Présidence de la République

République Centrafricaine

Unité - Dignité - Travail

LOI N°24.002

RELATIVE A LA CYBERSECURITE ET A LA LUTTE CONTRE LA CYBERCRIMINALITE

==========

L'ASSEMBLEE NATIONALE A DELIBERE ET ADOPTE,

LE PRESIDENT DE LA REPUBLIQUE, CHEF DE L'ETAT

PROMULGUE LA LOI DONT LA TENEUR SUIT :

TITRE I : DES DISPOSITIONS GENERALES

CHAPITRE I : DE L'OBJET ET DU CHAMP D'APPLICATION

Article 1 : La présente loi a pour objet de fixer les règles applicables en matière de cybersécurité et de lutte contre la cybercriminalité.

A ce titre, elle vise à :

- créer un environnement propice et sécurisé des systèmes d'information et réseaux de communications électroniques ainsi que dans le cyberespace ;
- définir les règles et les dispositions de sécurité applicables aux systèmes d'information et réseaux de communications électroniques ;
- 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 ;
- incriminer et réprimer les infractions informatiques ainsi que toutes les infractions commises au moyen des nouvelles technologies de l'information ;
- fixer le régime juridique de la preuve numérique, des activités de sécurité et de cryptographie.

Art. 2 : Les dispositions de la présente loi s'appliquent à toute personne physique et morale, quelle que soit sa nationalité, ayant commis une infraction par le biais des Technologies de l'Information et de la Communication en République Centrafricaine ou à l'étranger et dont les effets se produisent sur le territoire national.

Art. 3 : Sont exclues du champ de la présente loi, les applications spécifiques utilisées en matière de Défense et de Sécurité Nationale, lorsque les conditions de l'art. 114 de la présente loi sont réalisées.

Art. 4 : Les réseaux de communications électroniques visés par la présente loi comprennent : les réseaux satellitaires, les réseaux terrestres, les réseaux électriques lorsqu'ils servent à l'acheminement de communications électroniques, les réseaux assurant la diffusion ou la distribution de services de communication audiovisuelle.

CHAPITRE II : DES DEFINITIONS

Art. 5 : Au sens de la présente loi, on entend par :

- **Accès dérobé** : Mécanisme permettant de dissimuler l'accès à des données ou à un système d'information sans l'autorisation de l'utilisateur légitime ;
- **Antivirus** : Logiciel conçu pour identifier, neutraliser et éliminer des logiciels malveillants ;
- **CERT** : Computer Emergency Response Team ;
- **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 ;
- **Chiffrement** : Toute technique qui consiste à transformer des données numériques en un format inintelligible en employant des moyens de cryptologie ;
- **Clé privée** : Clé utilisée dans le mécanisme de chiffrement asymétrique (ou chiffrement à clé publique), qui appartient à une entité et qui doit être sécrète ;
- **Clé publique** : Clé servant au chiffrement d'un message dans un système asymétrique et donc librement diffusée ;
- **Clé** : Dans un système de chiffrement, elle correspond à une valeur mathématique, un mot, une phrase qui permet, grâce à l'algorithme de chiffrement, de chiffrer ou de déchiffrer un message ;
- **Code source** : Ensemble des spécifications techniques, sans restriction d'accès ni de mise en œuvre, d'un logiciel ou protocole de communication, d'interconnexion, d'échange ou d'un format de données ;
- **Communication au public par voie électronique** : Toute mise à la disposition du public ou d'une catégorie de public, par un procédé de communications électroniques ou magnétiques, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature ;
- **Communication audiovisuelle** : Transmission d'information sous forme de composante sonore et visuelle ;
- **Communication électronique** : Emission, transmission ou réception de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique;
- **Cryptage** : Utilisation de codes ou signaux non usuels permettant la conservation des informations à transmettre en des signaux incompréhensibles par les tiers ;

- **Cryptanalyse** : Ensemble des moyens qui permettent d'analyser une information préalablement chiffrée en vue de la déchiffrer ;
- **Cryptogramme** : Message chiffré ou codé ;
- **Cryptographie** : Application des mathématiques permettant d'écrire l'information, de manière à la rendre inintelligible à ceux ne possédant pas les capacités de la déchiffrer ;
- **Cryptologie** : Science relative à la protection et à la sécurité des informations notamment pour la confidentialité, l'authentification, l'intégrité et la non répudiation ;
- **CSIRT**: Computer Security Incident Response Team ;
- **Cybercriminalité** : Infraction pénale commise dans le cadre ou au moyen d'un système d'information, d'un réseau de télécommunication ou d'un système informatique, susceptible de se produire également dans le cyberespace ;
- **Cyberespace** : Ensemble de données numérisées constituant un univers d'information et un milieu de communication, lié à l'interconnexion mondiale des équipements de communications électroniques ;
- **Cybernétique** : Science qui utilise les résultats de la théorie du signal et de l'information pour développer une méthode d'analyse et de synthèse des systèmes complexes, de leurs relations fonctionnelles et des mécanismes de contrôle, en biologie, économie, informatique, etc ;
- **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 ;
- **Déchiffrement des données** : Opération inverse du chiffrement. Il s'agit du processus effectué pour déverrouiller les fichiers cryptés. Il intervient dans le domaine de la cryptographie, un ensemble d'algorithmes mathématiques qui codent les données de l'utilisateur de manière à ce que seul le destinataire puisse les lire. Le déchiffrement des données se fait grâce à une clé secrète ou un mot de passe. Il est à différencier du décryptage qui consiste à vouloir déchiffrer les données sans possession de la clé secrète ou du mot de passe ;
- **Déni de service** : Attaque par saturation d'une ressource du système d'information ou du réseau de communications

électroniques, afin qu'il s'effondre et ne puisse plus réaliser les services attendus de lui ;

- **Donnée à caractère personnel** : Toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique ;
- **Donnée informatique** : Toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction ;
- **Donnée relative au trafic** : Toutes données ayant trait à une communication passant par un système d'information, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent ;
- **Donnée relative aux abonnés** : Toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir :
- **Ecoute active** : Attaque où l'attaquant tente de modifier les ressources du système ou d'affecter leur fonctionnement ;
- **Ecoute passive** : Attaque ou l'attaquant tente de lire ou d'utiliser les informations du système sans modifier les ressources du système ;
- **Fournisseur de contenus** : Une personne ou une entreprise spécialisée dans la création, la structuration et la livraison de produits informationnels ;
- **Infrastructure essentielle** : Réseau de communications électroniques ou système d'information indispensable à la fourniture des services essentiels tels que l'ensemble des processus, des systèmes, des installations, des technologies, des réseaux, des biens et des services indispensables pour assurer la santé, la sûreté, la sécurité ou le bien-être économique des Centrafricains ;
- **Interception** : Processus par lequel une tierce partie non autorisée intercepte une conversation ou un transfert de données

en cours, soit en écoutant, soit en prenant connaissance des données informatiques y-relatives, soit en se faisant passer pour un participant légitime ;

- **Intrusion** : 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 ;
- **Logiciel d'accès à distance** : Accès à un ordinateur depuis un autre endroit via une connexion réseau ou via Internet, permettant d'effectuer de nombreuses tâches sur l'ordinateur distant, notamment installer des logiciels, modifier les paramètres et exécuter des applications ;
- **Logiciel espion** : Type particulier de logiciel trompeur collectant les informations personnelles (sites web les plus visités, mots de passe, etc.) auprès d'un utilisateur du réseau de communications électroniques ;
- **Logiciel Trompeur** : Logiciel effectuant des opérations sur un équipement terminal d'un utilisateur sans informer préalablement cet utilisateur de la nature exacte des opérations que le 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 ;
- **Matériel raciste et xénophobe** : Tout matériel écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence, contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments, ou qui incite à de tels actes ;
- **Matériel xénophobe** : Tout écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence contre une personne ou un groupe de personnes, en raison de la couleur, de l'ascendance ou de l'origine nationale ou ethnique ou de la religion, dans la mesure où ce dernier sert de prétexte à l'un ou à l'autre de ces éléments ou qui incite à de tels actes ;
- **Mineur ou Enfant** : Toute personne physique âgée de moins de 18 ans au sens de la Charte Africaine sur les droits et le bien-être de l'Enfant et de la Convention des Nations Unies sur les droits de

l'enfant ;

- **Moyens de diffusion publique** : Procédé technique destiné à atteindre le public et généralement tout moyen de communication numérique par voie électronique ; la radiodiffusion, la télévision, le cinéma, la presse en ligne, l'affichage, l'exposition, la distribution d'écrits ou d'images de toutes natures (sms, e-mail etc.), l'internet, les réseaux sociaux, les discours, chants, cris ou menaces proférés dans les lieux ou réunions publics ;
- **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 ;
- **Opérateur de services essentiels** : Tout opérateur, public ou privé, offrant des services essentiels au fonctionnement de la société ou de l'économie et dont la continuité pourrait être gravement affectée par des incidents touchant les réseaux de communications électroniques ou systèmes d'information nécessaires à la fourniture desdits services ;
- **Pare-feu** : Logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il surveille et contrôle les applications et les flux de données ;
- **Point de contact 24/7** : Point de contact joignable 24/24 heures, 7/7 jours, afin d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale ;
- **Politique de cyber sécurité** : Référentiel de sécurité établi par une organisation, reflétant sa stratégie de sécurité et spécifiant les moyens de la réaliser ;
- **Pornographie infantile** : Toute donnée, quelle qu'en soit la nature ou la forme ou le support, représentant ;
- **Pornographie** : Une représentation complaisante des sujets dans une œuvre littéraire, artistique ou cinématographique portant atteinte aux bonnes mœurs ;
- **Port** : Point d'entrée à un service, exemple le service web, le service mail. Dans le protocole TCP-IP chaque équipement possède au moins une adresse IP. Chaque adresse ne supporte pas moins de 65000 ports offrant chacun un service. L'ensemble

des services est référencé et donne lieu à une affectation précise des ports. Un site web est ainsi visible sur le port 80, l'envoi de mail se fait sur le port 25 et sa réception sur le port 110 ;

