Accordingly, it shall:

- promote the security of electronic communication networks and information systems and monitor the evolution of issues related to security and certification activities;

- coordinate activities that contribute to the security and protection of electronic communication networks and information systems at national level;

- ensure the setting up of an electronic communication's security framework;

- draw up the list of Certification Authorities;

- represent Cameroon in international bodies in charge of activities related to the security and protection of electronic communication networks and information systems.

Chapter II

Regulation andd Monitoring of Electronic Security Activities

Section 7. (1) The National Agency for Information and Communication Technologies, hereinafter referred to as the Agency, instituted by the Law governing electronic communications in Cameroon, shall be responsible for the regulation of electronic security activities in collaboration with the Telecommunications Regulatory Board.

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

(2) The Agency referred to in subsection 1 above shall be responsible for the regulation, control and monitoring of activities related to the security of electronic communication networks, information systems, and electronic certification on behalf of the State. Accordingly, its missions shall be to:

- examine applications for accreditation and prepare the specifications of Certification Authorities and submit them to the Minister in charge of telecommunications for signature;

- control the compliance of electronic signatures issued;

- participate in the development of the national policy on the security of electronic communication networks and certification;

- give an advisory opinion on instruments that fall under its area of competence;

- control activities aimed at ensuring the security of electronic communication networks, certification and information systems;

- examine applications for the certification of cryptographic means and issue certificates of homologation for security equipment;

- prepare agreements of mutual recognition with foreign parties and submit them to the Minister in charge of Telecommunication for signature;

- monitor technological developments and issue warnings and recommendations regarding the security of electronic communication networks and certification;

- participate in research, training and studies related to the security of electronic communication networks, certification and information systems;

- ensure the regularity and efficiency of security audits of information systems in accordance with established standards, public

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 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 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,

bodies and Certification Authorities

- monitor, detect and provide information on computer-related risks and cybercriminals activities ;

- carry out any other mission of general interest assigned to it by the supervisory authority.

(3) A decree of the Prime Minister shall determine the modalities of implementation of subsection 1 above.

Section 8. (1) The Agency shall be the Root Certification Authority.

(2) The Agency shall be the Certification Authority of the Public Administration.

Section 9. (1) The Certification Authorities, security auditors, editors of security programs and other authorized security services are subject to the payment of a 1.5 % annual contribution of their untaxed turnover value intended to a fund named "Special Fund for Security Activities," intended to finance research, development, training and studies in respect of cybersecurity.

(2) The resources referred to in Subsection 1 above shall be collected by the Agency and deposited in an account opened at the Central Bank.

(3) A Committee is hereby created to be in charge of the validation of priority projects for research, development, training and studies in the domain of cybersecurity.

The conditions and terms for the functioning of the Committee shall be defined by regulation.

(4) The Minister in charge of Telecommunications shall be the authorizing officer for expenses made under the fund referred to in subsection 1 above."

(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

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 activités de securité

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.

(5) The conditions and terms of collection and management of this contribution shall be defined by regulation.

Chapter III
Legal Regime of Certification Activities

Section 10. Electronic certification activities shall be subject to prior approval. It shall be carried out by Certification Authorities.

Section 11. The following activities may be subject to authorization:

- the setting up and exploitation of infrastructure to issue, preserve and deliver qualified electronic certificates ;

- the provision of public keys to all public users ;

- the provision of security auditing, security programs editing, and other authorized security services to the public.

Section 12. The conditions and terms for granting the authorization referred to in Section 10 above shall be laid down by regulation.

Chapter IV
Security Activities

Section 13. (1) Electronic communication networks and information systems of operators, certification authorities and electronic communication service providers shall be subject to an obligatory security audit.

(2) The conditions and terms for the conduct of the security audits provided for in Sub-Section 1 above shall be laid down by regulation.

Section 14. The staff of the Agency and experts recruited to carry out audit operations shall be required to maintain professional secrecy.

Chapitre V
De la certification électronique

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

Chapter V
Electronic Certification

Section 15. (1) Qualified electronic certificates shall be valid only for the objects for which they were issued.

(2) Devices used to design and verify qualified certificates shall, from the technological stand point, be neutral, standardized, certified and interoperable.

Section 16. (1) Certification Authorities shall be responsible for prejudice caused to people who relied on the certificates they presented as qualified in the case where:

- the information contained in the certificate on the date of its issuance was inaccurate;

- the data prescribed such that certificate could be considered as qualified was incomplete;

- the issuance of the qualified certificate did not give rise to the verification that the signatory holds the private convention corresponding to the public convention of the certificate;

- Certification Authorities and certification service providers, as the case may be, have not registered the repeal of the qualified certificate and placed this information at the disposai of third parties.

(2) Certification Authorities shall not be responsible for the prejudice caused by the use of the qualified certificate that exceeds the limits fixed for its use or the value of transactions for which it can be used, provided that such limits appear in the qualified certificate and are accessible to users.

(3) Certification Authorities must justify adequate financial guarantee, allocated particularly for the payment of sums they may owe people who relied logically on the qualified certificates they issue, or an insurance

qualifiés qu'elles délivrent, ou d'une assurance garantissant les conséquences pécuniaires de leur responsabilité civile professionnelle.

Chapitre VI
De la signature électronique

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 électroniques délivrés par les autorités 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.

that guarantees the pecuniary consequences of their civil professional responsibility.

Chapter VI
Electronic Signature

Section 17. The advanced electronic signature shall have the same legal value as that handwritten signature and produce the sa me effects as the latter.