- **Procédures Opérationnelles Standard pour la collecte, l'analyse et la présentation des preuves électroniques (POS)** : Ensemble de procédures à suivre pour la récupération, la sécurisation, le transport et le traitement des preuves numériques, ainsi que pour leur analyse et leur présentation ;
- **Programme informatique** : Séquence d'instructions qui spécifie, étape par étape, les opérations à effectuer par un ordinateur ou une composante d'ordinateur pour obtenir un résultat ;
- **Prolifération** : Activité visant à fabriquer, se procurer, mettre au point, posséder, transporter, transférer ou à utiliser des armes nucléaires, chimiques ou biologiques ou leurs vecteurs, en particulier à des fins terroristes ;
- **Raciste et xénophobe en matière des technologies de l'information et de la communication** : Tout matériel écrit, toute image ou tout autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance, de l'origine nationale ou ethnique ou de la religion ;
- **Reroutage anormal** : Modification du circuit d'acheminement des données dans un réseau de télécommunications de manière illégale. Le réseau peut être informatique, téléphonique ou encore de transports ;
- **Réseau de communications électroniques** : Systèmes 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 circuit ou de paquet, y compris l'Internet) et mobile, 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 câblés de télévision, quel que soit le type d'information transmise ;
- **Service essentiel** : Service répondant aux exigences indispensables de la vie collective, à la dignité humaine et servant l'intérêt général. Il s'agit notamment des services essentiels urbains en réseau qui gèrent

des flux (eau, assainissement, énergie, gestion des déchets et mobilité) des services sociaux qui se structurent autour d'équipements et structures d'accueil (éducation, santé, voire culture) ;

- **Système d'information** : Ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) qui permet de collecter, de regrouper, de classifier, de traiter et de diffuser l'information ;
- **Système de détection d'intrusions** : Systèmes permettant de détecter les incidents qui pourraient conduire aux violations de la politique de sécurité et permettant de diagnostiquer des intrusions potentielles ;
- **Système informatique** : Tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données ;
- **Technologie de l'Information et de la Communication** : Technologie employée pour recueillir, stocker, utiliser et envoyer des informations ainsi que celles qui impliquent l'utilisation des ordinateurs ou de tout système de communication, y compris de télécommunication :
- des images réalistes représentant un enfant se livrant à un comportement sexuellement explicite non effectif ;
- l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ;
- le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;
- toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services ;
- un enfant se livrant à un comportement sexuellement explicite et effectif ;
- une personne qui apparaît comme un enfant se livrant à un comportement sexuellement explicite.

Art. 6 : Les termes et expressions non définis dans cette loi, conservent leurs définitions ou significations données par les instruments juridiques internationaux auxquels l'Etat Centrafricain a souscrit, notamment, la Constitution de l'Union Internationale des Télécommunications, la Convention de l'Union Internationale des Télécommunications, le

Règlement des Radiocommunications et le Règlement des Télécommunications Internationales.

TITRE II : DE LA CYBERSECURITE

CHAPITRE I : DU CADRE DE LA GOUVERNANCE DE LA CYBERSECURITE

Art. 7 : La Présidence de la République est l'Autorité Gouvernementale en matière

de cybersécurité. Elle assure en collaboration avec le Ministère chargé de la Sécurité Publique et le Ministère chargé de l'Economie Numérique, la gouvernance stratégique de la cybersécurité en République Centrafricaine.

Art. 8 : Il est créé un établissement public, à caractère non commercial, doté de la personnalité juridique et de l'autonomie financière, assurant une mission d'utilité publique dénommée « Agence Nationale de la Cybersécurité, en abrégé ANCy ».

L'ANCy est l'autorité nationale en matière de sécurité des infrastructures essentielles et des systèmes d'information des autorités publiques.

Art. 9 : L'ANCy est placée sous les tutelles du Ministère chargé de la Sécurité Publique et du Ministère chargé de l'Economie Numérique.

Art. 10 : L'ANCy concourt à la définition et à la mise en œuvre de la politique et des orientations stratégiques en matière de cybersécurité et de lutte contre la Cybercriminalité. Elle apporte son concours aux services de Défense et de Sécurité Nationale.

A ce titre, elle :

- assure la fonction d'autorité nationale de sécurité des infrastructures essentielles et des systèmes d'information de l'Etat ;
- propose aux autorités gouvernementales compétentes les mesures destinées à répondre aux crises affectant ou menaçant la sécurité des infrastructures essentielles ou des systèmes d'information des autorités publiques ;
- anime et coordonne, dans le cadre des orientations fixées par les autorités gouvernementales compétentes, l'action gouvernementale en matière de sécurité des systèmes d'information ;
- désigne les opérateurs de services essentiels ;

- vérifie la pertinence, l'exhaustivité des listes d'infrastructures essentielles et assure leur mise à jour;
- fixe les règles relatives aux mesures de protection à mettre en œuvre par les opérateurs de services essentiels pour assurer la cybersécurité de leurs infrastructures essentielles et veille par des contrôles au respect desdites règles ;
- fixe les conditions financières de réalisation des contrôles et de délivrance des accréditations ;
- octroie des accréditations aux opérateurs de services essentiels qui respectent les règles en matière de cybersécurité ;
- prononce des astreintes et sanctions, y compris pécuniaires, à l'encontre des opérateurs de services essentiels qui ne respectent pas leurs obligations en termes de cybersécurité ;
- mène des inspections et audits des systèmes d'information des services de l'Etat et des infrastructures essentielles des opérateurs de services essentiels ;
- met en œuvre un système de détection et d'évaluation des menaces ou des évènements susceptibles d'affecter la sécurité des systèmes d'information de l'Etat, coordonne la réaction à ces évènements et apporte son concours pour répondre à ces incidents ;
- recueille les informations techniques relatives aux incidents affectant les infrastructures essentielles des opérateurs de services essentiels et les systèmes d'information de l'Etat ;
- délivre des agréments aux dispositifs et aux mécanismes de sécurité destinés à protéger, dans les systèmes d'informations, les informations couvertes par le secret défense ;
- certifie les dispositifs matériels ou logiciels et les services informatiques au regard de leur capacité à assurer des fonctions de cybersécurité ;
- recueille les descriptions des caractéristiques techniques des moyens de cryptologie ainsi que le code source des logiciels utilisés et délivre les autorisations d'exploiter et d'exporter aux prestataires de Services de Cryptologie ;
- participe aux négociations internationales et assure la liaison avec ses homologues étrangers ;

- assure la sensibilisation du public et la formation des personnels qualifiés dans le domaine de la sécurité des systèmes d'information ;
- assure la création d'une structure d'alerte et d'assistance sur l'Internet placée auprès de l'ANCy, chargée d'une mission de veille et de réponse aux attaques informatiques des systèmes d'information ;
- effectue des contrôles destinés à vérifier le respect par les opérateurs de services essentiels des obligations qui leur incombent et à les sanctionner en cas de non-respect.

Art. 11 : L'ANCy assume la fonction de Computer Emergency Response Team (CERT) ou Computer Security Incident Response Team (CSIRT) pour la République Centrafricaine et de point de contact 24/7.

A ce titre, elle :

- Contribue à la prévention des attaques informatiques ;
- Coordonne la prévention et la réponse aux incidents avec les entités partenaires nationales et les autres CERT étrangères ;
- Traite les alertes et réagit aux attaques informatiques ;
- Détecte les attaques ciblant les systèmes d'information gouvernementaux ;
- Détecte les vulnérabilités des systèmes ;
- Participe aux échanges d'informations avec d'autres CERT.

Art. 12 : L'organisation et le fonctionnement de l'ANCy sont définis par Décret pris en Conseil des Ministres.

CHAPITRE II : DES ACTIVITES DE SECURITE

Art. 13 : Il est créé un Fonds de Souveraineté Numérique, en abrégé FSN. Le Fonds de Souveraineté Numérique participe, entre autres, au financement des stratégies nationales de cybersécurité et appuie les actions de l'ANCy.

Un Décret pris en Conseil des Ministres définit les modalités de son financement et de sa gestion.

Art. 14 : Sont soumis à un audit obligatoire de sécurité, les réseaux de Communications Electroniques et les Systèmes d'Information des opérateurs, des autorités de certification et des fournisseurs de

services de Communications Electroniques.

Les conditions et les modalités de l'audit de sécurité ainsi que le suivi des recommandations contenues dans les rapports d'audit prévues à l'alinéa 1 ci-dessus sont définies par voie réglementaire.

Art. 15 : Le personnel de l'ANCy et les experts commis en vue d'accomplir des opérations d'audit sont astreints au secret professionnel.