Section 18. An advanced electronic signature must meet the following conditions:

- the data related to signature creation shall be exclusively linked to the signatory and be under his exclusive control;

- each modification shall be easily detectable;

- it shall be created using a protected device whose technical characteristics shall be defined by an instrument of the Minister in charge of telecommunications;

- the certificate used to generate signatures shall be a qualified certificate. An instrument of the Ministry in charge of telecommunications shall determine the criteria of the qualification of certificates.

Chapter VII
Electronic Certificates and Signatures Issued by Certification Authorities

Section 19. The certification authority that validated an electronic certificate may not retract.

Section 20. (1) An electronic certificate issued outside the national territory shall produce the same legal effects as a qualified certificate issued in Cameroon provide that there is a decision recognizing the issuing authority by the Minister in charge of telecommunications.

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

Chapitre VIII
Du document électronique

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 réseaux de communications électroniques, des systèmes d'information et de la vie privee des personnes

Section 1
De la protection des réseaux de communication électroniques

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

(2) The interoperability of qualified electronic certificates shall be regulated by an instrument of the Minister in charge of telecommunications.

Chapter III
Electronic Document

Section 21. Any person wishing to affix his electronic signature to a document can create the signature using a reliable device whose technical characteristics shall be determined by instrument of the Minister in charge of Telecommunications.

Section 22. Any person using an electronic signature device must:

- take minimum precautions fixed by the instrument referred to in Section 21 above to avoid any illegal use of the encoding elements or personal equipment related to its signature;

- inform the Certification Authority about any illegitimate use of his signature;

- ensure the authenticity of all the data he declared to the electronic certification service provider and to any person he requested to trust his signature.

Section 23. In the event of failure to honor the commitments under Section 22 above, the holder of the signature shall be responsible for the injury caused to others.

Chapter IX
Protection of Electronic Communication Networks, Information Systems and Personal Privacy

I- Protection of Electronic Communication Networks

Section 24. Electronic communication networks operators and electronic communication service providers must take all the necessary technical and administrative measures to guarantee the security of the servi-

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 risqué ;

- 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 systèmes 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.

ces provided. To that end, they shall be bound to inform users about:

- the risks of using their networks;

- the specific risks of security violation, notably the denial of services distributed, abnormal rerouting, traffic points, traffic and unusual ports, passive and active listening, intrusion and any other risk;

- the existence of techniques to ensure the security of their communications.

Section 25. (1) Network operators and electronic communication service providers shall be bound to conserve traffic connection data for a period of 10 (ten) years.

(2) Network operators and electronic communication service providers shall set up mechanisms for monitoring the traffic data of their networks. Such data may be accessible in the course of judicial inquiries.

(3) Network operators and electronic communication service providers shall be liable where the use of the data referred to in Subsection 2 above undermines the individual liberties of users.

II- Protection of Information Systems

Section 26. (1) Operators of information systems shall take every technical and administrative measure to ensure the security of services offered. To this end, they shall have standardized systems enabling them to at all times identify, assess, process or manage any risk relating to the security of the information systems of the services provided directly or indirectly.

(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

(2) Operators of information systems shall set up technical mechanisms to avoid any hitches that may be prejudicial to the steady functioning of systems, their integrity, authentication, non repudiation by third party users, confidentiality of data and physical security.

3) The mechanisms provided for in Subsection 2 above shall be subject to the approval and visa of the Agency.

(4) Information systems platforms shall be protected against any radiation or intrusion that may impair the integrity of data transmitted and any other external attack notably, through intrusions' detection system.

Section 27. Corporate bodies whose activity is to provide access to information systems shall be bound to inform users of:

- the dangers associated with the use of unprotected information systems notably for private individuals;

- the need to install parental control devices;

- specific security violation risks notably, the generic family of viruses;

- the existence of permanent technical means to restrict access to certain services and propose to them at least one of such means notably, the use of the most recent operating systems, the use of anti-viruses against spywares, misleading viruses, the activation of personal firewalls, intrusion detection systems and activation of automatic updating.

Section 28. (1) Operators of information systems shall inform users of the prohibition to use electronic communication networks for the publishing of illicit content or any other act that is likely to affect the security of net-

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.

works or information systems.

(2) Such prohibition shall equally concern the designing . of misleading viruses, spywares, potentially undesirable software or any other device leading to fraudulent practices.

Section 29. (1) Operators of information systems shall be bound to conserve the connection and traffic data of their information systems for a period of 10 (ten) years.

(2) Operators of information systems shall be bound to set up mechanisms for monitoring and controlling access to the data of their information systems. Such data may be accessible in the course of judicial inquiries.

(3) The installations of operators of information systems may be subject to search or seizure, on the order of a judicial authority, under conditions provided for by the laws and regulations in force.

Section 30. (1) Operators of information systems shall assess and revise their security systems and, where necessary, make the appropriate modifications to their security practices, measures and techniques according to technological change.

(2) Operators of information systems and users may cooperate mutually with a view to implementing the security practices, measures and techniques of their systems.

Section 31. (1) Electronic communication networks and information systems content providers shall be bound to ensure the availability of material, as well as the data stored in their installations.

(2) They shall be bound to set up filters in order to avoid any attacks that may be prejudicial to personal data and the privacy of users.

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.

Section 32. (1) Electronic communication networks and information systems shall be subject to a regime of compulsory and periodic auditing of their security systems by the Agency.