CHAPITRE III : DE LA PROTECTION DES RESEAUX DE COMMUNICATIONS ELECTRONIQUES, DES SYSTEMES D'INFORMATION, DES OBLIGATIONS DES FOURNISSEURS D'ACCES, DES SERVICES, DES CONTENUS ET DE LA PROTECTION DE LA VIE PRIVEE DES PERSONNES

SECTION I : DE LA PROTECTION DES RESEAUX DE COMMUNICATIONS ELECTRONIQUES

Art. 16 : Les opérateurs des réseaux de Communications Electroniques et les fournisseurs de services de Communications Electroniques prennent toutes les mesures techniques et administratives nécessaires pour garantir la sécurité des services offerts.

A cet effet, ils sont tenus d'informer les usagers :

- du danger encouru en cas d'utilisation de leurs réseaux ;
- des risques particuliers de violation de la sécurité notamment, les dénis de services distribués, le reroutage anormal, les pointes de trafic, le trafic et les ports inhabituels, les écoutes passives et actives, les intrusions et tout autre risque ;
- de l'existence de moyens techniques permettant d'assurer la sécurité de leurs communications.

Art. 17 : Les opérateurs de réseaux et les fournisseurs de services de Communications Electroniques ont l'obligation de conserver les données de connexion et de trafic pendant une période d'au moins dix (10) ans.

Ils installent des mécanismes de surveillance de trafic des données de leurs réseaux. Ces données doivent être accessibles lors des investigations judiciaires.

Art. 18 : La responsabilité des opérateurs de réseaux et celle des fournisseurs de services de Communications Electroniques sont engagées lorsque l'utilisation des données prévues à l'article précédent porte atteinte aux libertés individuelles ou collectives des usagers et n'est pas

justifiée par un intérêt public ou privé prépondérant au sens de la Loi sur la Protection des données à caractère personnel.

SECTION II : DE LA PROTECTION DES SYSTEMES D'INFORMATION

Art. 19 : Les exploitants des Systèmes d'Information prennent toutes les mesures techniques et administratives afin de garantir la sécurité des services offerts.

A cet effet, ils se dotent de systèmes normalisés leur permettant d'identifier, d'évaluer, de traiter et de gérer continuellement les risques liés à la sécurité des Systèmes d'Information dans le cadre des services offerts directement ou indirectement.

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.

Les mécanismes prévus à l'alinéa ci-dessus, sont soumis à l'approbation et au visa conforme de l'ANCy.

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 autre attaque externe notamment par un système de détection d'intrusions.

Art. 20 : 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 violation 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-feu personnels, de systèmes de détection d'intrusions et l'activation des mises à jour automatiques.

Toutefois, lorsque de tels moyens techniques n'existent pas ou ne sont pas disponibles, les personnes morales dont l'activité est d'offrir un accès à des Systèmes d'information sont tenues d'informer les usagers de l'inexistence de tels moyens techniques et des risques y relatifs.

Art. 21 : Les exploitants des Systèmes d'Information informent les utilisateurs de l'interdiction faite d'utiliser le réseau de Communications Electroniques pour diffuser des contenus illicites au sens de la présente Loi ou tout autre acte de nature à entamer la sécurité des réseaux ou des Systèmes d'Information.

L'interdiction porte également sur la conception de logiciel trompeur, de logiciel espion, de logiciel potentiellement indésirable ou de tout autre outil pouvant conduire à un acte frauduleux.

Art. 22 : 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 d'au moins dix (10) ans.

Ils sont tenus d'installer des mécanismes de surveillance de contrôle d'accès aux données de leurs Systèmes d'Information.

Les données conservées doivent être accessibles lors des investigations judiciaires.

Les installations des exploitants des Systèmes d'Information ainsi que toutes entités collectant, stockant ou traitant des données de connexion et de trafic pour leur compte sur le territoire de la République Centrafricaine peuvent faire l'objet de perquisitions ou de saisies sur ordre d'une autorité judiciaire dans les conditions prévues par les lois et règlements en vigueur.

Art. 23 : Les exploitants des Systèmes d'Information évaluent et révisent leurs systèmes de sécurité de manière périodique. Ils introduisent en cas de nécessité les modifications appropriées dans leurs pratiques, mesures et techniques de sécurité en fonction de l'évolution des technologies, ce sous le contrôle de l'ANCy.

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

Art. 24 : Les fournisseurs de contenus des réseaux de Communications Electroniques et Systèmes d'Information sont tenus d'assurer la disponibilité des contenus, ainsi que celle des données stockées dans

leurs installations.

Ils ont l'obligation de mettre en place les filtres adéquats pour faire face aux atteintes préjudiciables aux données personnelles et à la vie privée des utilisateurs pour autant que ceux-ci existent et soient disponibles.

Art. 25 : Les réseaux de Communications Electroniques et les Systèmes d'Information sont soumis à un régime d'audit obligatoire de sécurité et de leurs systèmes par l'ANCy.

L'audit de sécurité et les mesures d'impact de gravité sont effectués chaque année au moins ou à chaque fois que les circonstances l'exigent.

Les rapports d'audit adressés à l'ANCy pour approbation sont confidentiels. Elle les transmet aux Ministères en charge de la Sécurité Publique et de l'Economie Numérique pour décision.

Un texte règlementaire fixe les conditions d'évaluation des niveaux d'impact de gravité.

SECTION III : DES OBLIGATIONS DES FOURNISSEURS D'ACCES, DE SERVICES, DES CONTENUS ET DES PRESTATAIRES DE SERVICES DE CRYPTOLOGIE

Art. 26 : Les fournisseurs dont l'activité est d'offrir un accès à des services de Communications Electroniques, informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposent au moins un de ces moyens.

Art. 27 : La responsabilité des fournisseurs 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, est engagée en cas de manquement à leurs obligations.

Art. 28 : Les fournisseurs susmentionnés, sont astreints au secret professionnel et sont tenus de conserver, pendant une durée d'au moins dix (10) ans, les données permettant l'identification de toute personne ayant contribué à la création du contenu des services dont ils sont prestataires.

Les fournisseurs prennent toutes mesures propres à assurer la sécurité et l'intégrité de ces données, notamment par des techniques de cryptage.

Ils fournissent aux personnes qui offrent un service de Communications Electroniques des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues par la présente loi.

L'Autorité Judiciaire peut requérir la communication des donnés prévues à l'alinéa 1 auprès des prestataires mentionnés aux articles 25 et 26 de la présente loi.

Art. 29 : Les fournisseurs dont l'activité consiste à éditer les contenus d'un service de Communications Electroniques, mettent à la disposition du public les informations ci-après :

- pour les personnes physiques : nom, prénoms, domicile et numéro de téléphone, e-mail et, si elles sont assujetties aux formalités d'inscription au registre de commerce et du crédit mobilier (RCCM), le numéro de leur inscription ;
- pour les personnes morales : leur dénomination ou raison sociale, leur siège social, leur numéro de téléphone, leur e-mail et, s'il s'agit des personnes morales assujetties aux formalités d'inscription au registre de commerce et du crédit mobilier (RCCM), le numéro de leur inscription, le capital social et l'adresse de leur siège social ;
- pour l'éditeur du contenu : nom, prénoms, numéro de téléphone, e-mail du directeur ou du codirecteur de la publication et, le cas échéant, ceux du responsable de la rédaction.

Art. 30 : Les fournisseurs éditant à titre non professionnel un service de Communications Electroniques ne peuvent tenir à la disposition du public que le nom, la dénomination ou la raison sociale et l'adresse du prestataire.

Art. 31 : Les fournisseurs de service des communications électroniques ont obligation de répondre à la demande d'une exigence d'un droit de réponse d'une personne victime d'une diffamation ou de toute autre atteinte à la personnalité.

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

En cas de refus de s'exécuter, la victime dispose d'un droit de contrainte par voie judiciaire.

Art. 32 : Toute personne assurant une activité de stockage automatique et de transmission de contenus sur un réseau de Communications

Electroniques ou de fourniture d'accès à un réseau de Communications Electroniques ne peut voir sa responsabilité engagée que lorsqu'elle :

- est à l'origine de la demande de transmission litigieuse ;
- a sélectionné ou modifié les contenus faisant l'objet de la transmission sans autorisation ;
- ne s'est pas conformée à leurs 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.

Art. 33 : Tout prestataire de services de cryptologie a l'obligation de communiquer spontanément à l'ANCy une description des caractéristiques techniques du moyen de cryptologie ainsi que le code source des logiciels utilisés.

SECTION IV: DE LA PROTECTION DE LA VIE PRIVEE DES PERSONNES

Art. 34 : Toute personne a droit au respect de sa vie privée. Les juges peuvent prendre les mesures qui s'imposent pour empêcher ou faire cesser toute atteinte à la vie privée.

Art. 35 : La confidentialité des communications acheminées à travers les réseaux de Communications Electroniques et les Systèmes d'Information, y compris les données relatives au trafic, est assurée par les opérateurs et exploitants des réseaux de Communications Electroniques et des Systèmes d'Information.

Art. 36 : Le fournisseur est responsable des contenus véhiculés par son Système d'Information, lorsque ceux-ci portent atteinte à la dignité humaine, à l'honneur et à la vie privée.

Art. 37 : Il est fait interdiction à toute personne physique ou morale d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic, 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 autorisée par la loi ou par une autorité judiciaire compétente.

Toutefois, le stockage technique préalable à l'acheminement de toute communication est autorisé aux opérateurs et exploitants des réseaux de Communications Electroniques, sans préjudice du principe de

confidentialité.

Art. 38 : Est autorisé, l'enregistrement des communications et des données de trafic effectué dans le cadre professionnel au sens des articles 17, 22 et 28 de la présente loi en vue de servir de preuve numérique conformément aux dispositions du Code Pénal et du Code de Procédure Pénale.

Art. 39 : L'utilisation des réseaux de Communications Electroniques 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 sur la base de la présente loi et avec l'autorisation expresse d'une autorité judiciaire compétente.

Art. 40 : Est interdite, 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.

Il en est de même de l'émission des messages électroniques en usurpant l'identité d'autrui.

TITRE III : DE LA CYBERCRIMINALITE

CHAPITRE I : DES INFRACTIONS ET DES SANCTIONS

SECTION I : DES INFRACTIONS ET DES PEINES

Art. 41 : Sont punis d'un emprisonnement d'un (1) à cinq (5) ans et d'une amende d'un million (1.000.000) à dix millions (10.000.000) de FCFA, le personnel de l'ANCy 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.

Art. 42 : Est puni d'un emprisonnement d'un (1) mois et un (1) jour à un (1) an, le refus de déférer aux convocations des Agents habilités de l'ANCy.

Art. 43 : Est puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende de cent mille (100.000) à un million (1.000.000) de FCFA 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 ou refuse de fournir les informations ou documents y afférents.

Art. 44 : Est puni d'un emprisonnement d'un (01) an à cinq (5) ans et d'une amende de dix millions (10.000.000) à cinquante millions (50.000.000) de FCFA 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 Electroniques ou d'un Système d'Information, notamment en transmettant, endommageant, provoquant une perturbation grave ou une interruption du fonctionnement dudit système ou dudit réseau.

Ces peines sont portées au double en cas de suppression, modification ou altération des données contenues dans le Système d'Information.

Art. 45 : Est puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende de dix millions (10.000.000) à cinquante millions (50.000.000) de FCFA 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 Electroniques, d'un Système d'Information, d'un équipement terminal ou à tout autre support de données, afin d'obtenir des informations ou des données informatiques en relation avec un Système d'Information connecté à un autre.

Art. 46 : Est puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende de dix millions (10.000.000) à cinquante millions (50.000.000) de FCFA, celui qui provoque par saturation, l'attaque d'une ressource de réseau de Communications Electroniques ou d'un Système d'Information dans le but de l'effondrer ou d'empêcher la réalisation des services attendus.

Art. 47 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende de dix millions (10.000.000) à cinquante millions (50.000.000) de FCFA, toute personne qui, frauduleusement :

- introduit, supprime ou modifie les données d'un système informatique ;
- détruit, détériore, altère, rend inaccessibles ou endommage ces données ;
- soustrait ces données pour son usage personnel ou pour les céder

à un tiers, à titre onéreux ou gratuit ;

- détruit, entrave, fausse, perturbe, interrompt le fonctionnement d'un système informatique.

Est punie des mêmes peines, toute personne qui intercepte frauduleusement par des moyens techniques des données informatisées lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système informatique.

Lorsque l'infraction est commise au préjudice de l'Etat Centrafricain, son auteur est puni d'une peine de vingt (20) ans à trente (30) ans des travaux forcés à temps et d'une amende de cinquante millions (50 000 000) à cent millions (100 000 000) de FCFA.

Art. 48 : Est puni d'un emprisonnement de cinq (5) ans à dix (10) ans et d'une amende de vingt-cinq millions (25.000.000) à cinquante millions (50.000.000) de FCFA, ou de l'une de ces deux peines seulement, celui qui, par la voie d'un Système d'Information, d'un système informatique ou d'un réseau de Communications Electroniques contrefait, falsifie une carte de paiement, de crédit, ou de retrait en fait usage ou tente d'en faire usage en connaissance de cause.

Est puni des mêmes peines, quiconque, en connaissance de cause, accepte de recevoir par voie de Communications Electroniques, un règlement au moyen d'une carte de paiement, de crédit ou de retrait contrefaite ou falsifiée.

Art. 49 : Est puni d'un emprisonnement d'un (1) à cinq (5) ans et d'une amende d'un million (1.000.000) à cinq millions (5.000.000) de FCFA, quiconque, au moyen d'un procédé quelconque porte atteinte à l'intimité de la vie privée d'autrui en observant, fixant, enregistrant ou transmettant, sans le consentement de la victime, des données électroniques se rapportant à des faits ayant un caractère privé ou confidentiel.

Art. 50 : Est puni d'un emprisonnement d'un (1) à cinq (5) ans et d'une amende d'un million (1.000.000) à cinq millions (5.000.000) de FCFA ou de l'une de ces deux peines seulement, quiconque collecte par des moyens illicites, des données nominatives d'une personne en vue de porter atteinte à son intimité et à sa dignité ou à sa personnalité.

Ces peines sont portées au double à l'encontre de celui qui met ou fait mettre en ligne, conserve ou fait conserver en mémoire informatisée, sans l'accord expres 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.

Art. 51 : Est puni d'un emprisonnement de deux (2) à cinq (5) ans et d'une amende d'un million (1.000.000) à cinq millions (5.000.000) de FCFA ou de l'une de ces deux peines seulement, celui qui enregistre et diffuse à but lucratif, par la voie de Communications Electroniques ou d'un Système d'Information sans le consentement de l'intéressé, des images portant atteinte à son intégrité morale.

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 en vue de servir de preuve en justice conformément aux dispositions du Code de Procédure Pénale.

Art. 52 : Est puni d'un emprisonnement d'au moins dix (10) ans et d'une amende de cinq millions (5.000.000) à dix millions (10.000.000) de FCFA ou de l'une de ces deux peines seulement, celui qui confectionne, transporte, diffuse, par voie de Communications Electroniques ou d'un Système d'Information, un message à caractère pornographique infantile, ou de nature à porter gravement atteinte à la dignité d'un enfant.

Art. 53 : Est puni d'un emprisonnement de six (6) mois à deux (2) ans et d'une amende de cinq millions (5.000.000) à dix millions (10.000.000) de FCFA ou de l'une de ces deux peines seulement, celui qui publie ou propage par voie de Communications Electroniques ou d'un Système d'Information, une nouvelle des informations fausses, des pièces fabriquées, falsifiées voire mensongères et basées sur la mauvaise foi sans pouvoir en rapporter la preuve de véracité ou justifier qu'il a de bonnes raisons de croire à la véracité de ladite nouvelle dans le but d'inquiéter un tiers ou de l'importuner.

Ces peines sont portées au double lorsque l'infraction est commise dans le but de porter atteinte à la paix publique.

SECTION II : DE L'ABUS DE DISPOSITIFS INFORMATIQUES ET DE L'ASSOCIATION DE MALFAITEURS INFORMATIQUES

Art. 54 : Quiconque produit, vend, importe, diffuse, offre, cède ou met à disposition un équipement, un programme informatique, tout dispositif ou toute donnée conçue ou spécialement adaptée ou un mot de passe, un code d'accès ou des données informatisées

similaires permettant d'accéder à tout ou partie d'un système d'information, est puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un million (1 000 000) à cinq millions (5 000 000) FCFA.

Art. 55 : Est puni d'un emprisonnement d'au moins dix (10) ans et d'une amende de cinq millions (5.000.000) à dix millions (10.000.000) de FCFA ou de l'une de ces deux peines seulement, celui qui confectionne, transporte, diffuse, par voie de Communications Electroniques ou d'un Système d'Information, un message à caractère pornographique infantile, ou de nature à porter gravement atteinte à la dignité d'un enfant.

Art. 56 : Quiconque, ayant connaissance de la convention secrète de déchiffrement, d'un moyen de cryptographie susceptible d'être utilisé pour préparer, faciliter ou commettre un crime ou un délit, refuse de remettre ladite convention aux Autorités Judiciaires ou de la mettre en œuvre, sur les réquisitions de ces Autorités est puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende de cent mille (100.000) à un million (1.000.000) de FCFA ou de l'une de ces deux peines.

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) ans à cinq (5) ans d'emprisonnement et l'amende d'un million (1.000.000) à cinq millions (5.000.000) de FCFA.

SECTION III : DES ATTENTATS A LA PUDEUR ET DE LA PORNOGRAPHIE INFANTILE

Art. 57 : Quiconque commet les faits d'attentat à la pudeur prévus par le Code Pénal, lorsque la victime est mise en contact avec l'auteur desdits faits, grâce à l'utilisation des Communications Electroniques ou des Systèmes d'Information, est puni d'un emprisonnement de cinq (5) à dix (10) ans et d'une amende de cinq millions (5.000.000) à dix millions (10.000.000) de FCFA ou de l'une de ces deux peines seulement.

Ces mêmes peines s'appliquent aux coauteurs et complices.

Art. 58 : Quiconque fixe, enregistre, confectionne, produit, importe, exporte, diffuse, offre, met à disposition, procure, rend disponible à titre

onéreux ou gratuit, par voie de Communications Electroniques, d'un Système d'Information, d'un Système informatique ou par quelque moyen électronique que ce soit, un message, une image ou une présentation à caractère de pornographie infantile est puni d'un emprisonnement d'au moins dix (10) ans et d'une amende de cinq millions (5.000.000) à dix millions (10.000.000) de FCFA ou de l'une de ces deux peines seulement.