(2) Security audit and severity scale rating shall be undertaken each year or as required by the prevailing circumstances.

(3) Audit reports shall be confidential and addressed to the Minister in charge of Telecommunications.

(4) An instrument of the Minister in charge of Telecommunications shall fix conditions for rating the severity scale.

III - Obligations of Access, Service and Content providers

Section 33. Persons whose activity consists in providing access to electronic communication services shall inform their subscribers of the existence of technical means of restricting access to certain services of choosing them and propose to them at least one of such means.

Section 34. (1) The persons in charge, even gratuitously, of the storage of signais, written material, images, sound or messages of any nature supplied by the users of such services may be liable.

(2) However, the liability under sub-section 1 above shall not apply where:

- the said persons were not effectively aware of the illicit nature of the facts or circumstances characterizing them as such;

- once they became aware of the facts, acted promptly to withdraw such data or render them inaccessible.

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 ;

Section 35. (1) The persons referred to in Sections 33 and 34 above shall be bound to preserve, for a period of 10 (ten) years, data enabling the identification of any person who contributed to the creation of the content of the services they provided.

(2) They shall provide the persons who edit electronic communication services with the technical means enabling them to fulfill the identification conditions referred to in Sections 37 and 38 below.

(3) A judicial authority may request the providers referred to in Sections 33 and 34 above to communicate communication data referred to in Subsection 1 above.

Section 36. The competent court referred to shall rule, within a maximum time-limit of 30 (thirty) days, on all measures to prevent or stop any damage caused by the content of an electronic communication service.

Section 37. Persons engaged in editing electronic communication services shall inform the public of:

- their full name, domicile and telephone numbers and, where they are subject to trade registration, personal property loan formalities and their registration number, in case of corporate bodies;

- their company or corporate name and head offices, telephone numbers and, where they are corporate bodies subject to trade registration, personal property loan formalities, their registration number, share capital, head office addresses, in case of corporate bodies;

- the name of the publisher or co-publisher and, where necessary, that of the editor in chief;

- 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.

- the name, company or corporate name, address and telephone number of the provider referred to in Sections 33 and 34 above.

Section 38. (1) Persons editing an electronic communication's service may place at the disposai of the public only the name, company or corporate name and the address of the provider.

(2) The persons referred to in Sections 33 and 34 above shall be bound to confidentiality.

Section 39. (1) Any person who is victim of defamation by means of an electronic communication's service shall have the right to reply and may request for correction.

(2) Conditions for the insertion of a rejoinder of reply shall be those provided for by the instruments in force.

Section 40. (1) Any person engaged in transmitting electronic communication networks content or providing access to an electronic communication's network may be not liable where they:

- requested the contentious transmission;

- select or modify the content transmitted.

(2) Any person whose activity, for the sole purpose of rendering its subsequent transmission more efficient, is the automatic, intermediary and temporary storage of content transmitted by a provider, may be criminally or civilly liable in respect of such content only in the case where they modify such content, do not comply with the required conditions of access and ordinary updating rules or where they impede the licit and normal use of the technology used to obtain data.

Section IV
De la protection de la vie privée 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 pen-

IV - Protection of Privacy

Section 41. Every individual shall have the right to the protection of their privacy. Judges may take any protective measures notably, sequestration or seizure to avoid or end the invasion of privacy.

Section 42. The confidentiality of information channelled through electronic communication and information systems networks, including traffic data, shall be ensured by operators of electronic communication and networks information systems.

Section 43. Content providers shall be responsible for data transmitted through their information system notably, if such content may entail infringement of human dignity, injury to character and invasion of privacy.

Section 44. (1) It shall be forbidden for any natural person or corporate body to listen, intercept and store communications and the traffic data related thereto, or to subject them to any other means of interception or monitoring without the consent of the users concerned, save where such person is so authorized legally.

(2) However, technical storage prior to transmission of any communication shall be authorized for electronic communications' networks and information systems operators, without prejudice to the principle of confidentiality.

Section 45. The recording of communications and traffic data related thereto in a professional setting with a view to providing digital evidence of an electronic communication shall be authorized.

Section 46. (1) Electronic communication networks and information systems content providers shall be bound to conserve such content and stored data in their installations for a period of the 10 (ten) years.

dant 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 électroniques

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 électroni-

(2) Electronic communication networks and information systems content providers shall be bound to set up filters in order to contain any attacks that may be prejudicial to the personal data in privacy of users.

Section 47. The use of electronic communication networks and information systems for the purpose of storing information or accessing information stored in the terminal equipment of a natural person or corporate body shall be made only with their prior consent.

Section 48. (1) The sending of electronic messages for prospecting purposes by dissimulating the sender identity or without indicating the valid address to which the addressee may send a request aimed at blocking such information shall be prohibited.

(2) The sending of electronic mails by usurping the identity of another user shall be prohibited.

V - Interception of Electronic Communication

Section 49. Notwithstanding the provisions of the Criminal Procedure Code, in case of crimes or offences provided for hereunder, cri minal investigation officers may intercept record or transcribe any electronic communication.

Section 50. In the event of encoding, compressing or ciphering of data transmitted by electronic communication networks or electronic communication service providers, clear corresponding interceptions shall be provided to the services that requested them.

Section 51. The personnel of electronic communication network operators or electronic

ques ou des fournisseurs de services de communications électroniques sont astreints au secret professionnel quant aux réquisitions reçues.

Titre III
De la cybercriminalité

Chapitre 1
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

communication service providers shall be bound to secrecy for any requests they receive.

Part III
Cybercriminallity

Chapter I
Procedural Law Provisions

Section 52. (1) In case of any cyberoffence, Criminal Investigation Officers with general jurisdiction and authorized officials of the Agency shall carry out investigations, in accordance with the provisions of the Criminal Procedure Code.

(2) Prior to assuming duty, authorized officiais of the Agency shall take an oath before the competent Court of First Instance as follows: I swear to perform my duties loyally and to always abide by the responsibilities bestowed on me, to keep secret information I am aware of on the occasion of or in the discharge of my duties

(3) Criminal Investigation Officers and authorized officials of the Agency may, in the course of investigations, have access to means of transport, any professional premises, with the exception of private residences, with a view to seeking and recording offences, requesting the production of all professional documents and taking copies thereof and gathering any information and evidence, upon a summons or in situ.

Section 53. (1) Cybercriminal-related searches may concern data. Such data may be physical material or copies made in the presence of persons taking part in the search.

(2) When a copy of seized data is made, it may, for security reasons be destroyed on the instruction of the State Counsel.

(3) On the approval of State Counsel, only

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

objects, documents and data used as evidence may be kept under seal.

(4) Persons present during searches may be requested to provide information on any seized objects, document and data.

Section 54. Searches and seizures shall be carried out in accordance with the provisions of the Cri minai Procedure Code, taking into account the loss of validity of evidence.

Section 55. (1) When it appears that data seized or obtained in the course of an investigation or inquiry has been the subject of transformation, thus hindering clear access or is likely to impair the information it contains, the State Counsel, the Examining Judge or the Court may request any qualified natural person or corporate body to perform technical operations to obtain the clear version of the said data.

(2) When a cryptographic means has been employed, judicial authorities may request the secret conversion of the encrypted text.

Section 56. The request provided for in Section 50 above may be made to any expert. In such case, it shall conform with the provisions of the Criminal Procedure Code relating to the commissioning of an expert.

Section 57. (1) Cameroonian judicial authorities may set up a rogatory commission at, both the national and international level, any corporate body or natural person to search the elements of cybercrime offences of which at least one of the elements was committed on Cameroonian territory or of which one of the offenders or accomplices resides on the said territory.

(2) Subject to rules of reciprocity between

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.

Cameroon and foreign countries with which it has concluded a judicial cooperation agreement, rogatory commissions shall be executed in accordance with the provisions of the Criminal Procedure Code.

Section 58. (1) Natural persons or corporate bodies that provide cryptographic services aimed at performing a duty of confidentiality shall be bound to hand over to criminal investigation officers or authorized officials of the Agency, at their request, the agreements allowing the conversion of data transformed by means of the services that they deliver.

(2) Criminal investigation officers and authorized officials of the Agency may request the service providers referred to in Sub-section 1 above to implement these agreements of their own motion, except where they are unable to satisfy such requests.

Section 59. (1) For purposes of investigation or examination, the hearing or interrogation of a person and/or confrontation of several persons may be carried out on several locations on the national territory linked by electronic communication means that ensure the confidentiality of transmissions. A report shall be drawn up on the operations carried out in each location. Such operations may be subject to audiovisual and/or sound recording.

(2) According to the prevailing circumstances, their interpretation may be done by means of electronic communication in the course of a hearing, interrogation or confrontation.

(3) The provisions of this Section shall equally be applicable for the concurrent implementation, on a location on the national territory or on a location situated outside the national territory, of mutual assistance requests from foreign judicial officers or acts of mutual assistance performed outside the national territory, at the request of Cameroonian judicial authorities.

(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 (3) mois à trois (3) 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 (3) mois à quatre (4) ans, le refus de déférer aux convocations des agents habilités de l'Agence.

(3) Est puni d'un emprisonnement de un (1) à cinq (5) ans et d'une amende de 100.000

(4) Conditions for the implementation of this section shall be defined by regulation.

Chapter II
Offences and Penalities

Section 60. (1) When a Certification Authority is non-compliant, the Agency may, after serving a warning on the structure for comment, prohibit the circulation of the means of cryptography concerned.

(2) The prohibition of circulation shall be applicable throughout the national territory. It equally entails, for the provider, the obligation to withdraw:

- the means of cryptography whose circulation among commercial publishers was prohibited;

- materials that constitutes a means of cryptography and whose circulation was prohibited and that was acquired directly or through commercial publishers for a consideration.

(3) The means of cryptography concerned could be put back into circulation once the previously obligations are fulfilled and duly ascertained by the Agency.

Section 61. (1) Agency personnel and experts of corporate bodies in charge of security audits who without any authorization, disclose confidential information they are privy to on the occasion of a security audit shall be punished with imprisonment for from three 3 (three) months to (three) 3 years and a fine of from 20,000 (twenty thousand) to 100,000 (one hundred) CFA francs

(2) Refusal to comply with the summons of authorized officials shall be shall be punished with imprisonment for from (three) 3 months to (four) 4 years.

(3) Whoever, by any means whatsoever, obstructs, gives incitement to resist or prevent

(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 (1) à cinq (5) 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 (1) à cinq (5) 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.

the conduct of the investigation provided for in this section or refuses to provide information or documents related thereto shall be punished with imprisonment for from 1 (one) to 5 (five) years or a fine of from 100,000 (one hundred thousand) to 1,000,000 (one million) CFA francs or both of such fine and imprisonment.