Ces mêmes peines s'appliquent aux coauteurs et complices.

Art. 59 : Quiconque télécharge, obtient par voie électronique, possède, détient ou consulte, dans un réseau de Communications Electroniques, dans un Système d'Information ou dans un Système informatique, un message, une image ou une présentation à caractère de pornographie infantile est puni d'un emprisonnement d'un (1) à cinq (5) ans et d'une amende de cinq millions (5.000.000) à dix millions (10.000.000) de FCFA ou de l'une de ces deux peines seulement.

Ces peines sont portées au double, lorsqu'un réseau de Communications Electroniques a été utilisé pour la diffusion de l'image ou la représentation du mineur à destination du public.

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

Est puni des mêmes peines, quiconque facilite l'accès à des images, des documents, du son ou à une représentation à caractère de pornographie à un enfant.

Art. 60 : Toute personne adulte qui propose intentionnellement, par le biais des Technologies de l'Information et de la Communication, une rencontre à un enfant, dans le but de commettre à son encontre une des infractions prévues aux articles 57, 58 et 59 commet un crime.

SECTION IV : DE LA XENOPHOBIE PAR LE BIAIS D'UN SYSTEME D'INFORMATION

Art. 61 : Quiconque, par le biais d'un Système d'Information, crée, télécharge, diffuse, propage ou met à disposition, sous quelque forme que ce soit, du matériel raciste et xénophobe ou ayant pour but de dénigrer autrui ou un groupe de personnes en raison de son appartenance, ascendance, origine ethnique, sa religion ou son opinion, est puni d'un emprisonnement de six (6) mois à cinq (5) ans et d'une amende d'un million (1.000.000) à dix millions (10.000.000) de CFA ou de

l'une de ces deux peines seulement.

Art. 62 : Quiconque, par le biais d'un Système d'Information, profère ou propage, une menace envers autrui ou un groupe de personnes en raison de son appartenance, ascendance, origine ethnique, sa religion ou son opinion, est puni d'un emprisonnement de six (6) mois à cinq (5) ans et d'une amende d'un million (1.000.000) à dix millions (10.000.000) de FCFA ou de l'une de ces deux peines seulement.

Art. 63 : Quiconque, par le biais d'un Système d'Information outrage, profère ou propage une insulte envers une personne en raison de son appartenance à un groupe, qui se caractérise par sa couleur, son ascendance ou sa religion, ou l'opinion politique est puni d'un emprisonnement de six (6) mois à cinq (5) ans et d'une amende d'un million (1.000.000) à dix millions (10.000.000) de FCFA ou de l'une de ces deux peines seulement.

Art. 64 : Quiconque, par le biais d'un Système d'Information, diffuse, propage ou met à disposition des propos, vidéo ou des images qui nient, minimisent ou font l'apologie des actes constitutifs de génocide ou de crimes contre l'humanité, est puni d'un emprisonnement de six (6) mois à cinq (5) ans et d'une amende d'un million (1.000.000) à dix millions (10.000.000) de FCFA ou de l'une de ces deux peines seulement.

Art. 65 : La juridiction peut, concomitamment à la condamnation, prononcer la confiscation des matériels, équipements, instruments, programmes informatiques ou tout dispositif ou données appartenant au condamné et ayant servi à commettre les infractions prévues aux articles 61 à 64 de la présente loi.

SECTION V : DES INFRACTIONS LIEES AUX ACTIVITES DES PRESTATAIRES DE SERVICES DE COMMUNICATION AU PUBLIC PAR VOIE ELECTRONIQUE

Art. 66 : Quiconque, en connaissance de cause, et par voie électronique, présente un contenu ou une activité illicite aux personnes mentionnées aux articles 26 et 27 ci-dessus dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion par un prestataire de service de communication, est puni d'un emprisonnement de six (6) mois à un (1) an et d'une amende de deux cent mille (200.000) à un million (1.000.000) de FCFA ou l'une de ces deux peines seulement.

Toute personne nommée ou désignée dans un service de

communication au public par voie électronique qui ne publie pas la réponse découlant de l'exercice du droit de réponse quarante-huit (48) heures ouvrables après la réception de la demande, est punie d'une amende de deux cent mille (200.000) à deux millions (2.000.000) de FCFA, sans préjudice de toutes autres peines prévues par les textes en vigueur.

Art. 67 : Est puni d'un emprisonnement de six (6) mois à un (1) an et d'une amende de cent mille (100.000) à cinq cent mille (500.000) FCFA ou de l'une de ces deux peines seulement, tout prestataire de service de communication au public par voie électronique qui ne satisfait pas à l'obligation de :

- mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à sa connaissance les données illicites telles, l'incitation à la haine raciale, la pornographie infantile, le terrorisme ;
- informer promptement les Autorités Publiques compétentes de toutes les activités illicites qui lui sont signalées et qu'exercent les destinataires de ses services ;
- conserver des données permettant l'identification de quiconque a contribué à la création du contenu, ou de l'un des contenus des services dont il est prestataire.

En cas de refus du prestataire de services de communication défère à la demande d'une Autorité Judiciaire en vue d'obtenir communication des données il est fait application des mêmes peines.

Art. 68 : Toute personne exerçant une activité dans le domaine du commerce électronique qui ne satisfait pas aux obligations d'information relatives au maintien de l'ordre et de la Sécurité Publique, à la préservation des intérêts de la Défense Nationale, à la protection des enfants, de la vie privée, de la santé publique ou des consommateurs, est punie d'un emprisonnement de six (6) mois à un (1) an et d'une amende de cent mille (100.000) à cinq cent mille (500.000) FCFA ou de l'une de ces deux peines seulement.

Art. 69 : Quiconque trompe ou tente de tromper, par des manœuvres frauduleuses, l'acheteur sur l'identité, la nature ou l'origine du bien vendu, en livrant un bien autre que celui commandé par le consommateur, est puni d'un emprisonnement de trois (3) mois à un (1) an et d'une amende de cinq cent mille (500.000) à dix millions (10.000.000) de FCFA ou de l'une de ces deux peines seulement.

Art. 70 : Est puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un million (1.000.000) à cinq millions (5.000.000) de FCFA, le dirigeant de droit ou de fait d'une personne morale exerçant les activités définies aux articles 26 et 27 de la présente loi, qui n'a pas conservé les éléments d'information visés aux articles 17 et 22 ci-dessus.

Est passible des mêmes peines, le dirigeant de droit ou de fait d'une personne morale exerçant les activités définies aux articles 29 à 31.

Art. 71 : Les personnes morales sont pénalement responsables des infractions commises, pour leur compte, par leurs organes dirigeants.

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

Les personnes morales sont punies d'une amende de cinq millions (5.000.000) à cinquante millions (50.000.000) de FCFA.

Art. 72 : Nonobstant la peine prévue à l'alinéa 3 de l'article ci-dessus, les peines accessoires suivantes peuvent être prononcées :

- la dissolution, lorsque la personne morale a été détournée de son objet pour servir de support à la commission des faits incriminés, ou lorsqu'il s'agit d'un crime ou d'un délit puni en ce qui concerne les personnes physiques d'une peine d'emprisonnement supérieure ou égale à cinq (5) ans ;
- l'interdiction, à titre définitif ou pour une durée de cinq (5) ans au plus, d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ;
- la fermeture temporaire pour une durée de cinq (5) ans au plus, dans les conditions prévues par le Code Pénal, de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés;
- l'exclusion des marchés publics à titre définitif ou pour une durée de cinq (5) ans au plus ;
- l'interdiction, à titre définitif ou pour une durée de cinq (5) ans au plus, de faire appel public à l'épargne ;
- l'interdiction, pour une durée de cinq (5) ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ou d'utiliser des cartes de paiement;
- 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.

SECTION VI : DES INFRACTIONS LIEES A LA PROSPECTION DIRECTE ET A LA PUBLICITE PAR VOIE ELECTRONIQUE

Art. 73 : L'utilisation de courriers électroniques, télécopieurs, messageries instantanées, réseaux sociaux ou de systèmes automatisés, d'appel et de communication sans intervention humaine, tels que d'automates d'appel, à des fins de publicité, n'est autorisée qu'avec le consentement préalable, libre et spécifique du destinataire des messages.

Quiconque contrevient aux dispositions ci-dessus, est puni d'un emprisonnement d'un (1) à trois (3) mois et d'une amende de cent mille (100. 000) à cinq cent mille (500. 000) FCFA ou de l'une de ces deux peines seulement.

Art. 74 : Quiconque émet, à des fins de prospection directe, des messages au moyen d'automates d'appel, télécopieurs, courriers électroniques, messageries instantanées et réseaux sociaux sans indiquer de coordonnées valables permettant aux destinataires de demander la cessation de telles communications, est puni d'un emprisonnement d'un (1) mois à trois (3) mois et d'une amende de cent mille (100.000) à cinq cent mille (500.000) FCFA ou l'une de ces deux peines seulement.

Est puni des mêmes peines, quiconque dissimule ou tente de dissimuler l'identité de la personne pour le compte de laquelle la communication est émise et mentionne un objet sans rapport avec la prestation ou le service proposé.