Section 62. (1) Whoever presents the content or activity to the person referred to in Sections 33 and 34 above as illicit so as to cause the withdrawal or stop the publication thereof, knowing such information to be untrue, shall be punished with imprisonment for from 01 (one) to 05 (five) years and a fine of from 200,000 (two hundred thousand) to 2,000,000 (two million) CFA francs.

(2) The publisher, under pain of a fine of from 100,000 (one hundred thousand) to 2,000,000 (two million) CFA francs shall be bound to insert within 48 (forty-eight) hours of their reception, the response of any person designated in the electronic communication service.

Section 63. (1) The de jure or de facto manager of a corporate body exercising the activity defined in Sections 33 and 34 of this law who fails to conserve the information elements referred to in Sections 25 and 29 shall be punished with imprisonment for from 1 (one) to 5 (five) years and a fine of from 40,000 (forty thousand) to 4,000,000 (four million) CFA francs.

(2) The de jure or de facto manager of a corporate body exercising the activity defined in Sections 37 and 38 who fails to comply with the provisions of the said Sections shall be liable to the same sanctions.

Section 64. (1) Corporate bodies shall be criminally liable for offences committed on their account by their management structures.

(2) The criminal liability of corporate bodies shall not preclude that of natural persons who commit such offences or are accomplices.

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 (3) 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 (5) ans au moins, dans les conditions prévues par l'article 34 du Code Pénal, des établissements ou de 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 (5) ans au moins ;

- l'interdiction, à titre définitif ou pour une durée de cinq (5) ans au moins, de faire appel public à l'épargne ;

- l'interdiction, pour une durée de cinq (5) 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.

(3) The penalties to be meted out on defaulting corporate bodies shall be fines of from 5,000,000 (five million) to 50,000,000 (fifty million) CFA francs.

(4) The penalties provided for in Subsection 3 above, not withstanding one of the following other penalties may equally be meted out on corporate bodies:

- dissolution in case of a crime or felony punishable with respect to natural persons with imprisonment of 03 (three) years and above and where the corporate body has departed from its declared object to aid and abet the incriminating acts;

- definitive prohibition or temporary prohibition for a period not less than 5 (five) years, from directly or indirectly carrying out one or more professional or corporate activities;

- temporary closure for a period of not less than 5 (five) years under the conditions laid down in Section 34 of the Penal Code of the establishments or one or more establishments of the company that was used to commit the incriminating acts;

- barring from bidding for public contracts either definitively or for a period of not less than 5 (five) years;

- barring from offering for public issues either definitively or for a period of not less than 5 (five) years;

- prohibition for a period of not less than 5 (five) years from issuing cheques other than those to be used by the drawer to withdraw money from the drawer or certified checks or from using payment cards;

- seizure of the device used or intended to be used in committing the offence or the proceeds of the offence;

- publication or dissemination of the decision taken either through the print media or through any electronic means of communication to the public.

Article 65.- (1) Est puni d'un emprisonnement de cinq (5) 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 (2) à cinq (5) ans et d'une amende de 1.000.000 (un million) à 2.000.000 (deux millions) . 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.

Section 65. (1) Whoever, without any right or authorization, proceeds by electronic means to intercept or not during transmission, intended for, whether or not within an electronic communication network, an information system or a terminal device shall be punished with imprisonment for from 5 (five) to 10 (ten) years or a fine of from 5,000,000 (five million) to 10,000,000 (ten million) CFA francs or both such fine and imprisonment.

(2) Any unauthorized access to all or part of an electronic communication network or an information system or a terminal device shall be liable to the sa me sanctions in accordance with Subsection 1 above.

(3) The penalties provided for in Subsection 1 above, shall be doubled where unauthorized access violates the integrity, confidentiality, availability of the electronic communication network or the information system.

(4) Whoever, without any right, allows access to an electronic communication network or an information system as an intellectual challenge shall be punished in accordance with Subsection 1 above.

Section 66. (1) Whoever causes disturbance or disruption of the functioning of an electronic communication network or a terminal device by introducing, transmitting, destroying, erasing, deteriorating, altering, deleting data or rendering data in inaccessible shall be punished with imprisonment for from 2 (two) to 5 (five) years or a fine of from 1,000,000 (one million) to 2,000,000 (two million) CFA francs or both of such fine an imprisonment.

(2) Whoever uses the deceptive or undesirable software to carry out operations on a user's terminal device without first informing the later of the true character of the operation which the said software is likely to damage shall be punishable with the same penalties.

(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'unréseau 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 (5) 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 (5) 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.

(3) Whoever uses potentially undesirable software to collect, try to collect or facilitate any of such operations in order to access information of the operator or supplier of an electronic network or services and commit a crime shall be punishable in accordance with Subsection 1 above.

Section 67. Causing serious disturbance or disruption of the functioning of an electronic communication network or terminal equipment by introducing, transmitting changing, deleting or altering data shall constitute a breach of the integrity of an electronic communication network or an information system and shall be punishable in accordance with Section 66 above.

Section 68. (1) Whoever fraudulently gains access or remains in all or part of an electronic communication network or an information system by transmitting, destroying, causing serious disturbance or disruption to the functioning . of the said system or network shall be punished with imprisonment for from 5 (five) to 10 (ten) years or a fine of from 10,000,000 (ten million) to 50,000,000 (fifty million) CFA francs or both of such fine and imprisonment.

(2) The same penalties provided for in subsection 1 above shall be doubled where such acts result in the deletion or change to the data contained in the information system or a change in its functioning.

Section 69. Whoever accesses all or part of an electronic communication network, an information system or terminal equipment without authorization and in violation of security measures in order to obtain information or data relating to an information system connected to another information system shall be punished with imprisonment for from 5 (five) to 10 (ten) years or a fine of from 10,000,000 (ten million) to 100,000,000 (one hundred million) CFA francs or both of such and imprisonment.

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.

Section 70. Whoever causes through saturation, the attack of an electronic communication network device or an information system with the intention to cause its collapse thus preventing it from rendering the expected services, shall be punished with a fine of from 1,000,000 (one million) to 5,000,000 (five million) CFA francs.

Article 71.- Est puni d'un emprisonnement de deux (2) à cinq (5) 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.

Section 71. Whoever without permission, introduces data into an information system or an electronic communication network in order to delete or change the data contained therein, shall be punished with imprisonment for from 2 (two) to 5 (five) years and a fine of from 1,000,000 (one million) to 25,000,000 (twenty five million) CFA francs.

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.

Section 72. Whoever without authorization and for financial gain, uses any means to introduce, alter, erases or delete electronic data such as to cause damage to someone else's property shall be punished with the penalties provided for in Section 66 above.

Article 73.- (1) Est puni d'un emprisonnement deux (2) 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.

Section 73. (1) Whoever uses an information system or a counterfeit communication network to falsify payment, credit or cash withdrawal card or uses or attempts to use, in full knowledge of the facts, a counterfeit or falsified payment, credit or withdrawal card shall be punished with imprisonment for from 2 (two) to 10 (ten) years and a fine of from 25,000,000 (twenty five million) to 50,000,000 (fifty million) CFA francs or both of such fine and imprisonment.

(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.

(2) Whoever deliberately accepts to receive electronic communications payment using a forged or falsified payment, credit or cash withdrawal card shall be punished in accordance with Subsection 1 above.

Article 74.- (1) Est puni d'un emprisonnement de un (1) à deux (2) 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'in-

Section 74. (1) Whoever uses any device to receive the privacy of another person by attaching, recording or transmitting private or confidential electronic data without the consent of their authors shall be punished

timité 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 (1) à trois (3) 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 (6) mois à deux (2) 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 (6) mois à deux (2) 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

with imprisonment for from 1 (one) to 02 (two) years and a fine of from 1,000,000 (one million) to 5,000,000 (five million) CFA francs.

(2) Whoever, without authorization, intercepts personal data in the course of their transmission, from one information system to another, shall be punished in accordance with Subsection 1 above.

(3) Whoever, even through negligence processes or causes the processing of personal data in violation of the conditions precedent to their implementation shall be punished with imprisonment from 1 (one) to 3 (three) years and a fine of from 1,000,000 (one million) to 5,000,000 (five million) or both of such fine and imprisonment.

(4) Whoever uses illegal means to collect the personal data of another in order to invade his or her privacy and undermine his or her self esteem shall be punishable with imprisonment for from 6 (six) months to 2 (two) years or a fine of from 1,000,000 (one million) to 5,000,000 (five million) CFA francs or both of such fine and imprisonment.

(5) The penalties provided for in Subsection 4 above shall be doubled where anyone posts online, stores or has someone else store in a computerized memory, without the express consent of the person concerned, personal data which directly or indirectly discloses his/her tribal origin, political opinions, religious beliefs, trade union membership or values.

(6) The penalties provided for in Subsection 5 above shall apply to persons found guilty of diverting information, in particular, during the recording, filing or transmission thereof.

(7) Whoever keeps information in works or in figures beyond the legal time-limit specified in the application for a prior opinion or declaration for use of data processing shall be punished with imprisonment for from 6 (six) months to 2 (two) years or a fine of from

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 (2) à cinq (5) 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 (5) 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 (2) à cinq (5) 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 com-

5,000,000 (five million) to 50,000,000 (fifty million) CFA francs or both of such fine and imprisonment.

(8) Whoever discloses personal information that undermines the consideration due to the victim shall be punished with the penalties provided for in Subsection 7 above.

Section 75. (1) Whoever for financial gain, records or publishes images that undermine the bodily integrity of another person through electronic communications or an information system without the consent of the person concerned shall be punished with imprisonment for from 2 (two) years to 5 (five) years or a fine of from 1,000,000 (one million) to 5,000,000 (five million) CFA francs or both of such fine and imprisonment.

(2) This section shall not apply where such recording and publication fall under the normal exercise of profession aimed at informing the public or where they are carried out in order to be used as evidence in Court in accordance with the provisions of Cri minal Procedure Code.

Section 76. Whoever uses electronic communications or an information system to design, carry or publish a child pornography message or a message likely to seriously injure the self-respect of a child shall be punished with imprisonment for from 5 (five) years to 10 (ten) years or a fine of from 5,000,000 (five million) to 10,000,000 CFA francs or both of such fine and imprisonment.

Section 77. (1) Whoever uses electronic communication or an information system to act in contempt of race or religion shall be punished with imprisonment for from 2 (two) years to 05 (five) years or a fine of from 2,000,000 (two million) to 5,000,000 (five million) CFA francs or both of such fine and imprisonment.

(2) The penalties provided for in Subsection 1 above shall be doubled where the offence is

mise dans le but de susciter la haine ou le mépris entre les citoyens.