Art. 75 : Tout prestataire qui ne satisfait pas à la demande d'un destinataire de faire cesser l'envoi de messages, à des fins de prospection directe, au moyen d'automates d'appel, télécopieurs, courriers électroniques, messageries instantanées et réseaux sociaux, est puni d'un emprisonnement d'un (1) mois à trois (3) mois et d'une amende de cent mille (100.000) à cinq cent mille (500.000) FCFA ou de l'une de ces deux peines seulement.

Art. 76 : Tout prestataire de service des communications électroniques qui dans l'exercice de ses activités ne satisfait pas aux exigences des

publicités, des offres promotionnelles et des jeux concours, est puni d'un emprisonnement de six mois (06) à deux (02) ans et d'une amande de cent mille (100.000) à cinq cent mille (500.000) FCFA ou de l'une de ces deux peines seulement.

SECTION VII : DES INFRACTIONS RELATIVES A LA CRYPTOLOGIE

Art. 77 : Tout prestataire de service de cryptologie qui ne satisfait pas à l'obligation de communiquer à l'ANCy une description des caractéristiques techniques du moyen de cryptologie ainsi que le code source des logiciels utilisés, est puni d'un emprisonnement de six (6) mois à deux (2) ans et d'une amende de quatre cent mille (400.000) à deux millions (2.000.000) de FCFA ou de l'une de ces deux peines seulement.

Art. 78 : Quiconque fournit ou importe un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité, sans satisfaire à l'obligation de déclaration préalable auprès de l'ANCy, est puni d'un emprisonnement de six (6) mois à cinq (5) ans et d'une amende de quatre cent mille (400.000) à cinq millions (5.000.000) de FCFA ou de l'une de ces deux peines seulement.

Art. 79 : Quiconque exporte un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sans avoir obtenu préalablement l'autorisation de l'ANCy est puni d'un emprisonnement d'un (1) à cinq (5) ans et d'une amende d'un million (1.000.000) à vingt millions (20.000.000) de FCFA ou de l'une de ces deux peines seulement.

Art. 80 : Quiconque fournit des prestations de cryptologie, sans avoir obtenu préalablement l'agrément de l'ANCy est puni d'un emprisonnement d'un (1) à cinq (5) ans et d'une amende d'un million (1.000.000) à vingt millions (20.000 000) de FCFA ou de l'une de ces deux peines seulement.

Art. 81 : Quiconque met à la disposition d'autrui un moyen de cryptologie ayant fait l'objet d'une interdiction d'utilisation et de mise en circulation, est puni d'un emprisonnement d'un (1) à cinq (5) ans et d'une amende d'un million (1.000.000) à vingt millions (20.000.000) de FCFA ou de l'une de ces deux peines seulement.

Art. 82 : Quiconque fait obstacle à une mission de contrôle de l'ANCy, est puni d'un emprisonnement d'un (1) à cinq (5) ans et d'une amende d'un million (1.000.000) à vingt millions (20.000.000) de FCFA ou de l'une de ces deux peines seulement.

Art. 83 : Quiconque met en place un accès dérobé à des données ou à un Système d'Information sans l'autorisation de l'utilisateur légitime, est puni d'un emprisonnement de deux (2) à cinq (5) ans et d'une amende de deux millions (2.000.000) à trente millions (30.000.000) de FCFA ou de l'une de ces deux peines seulement.

SECTION VIII : DE L'ADAPTATION DES INFRACTIONS DE DROIT COMMUN AUX TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Art. 84 : Quiconque commet un vol, au sens du Code Pénal, par le biais des technologies de l'information et de la communication est puni d'un emprisonnement de six (6) mois à cinq (5) ans et d'une amende de quatre cent mille (400.000) à cinq millions (5.000.000) de FCFA ou de l'une de ces deux peines seulement.

Art. 85 : Quiconque extorque des fonds, des valeurs, une signature, un écrit, un acte, un titre ou une pièce quelconque contenant ou opérant obligation, disposition ou décharge, par le biais des Technologies de l'Information et de la Communication, est puni d'un emprisonnement de six (6) mois à cinq (5) ans et d'une amende de quatre cent mille (400.000) à cinq millions (5.000.000) de FCFA ou de l'une de ces deux peines seulement.

Art. 86 : Quiconque, par le biais des Technologies de l'Information et de la Communication, commet un abus de confiance tel que défini par le Code Pénal encourt une peine qui peut être portée au double de celle prévue par le Code Pénal.

Art. 87 : Quiconque, par le biais des Technologies de l'Information et de la Communication, commet un acte d'escroquerie encourt le double des peines prévues par le Code Pénal.

Art. 88 : Quiconque, par le biais des Technologies de l'Information et de la Communication trompe ou tente de tromper le destinataire de produits ou de services sur l'objet, l'origine, la nature, la qualité substantielle, la quantité, la teneur ou la composition est puni d'un

emprisonnement de deux (2) à dix (10) ans et d'une amende de quatre cent mille (400.000) à quatre millions (4.000.000) de FCFA.

Art. 89 : Quiconque, par le biais des Technologies de l'Information et de la Communication recèle, en tout ou partie, les choses enlevées, détournées ou obtenues à l'aide d'un crime ou d'un délit, est puni d'un emprisonnement d'un (1) à dix (10) ans et d'une amende de cent mille (100.000) à deux millions (2.000.000) de FCFA, sans préjudice des peines plus fortes s'il échet, en cas de complicité de crime ou du délit.

Art. 90 : Quiconque par le biais des Technologies de l'Information et de la Communication, commet un acte qualifié de blanchiment de capitaux, commet un crime punissable de la réclusion à temps ou à perpétuité.

Art. 91 : Quiconque, par le biais des Technologies de l'Information et de la Communication, accomplit intentionnellement un acte qui constitue une infraction de terrorisme ou de financement de terrorisme, commet un crime punissable de la réclusion à temps ou à perpétuité.

Art. 92 : Quiconque copie ou tente de copier frauduleusement des données informatiques au préjudice d'un tiers est puni d'un emprisonnement de six (6) mois à cinq (5) ans et d'une amende de cent mille (100.000) à cinq millions (5.000.000) de FCFA.

Art. 93 : Ceux qui, sciemment, auront, recelé, en tout ou partie, des données informatiques soustraites, détournées ou obtenues à l'aide d'un crime ou d'un délit, seront punis d'un an à dix ans d'emprisonnement et d'une amende de cent mille deux (100.002) à deux millions (2 000 000) de FCFA sans préjudice des peines plus fortes.

Art. 94 : Quiconque extorque ou tente d'extorquer des données informatiques, est puni d'un emprisonnement de six (6) mois à cinq (5) ans et d'une amende de cent mille (100.000) à cinq (5.000.000) millions de FCFA.

Est passible de la même peine quiconque extorque ou tente d'extorquer des fonds, choses mobilières ou valeurs patrimoniales par le biais des Technologies de l'Information et de la Communication.

Art. 95 : L'application des dispositions des articles 93 et 94 de la présente loi ne fait pas obstacle à la prise en compte des circonstances aggravantes découlant de l'utilisation des Technologies de l'Information et de la Communication prévues aux articles 84 à 89 de la présente loi.

SECTION IX : DES INFRACTIONS COMMISES PAR TOUT MOYEN DE DIFFUSION PUBLIQUE

Art. 96 : Sont considérés comme moyens de diffusion publique : la radiodiffusion, la télévision, le cinéma, la presse en ligne, l'affichage, l'exposition, la distribution d'écrits ou d'images de toutes natures (sms, e-mail etc.), l'internet, les réseaux sociaux, les discours, chants, cris ou menaces proférés dans les lieux ou réunions publics ou tout autre procédé technique destiné à atteindre le public et généralement tout moyen de communication numérique par voie électronique.

Art. 97 : Est puni d'un emprisonnement de six (6) mois à cinq (5) ans et d'une amende de cinq cent mille (500.000) à dix millions (10.000.000) de FCFA ou de l'une de ces deux peines seulement, quiconque, par le biais des Technologies de l'Information et de la Communication, utilise tout imprimé, tout écrit, dessin, toute affiche, toute gravure, toute peinture, toute photographie, tout film ou cliché, toute matrice ou toute reproduction photographique, tout emblème, tout objet ou toute image, par les moyens de discours, cris ou menaces proférés, contraire aux bonnes mœurs notamment en les :

- fabriquant ou détenant sous un format électronique en vue d'en faire commerce, distribution, location, affichage ou exposition ;
- important ou faisant importer, exportant ou faisant exporter, transportant ou faisant transporter, diffusant sciemment aux mêmes fins ;
- affichant, exposant, projetant ou rendant accessible au regard du public ;
- vendant, louant, mettant en vente ou en location, même non publiquement ;
- offrant, même à titre gratuit, même non publiquement sous quelque forme que ce soit, directement ou par moyen détourné ;
- distribuant ou remettant en vue de leur distribution par un moyen quelconque.

Ces mêmes peines s'appliquent en cas de :

- injure ou diffamation commise envers les Corps constitués, les Cours, les Tribunaux, les Forces de Défenses et Sécurités, les Administrations Publiques, les membres du Gouvernement ou de l'Assemblée Parlementaire, les Fonctionnaires et Agents de l'Etat, les dépositaires de l'Autorité Publique, les citoyens chargés d'un service ou d'un mandat public, temporaire ou permanent, les

assesseurs ou les témoins en raison de leurs dépositions ;

- injure commise dans les conditions prévues à l'alinéa précédent, envers une personne ou un groupe de personnes en raison de leur sexe, de leur handicap, de leur origine, de leur appartenance ou non à une ethnie, une nation, une race ou une religion déterminée.