Article 78.- (1) Est puni d'un emprisonnement de six (6) mois à deux (2) 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 (5) 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 (3) à six (6) 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 cidessus, 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 (1) à cinq (5) 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 seule-

committed with the aim of stirring up hatred and contempt between citizens.

Section 78. (1) Whoever uses electronic communications or an information system to design, to publish or propagate a piece of information without being able to attest its veracity or prove that the said piece of information was true shall be punished with imprisonment for from 6 (six) months to 2 (two) years or a fine of from 5,000,000 (five million) to 10,000,000 (ten million) CFA francs or both of such fine and imprisonment.

(2) The penalties provided for in Subsection 1 above shall be doubled where the offence is committed with the aim of disturbing public peace.

Section 79. Penalties against private acts of indecency set forth in Section 295 of the Penal Code shall be punished with imprisonment for from 5 (five) years to 10 (ten) years or a fine of from 5,000,000 (five million) to 10,000,000 (ten million) CFA francs where the victim has been put in contact with the author of the said acts using electronic communication or an information system.

Section 80. (1) Whoever for consideration or free of charge, uses electronic communications or an information system to publish, attach, record or transmit an image showing acts of pedophilia or a minor shall be punished with imprisonment for from 1 (one) to 5 (five) years or a fine of from 5,000,000 (five million) to 10,000,000 (ten million) CFA francs or both of such fine and imprisonment.

(2) Whoever uses electronic means whatsoever to offer provide or publish, import or export an image or picture portraying pedophilia shall be punished with the penalties provided in Subsection 3 above.

(3) Whoever keeps an image or picture portraying pedophilia in an electronic communication network or an information system shall be punished with imprisonment for

ment, 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.

from 1 (one) to 5 (five) years or a fine of from 5,000,000 (five million) to 10,000,000 (ten million) CFA francs or both of such fine and imprisonment.

(4) The penalties provided for in Subsection 3 above shall be doubled where an electronic communication network is used to publish an image or picture of a minor.

(5) The provisions of this section shall equally apply to pornographic pictures showing minors.

Section 81. (1) The following offences shall be punishable with the penalties provided for in Section 82 below where they are committed using an electronic communication network or an information system:

- offering, producing, providing child pornography for publication;

- acquiring child pornography for oneself or for someone else using an information system;

- where adult persons make sexual proposals to minors below 15 years old or to a person having the features of a minor;

- dissemination or transmission of child pornography using an information system.

(2) Child pornography shall be any act which visually presents:

- a minor involved in sexually explicit behavior;

- any person with the physical features of a minor involved in sexually explicit acts;

- real images of a minor involved in sexually explicit acts.

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 (1) à deux (2) 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 (6) à deux (2) 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,

Section 82. The penalties provided for in Section 79 above shall be doubled for whoever uses electronic communication devices to commit or attempt to commit any act of indecency on a minor less than 15 (fifteen) years old.

Section 83. (1) Whoever uses electronic communication devices to make sexual proposal to a person of the same sex shall be punished with imprisonment for from 1 (one) to 2 (two) years or a fine of from 500,000 (five hundred thousand) to 1,000,000 (one million) CFA francs or both of such fine and imprisonment.

(2) The penalties provided for in subsection (1) above shall be doubled if sexual proposals are followed by sexual intercourse.

Section 84. (1) Whoever fraudulently becomes acquainted with, delays access to or deletes electronic messages addressed to another shall be punished with imprisonment for from 6 (six) months to 2 (two) years of a fine of from 500,000 (five hundred thousand) to 1,000,000 (one million) CFA francs or both of such fine and imprisonment.

(2) The same penalties provided for in subsection 1 above shall apply against whoever, without authorization, intercepts, diverts, uses or divulges electronic messages sent or received by electronic means or proceeds to install equipment designed for such interceptions.

Section 85. The penalties provided for in section 84 above shall apply against whoever, being responsible for a public service mission and acting in the discharge or during the discharge of his/her duties, diverts or facilitates the diversion, deletion or access to electronic messages or reveals the content thereof.

Section 86. (1) The penalties provided for in section 71 above shall apply against whoever imports, keep, offers, transfers, sells or provides, in any form whatsoever, a computer program, a password, an access code or any

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 (5) ans au moins, d'exercer une fonction publique ou une activité socio-professionnelle, 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 (5) 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 (5) ans au moins, des marchés publics.

Article 88.- 1) Est puni d'un emprisonnement de (1) à cinq (5) 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 com-

similar computer data designed and/or specially adapted to facilitate access to all or part of an electronic communication or an information system.

(2) Whoever causes serious disturbance or disruption on an electronic communication, or whoever uses electronic communication network or an information system with the intention of breaching the integrity of the data, shall be punishable with the penalties provided for in Subsection 1 above.

Section 87. Authors of the offences provided for in Section 86 above , shall be punishable with the following additional penalties:

- seizure, in accordance with the conditions laid down in Section 35 of the Penal Code, of any object used or intended to be used to commit the offence or considered to be the proceed thereof, with the exception of objects likely to be restituted;

- prohibition, in accordance with the conditions laid down in section 36 of the Penal Code, for a period of not less than 5 (five) years from the holding a public office or carrying out a socio-professional activity where the offence was committed in the discharge or during the discharge of one's duties;

- closure, in accordance with the conditions laid down in Section 34 of the Penal Code, for a period of not less than 5 (five) years, of establishments or of one or more of the establishments of the company that was used to commit the offence;

- barring, for a period of not less than 5 (five) years, from public contracts.

Section 88. (1) Whoever, knowing about the secret decoding convention, a cryptographic means likely to have been used to prepare, facilitate or commit a crime or felony, refuses to hand over the said convention to judicial authorities or to use it upon request by such authorities shall be punished with imprisonment for from 1 (one) to 5 (five) years or a

mettre 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 (3) à cinq (5) 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 coopération et de l'entraide judiciaire internationales

Chapitre 1
De la coopération 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

fine of from 1,000,000 (one million) to 5,000,000 (five million) CFA francs or both of such fine and imprisonment.

(2) Where such refusal occurs whereas the handing over or use of the convention could have helped prevent the commission of the crime or felony or limit the effects thereof, the penalties provided for in Subsection 1 above shall be increased to imprisonment for from 3 (three) to 5 (five) years and a fine of from 1,000,000 (one million) to 5,000,000 (five million) CFA francs.

Section 89. There shall be no suspended sentence for the offences provided for in this law.

Part IV
International Cooperation and Mutual Judicial Assistance

Chapter1
International Cooperation

Section 90. (1) In the discharge of their duties, Cameroonian Certification Authorities may, under the control of the Agency, conclude conventions with foreign Certification Authorities.

(2) The conditions for concluding the conventions referred to in Subsection 1 above shall be laid down by regulation.

Chapter II
International and mutual Judicial Assistance

Section 91. (1) Unless otherwise provided for by an international convention to which Cameroon is signatory, requests for judicial assistance from Cameroonian judicial officers to foreign judicial officers shall be sent through the Ministry in charge of External Relations. Enforcement documents shall be sent to the authorities of the requesting State through the same channel.

(2) Requests for mutual judicial assistance from foreign authorities to Cameroonian

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.

judicial authorities must be presented through diplomatie channels by the foreign Government concerned. Enforcement documents shall be sent to the authorities of the requesting State through the same channel.

(3) In case of emergency, requests for judicial assistance from Cameroonian or foreign authorities may be sent directly to the authorities of the requested State for enforcement. The enforcement documents shall be dispatched to the relevant State authorities under the same conditions.

(4) Subject to international conventions, request for mutual judicial assistance from foreign authorities to Cameroonian judicial authorities shall be subject to an opinion of foreign Government concerned. Such opinion shall be forwarded to the relevant judicial authorities through diplomatic channels.

(5) In case of emergency, requests for mutual judicial assistance from foreign judicial authorities shall be forwarded to the State Counsel or Examining Magistrate with territorial jurisdiction.

(6) Where the State Council receives a request for mutual judicial assistance directly from authority, but which can only be enforced by the Examining Magistrate, he shall forward it to the latter for enforcement or refer to the General Prosecutor in the case provided for in Section 94 below.

(7) Before proceeding to enforce a request for mutual assistance forwarded directly to him, the Examining Magistrate shall immediately communicate same to the State Counsel for an opinion.

Section 92. (1) Requests for mutual judicial assistance from foreign judicial officers shall be enforced by the State Counsel or judicial Police Officers or Agents requested for this purpose by the said State Counsel.

(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 éxécutée 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) The requests shall be enforced by the Examining Magistrate or Judicial Police Officers acting on the rogatory commission of the Examining Magistrate where they require certain procedural measures which can be ordered or enforced only during a preliminary investigation.

Section 93. (1) Request for mutual judicial assistance from foreign judicial officers shall be enforced in accordance with the procedure laid down by the Criminal Procedure Code.

(2) However, where the request for assistance so specifies, it shall be enforced in accordance with the procedure explicitly indicated by the relevant authorities of the requesting State, without such ru les violating the rights of the parties or the procedural guarantees provided for by the Cri minai Procedure Code.

(3) Where the request for mutual assistance cannot be enforced in accordance with the requirements of the requesting Sate, the relevant Cameroonian authorities shall immediately inform the authorities of the requesting State of such impossibility and specify under what conditions the request may be enforced.

(4) The relevant Cameroonian authorities and those of the requesting State may subsequently agree on the onward processing of the request, where necessary, by subjecting it to compliance with such conditions.

(5) Irregularity in the transmission of the request for judicial assistance shall not constitute grounds for nullity of actions undertaken in enforcing such a request.

Section 94. (1) Where the enforcement of a request for judicial assistance from a foreign judicial authority is such as can breach public law and order or negatively affect the essential interests of the Nation, the State Counsel to whom the request is addressed or who is apprised thereof shall forward same to the General Prosecutor who shall transmit to the Minister in charge of Justice and where necessary, inform the State Counsel of such transmission.

(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 piéces 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.

Yaoundé, le 21 décembre 2010.
Le président de la République,
Paul Biya.

---

(2) Where the request is forwarded to the Minister in charge of Justice, he shall inform the requesting authority, where necessary, that it is not possible to totally or partially accede to the request. Such information shall be communicated to the judicial authority concerned and shall block the enforcement of the request for mutual judicial assistance or the return of the enforcement papers.

Part V
Transitional and Final provisions

Section 95. The conditions of applications of this law shall, as and when necessary, be laid down by implementation instruments.

Section 96. Authorizations and declarations for the supply, import and export of cryptographic devices issued by the relevant authorities shall remain valid until the expiry of the time-limit specified therein.

Section 97. This law shall be registered, published according to the procedure of urgency and inserted in the *Official Gazette* in English and French.

Yaoundé, 21 December 2010.
Paul Biya,
President of the Republic.