Art. 98 : Lorsque les faits visés à l'article 97 ci-dessus ont un caractère pornographique, le maximum de la peine est prononcé.

Le condamné peut, en outre, faire l'objet, pour une durée ne dépassant pas cinq (5) ans, d'une interdiction d'exercer, directement ou par personne interposée, en droit ou en fait, des fonctions de direction de toute entreprise d'impression, d'édition ou de groupage et de distribution de journaux et de publication périodiques.
Quiconque enfreint l'interdiction visée ci-dessus est puni des peines prévues au présent article.

SECTION X : DES ATTEINTES AU DROIT D'AUTEUR ET AUX DROITS VOISINS

Art. 99 : Quiconque commet délibérément, à une échelle commerciale et au moyen d'un système d'information, une atteinte au droit d'auteur et aux droits voisins définis par les textes en vigueur, à l'exception de tout droit moral conféré par les conventions relatives à la propriété intellectuelle, est puni d'un emprisonnement de six (6) mois à cinq (5) ans et d'une amende de cinq cent mille (500.000) à dix millions (10.000.000) de FCFA.

Art. 100 : Quiconque porte atteinte au droit patrimonial ou au droit moral de l'auteur d'une création informatique, à savoir un programme informatique ou une base de données tels que définis par la loi sur le droit d'auteur et les droits voisins, est puni d'un emprisonnement de six (6) mois à cinq (5) ans et d'une amende de cinq cent mille (500.000) à dix millions (10.000.000) de FCFA.

SECTION XI : DE L'USURPATION D'IDENTITE NUMERIQUE

Art. 101 : Quiconque usurpe l'identité numérique d'un tiers ou utilise frauduleusement une ou plusieurs données permettant de l'identifier, en vue de troubler sa tranquillité ou celle d'autrui ou de porter atteinte à son honneur, à sa dignité ou à ses intérêts, est puni d'un

emprisonnement de six (6) mois à cinq (5) ans et d'une amende de cinq cent mille (500.000) à dix millions (10.000.000) de FCFA.

SECTION XII : DU REFUS DE REPONDRE A UNE REQUISITION

Art. 102 : Quiconque, autre que le mis en cause, omet intentionnellement, sans excuse légitime ou justification, de se conformer à une réquisition judiciaire donnée, est puni d'un emprisonnement de six (6) mois à trois (3) ans et d'une amende de cinq cent mille (500.000) à cinq millions (5.000.000) de FCFA.

Art. 103 : Tout fournisseur de service qui, intentionnellement, sans excuse légitime ou justification, divulgue les informations relatives à une enquête criminelle, en violation d'enquête, une injonction stipulant explicitement que la confidentialité doit être maintenue ou qu'elle résulte de la loi, est puni d'un emprisonnement de six (6) mois à trois (3) ans et d'une amende de cinq cent mille (500.000) à cinq millions (5.000.000) de FCFA.

SECTION XIII : DES ATTEINTES A LA DEFENSE ET A LA SECURITE NATIONALE

Art. 104 : Est coupable de trahison et puni des travaux forcés à perpétuité tout centrafricain ou étranger qui :

- livre à une puissance étrangère ou à ses agents, sous quelque forme ou par quelque moyen que ce soit, un renseignement, objet, document, procédé, une donnée numérisée ou un fichier informatisé qui doit être tenu secret dans l'intérêt de la Défense et de la Sécurité Nationale ;
- s'assure, par quelque moyen que ce soit, la possession d'un tel renseignement, objet, document, procédé, d'une telle donnée numérisée ou d'un tel fichier informatisé en vue de le livrer à une puissance étrangère ou à ses agents ;
- détruit ou laisse détruire un tel renseignement, objet, document, procédé, une telle donnée numérisée ou un tel fichier informatisé en vue de favoriser une puissance étrangère.
- rassemble les renseignements, objets, documents, procédés, données ou fichiers informatisés dont la réunion et l'exploitation sont de nature à nuire à la Défense et à la Sécurité Nationale avec l'intention de les livrer à tout pays tiers.

- porte atteinte à des Infrastructures critiques de la République Centrafricaine.

Art. 105 : Est puni de la peine de réclusion à temps ou à perpétuité, tout Centrafricain ou étranger qui, sans intention de trahison ou d'espionnage:

- s'assure, étant sans qualité, la possession d'un renseignement, objet, document, procédé, des données ou fichiers informatisés tenus secrets dans l'intérêt de la défense et de la sécurité nationale ou dont la connaissance pourrait conduire à la découverte d'un secret Défense et de la Sécurité Nationale ;
- détruit, soustrait, laisse détruire ou soustraire, reproduit ou laisse reproduire un tel renseignement, objet, document, procédé, une telle donnée ou un tel fichier informatisé ;
- porte ou laisse porter à la connaissance d'une personne non qualifiée ou du public un tel renseignement, objet, document, procédé, de telle donnée ou fichier informatisé, ou en étend la divulgation.

SECTION XIV : DE LA RESPONSABILITE PENALE DES PERSONNE MORALES

Art. 106 : Les personnes morales autres que l'Etat, les Collectivités Locales et les Etablissements Publics sont pénalement responsables des infractions prévues par la présente loi, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé sur:

- un pouvoir de représentation de la personne morale ;
- une autorité pour prendre des décisions au nom de la personne morale;
- une autorité pour exercer un contrôle au sein de la personne morale.

Art. 107 : Les personnes morales visées à l'article 105 ci-dessus peuvent être tenues pour responsables lorsque l'absence de surveillance ou de contrôle de la part de leurs organes ou représentants a rendu possible la commission des infractions établies en application de la présente Loi pour le compte de ladite personne morale par une personne physique agissant sous leur autorité.

Art. 108 : La responsabilité des personnes morales définie aux articles 105 et 106 de la présente loi n'exclut pas celle des personnes physiques, auteurs, coauteurs ou complices des mêmes faits.

Art. 109 : Peuvent être prononcées contre les personnes morales, les peines suivantes :

- l'amende égale au quintuple de celle prévue pour les personnes physiques par la loi qui réprime l'infraction ;
- la dissolution, lorsque la personne morale a été créée ou détournée de son objet pour commettre les faits incriminés ;
- l'interdiction définitive ou temporaire ne pouvant dépasser une durée de cinq (5) ans, d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ;
- la fermeture définitive ou temporaire ne pouvant dépasser une durée de cinq (5) ans, d'un ou plusieurs des Etablissements 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 plus ;
- l'interdiction à titre définitif ou pour une durée de cinq (5) ans au plus de faire appel public à l'épargne ;
- l'interdiction pour une durée de cinq (5) ans au plus d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés, ou d'utiliser des cartes de paiement ;
- la confiscation de la chose ayant servi ou destinée à commettre l'infraction ou qui en est le produit ;
- l'affichage de la décision prononcée ou la diffusion de celle-ci soit par la presse écrite soit par tout moyen de communication au public par voie électronique.

SECTION XV : DE L'ADAPTATION DE CERTAINES SANCTIONS LIEES A L'UTILISATION DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Art. 110 : En cas de condamnation pour une infraction commise par le biais des Technologies de l'Information et de la Communication, la juridiction peut prononcer, à titre de peines complémentaires, l'interdiction à titre provisoire ou définitif d'émettre des messages de communication numérique, de l'accès au site ayant servi à commettre l'infraction, ou l'injonction d'en couper l'accès par tout moyen technique disponible

ou même en interdire l'hébergement.

Le juge peut également faire injonction à toute personne légalement responsable du site ayant servi à commettre l'infraction ou à toute personne qualifiée de mettre en œuvre les moyens techniques de nature à garantir l'interdiction d'accès, d'hébergement ou la coupure de l'accès au site incriminé.

La violation des interdictions ci-dessus, est punie d'un emprisonnement de un (1) à cinq (5) ans et d'une amende de deux millions (2.000.000) à dix millions (10.000.000) de FCFA.

Art. 111 : En cas de condamnation pour une infraction commise par le biais des Technologies de l'Information et de la Communication, le juge peut, à titre complémentaire, ordonner la diffusion aux frais du condamné, de l'extrait de la décision sur ce même support.

Lorsqu'elle est ordonnée, la publication est exécutée dans les quinze (15) jours suivant celui où la condamnation est devenue définitive, sous peine d'un emprisonnement d'un (1) mois à cinq (5) ans au plus et d'une amende de deux millions (2.000.000) à dix millions (10.000.000) de FCFA.

Art. 112 : Le juge peut ordonner la suppression de tout ou partie des données à caractère personnel faisant l'objet du traitement ayant donné lieu à l'infraction.

Art. 113 : Sans préjudice de l'application des dispositions des articles 82 à 88 de la présente loi, peuvent être prononcées, pour les infractions liées à la cryptologie, les peines complémentaires suivantes :

- la confiscation des outils ayant servi à commettre l'infraction ou qui en sont le produit ;
- l'interdiction d'exercer une fonction publique élective ou une activité professionnelle liée à la cryptologie pour une durée de cinq (5) ans au plus ;
- la fermeture de l'entreprise ayant servi à commettre les faits incriminés pour une durée de cinq (5) ans ;
- l'exclusion pour une durée de cinq (5) ans de l'entreprise des marchés publics.

Les peines complémentaires s'appliquent à toute personne physique ou morale coupable de l'une des infractions liées à la cryptologie.

TITRE IV : DE LA PROCEDURE ET DES MOYENS DE PREUVES

CHAPITRE I : DE LA PROCEDURE

Art. 114 : En cas d'infraction au sens de la présente Loi, les Officiers de Police Judiciaire à compétence générale le cas échéant assistés par les agents habilités de l'ANCy, procèdent aux enquêtes conformément aux dispositions du Code de Procédure Pénale.

Avant leur entrée en fonction, les Officiers de Police Judiciaires de l'ANCy prêtent serment, devant le Tribunal de Grande Instance compétent, en ces termes : « **Je jure de remplir loyalement mes fonctions et d'observer en tous les devoirs qu'elles m'imposent, de garder secrètes les informations dont j'ai eu connaissance à l'occasion ou dans l'exercice de mes fonctions**».

Les Officiers de Police Judiciaire et les agents habilités de l'ANCy peuvent, lors des investigations, accéder aux moyens de transport, à tout local en vue de rechercher, constater les infractions, demander la communication de tous les documents et en prendre copie, recueillir, sur convocation ou sur place, les renseignements et justifications.

Art. 115 : Les perquisitions en matière de cybercriminalité sont susceptibles de porter sur des données qui peuvent être des supports physiques ou des copies réalisées en présence des personnes qui assistent à la perquisition.

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.

Sur accord du Procureur de la République, seuls sont gardés sous scellé par l'Officier de Police Judiciaire, les objets, documents et données utilisés pour la manifestation de la vérité.

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

Tout opérateur, exploitant des réseaux de Communications Electroniques ou Systèmes d'Informations, personne physique ou morale surpris en flagrant délit d'infractions de cybercriminalité est traduit directement devant les juridictions compétentes.

Art. 116 : Les perquisitions et les saisies sont effectuées conformément aux dispositions du Code de Procédure Pénale en tenant compte du dépérissement des preuves.

Art. 117 : 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 compétente peuvent réquisitionner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair desdites données.

Lorsqu'un moyen de cryptographie est utilisé, les Autorités Judiciaires peuvent exiger la convention secrète de déchiffrement du cryptogramme.

Art. 118 : La réquisition prévue à l'article 41 ci-dessus peut être faite à tout expert.

Dans ce cas, son exécution est faite conformément aux dispositions du Code de Procédure Pénale relatives à la commission d'experts.

Art. 119 : Les Autorités Judiciaires 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 centrafricain ou dont l'un des auteurs, coauteurs ou complices se trouve sur ledit territoire.

Sous réserve des règles de réciprocité entre la République Centrafricaine et les autres Etats liés par un accord de coopération judiciaire, les commissions rogatoires sont exécutées conformément à la Convention des Nations Unies sur la criminalité transfrontalière, aux différentes conventions régionales, sous régionales et aux dispositions du Code de Procédure Pénale.

Art. 120 : Dans le cadre des investigations 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'ANCy, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies.

Les Officiers de Police Judiciaire et agents habilités de l'ANCy peuvent demander aux fournisseurs des prestations visées à l'alinéa 1 ci-dessus de mettre eux-mêmes en œuvre ces conventions, sauf si ceux-ci démontrent qu'ils ne sont pas en mesure de satisfaire à de telles réquisitions.

Art. 121 : 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 Electroniques garantissant la confidentialité de la transmission.

Il est dressé, dans chacun des lieux, un Procès-verbal des auditions qui y ont été effectuées. Celle-ci peut faire l'objet d'enregistrement audiovisuel et/ou sonore.

Lorsque les circonstances l'exigent, l'interprétation est faite au cours d'une audition, d'un interrogatoire ou d'une confrontation par des moyens de Communications Electroniques.

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 ou de coopération émanant des Autorités Judiciaires étrangères ou des actes d'entraide réalisés à l'étranger sur demande des Autorités Judiciaires.

SECTION I : DE LA PERQUISITION ET SAISIE MATERIEL OU DONNEES INFORMATIQUES

Art. 122 : Le Procureur de la République ou le Juge d'instruction peut ordonner une perquisition ou accéder à un Système d'Information ou à une partie de celui-ci ou dans un autre Système d'Information, lorsque des données stockées dans un Système d'Information ou dans un support permettant de conserver des données informatisées sur le territoire centrafricain sont utiles à la manifestation de la vérité, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.

S'il est préalablement établi que ces données, accessibles à partir du système initial ou disponible, sont stockées dans un autre Système d'Information situé en dehors du territoire national, elles sont recueillies par le Procureur de la République ou le Juge d'instruction, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur.

Art. 123 : Lorsque le Procureur de la République ou le juge d'instruction découvre dans un système d'information des données stockées utiles pour la manifestation de la vérité, et que la saisie du support ne paraît pas souhaitable, ces données, de même que celles qui sont nécessaires pour les comprendre, sont copiées sur des supports de stockage informatique pouvant être saisis et placés sous scellés.

Le Procureur de la République ou le Juge d'instruction désigne toute

personne qualifiée pour utiliser les moyens techniques appropriés afin d'empêcher l'accès aux données visées à l'article 21 de la présente loi dans le système d'information ou aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système d'information et de garantir leur intégrité.

Lorsque, pour des raisons techniques ou en raison du volume des données, la mesure prévue à l'alinéa 2 du présent article ne peut être prise, le Procureur de la République ou le Juge d'instruction utilise les moyens techniques appropriés pour empêcher l'accès à ces données dans le Système d'Information, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le Système d'Information et de même que pour garantir leur intégrité.

Art. 124 : 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'y accéder en clair ou sont de nature à compromettre les informations qu'elles contiennent, le Procureur de la République ou le Juge d'instruction peut réquisitionner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair desdites données.

Lorsqu'un moyen de cryptographie a été utilisé, les Autorités Judiciaires peuvent exiger la convention secrète de déchiffrement du cryptogramme.

Art. 125 : Lorsque les données liées à l'infraction, sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des Systèmes d'Informations ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, le Procureur de la République ou le Juge d'instruction ordonne les mesures conservatoires nécessaires, notamment en désignant toute personne qualifiée avec pour mission d'utiliser tous les moyens techniques appropriés pour rendre ces données inaccessibles.

Art. 126 : Le Procureur de la République informe le responsable du Système d'Information de la recherche effectuée dans le Système d'Information et lui communique une copie des données qui ont été copiées, rendues inaccessibles ou retirées.

Art. 127 : Le Juge compétent peut à tout moment, d'office ou sur la demande de l'intéressé, ordonner la main levée de la saisie.

Art. 128 : l'Officier de Police Judiciaire peut, pour nécessité d'enquête en exécution d'une délégation judiciaire, procéder aux opérations prévues aux articles 123 et 124 de la présente loi.

SECTION II : DE L'INJONCTION DE PRODUIRE

Art. 129 : Lorsque les nécessités de l'enquête l'exigent, le Procureur de la République ou le Juge d'instruction peut faire injonction à toute personne présente sur le territoire centrafricain de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un Système d'Information ou un support de stockage informatique.

L'injonction de produire peut être adressée, dans les mêmes conditions susmentionnées, à un fournisseur de services offrant des prestations en République Centrafricaine, en vue de communiquer les données, en sa possession ou sous son contrôle, relatives aux abonnés et concernant de tels services.

CHAPITRE II : DES MOYENS DE PREUVES EN MATIERE D'INFRACTIONS COMMISES PAR LE BIAIS DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

SECTION I : DE LA PREUVE ELECTRONIQUE EN MATIERE PENALE

Art.130 : L'écrit électronique en matière pénale est admis pour établir les infractions à la Loi pénale pour autant que cet élément de preuve soit rapporté au cours des débats et discuté devant le juge et que la personne dont il émane puisse être dûment identifiée les conditions dans lesquelles il a été conservé soient établies et documentées de sorte à en garantir l'intégrité.

SECTION II : DE L'INTERCEPTION DE DONNEES INFORMATISEES RELATIVES AU CONTENU

Art.131 : Si les nécessités de l'enquête l'exigent, le Procureur de la République ou le Juge d'instruction peut utiliser les moyens techniques appropriés pour collecter ou enregistrer en temps réel, les données relatives au contenu de communications spécifiques, transmises au moyen d'un Système d'Information ou obliger un fournisseur de services, dans le cadre de ses capacités techniques, à collecter ou à enregistrer lesdites données informatisées, en application de moyens techniques existants, ou à prêter aux Autorités Compétentes son concours et son assistance pour collecter ou enregistrer ces données.

Art.132 : L'écrit électronique en matière pénale est admis pour établir les infractions à la Loi pénale pour autant que cet élément de preuve soit rapporté au cours des débats et discuté devant le juge et que la personne dont il émane puisse être dûment identifiée les conditions dans lesquelles il a été conservé soient établies et documentées de sorte à en garantir l'intégrité.

SECTION III : DE LA CONSERVATION RAPIDE DES DONNEES INFORMATIQUES STOCKEES

Art.133 : Lorsque les nécessités de l'enquête l'exigent, le Procureur de la République ou le Juge d'instruction peut faire injonction à toute personne de conserver et de protéger l'intégrité des données en sa possession ou sous son contrôle, pendant une durée de cinq (5) ans maximum.

Toute personne chargée de conserver les données, est tenue de garder le secret sur la mise en œuvre desdites procédures ainsi que sur les données personnelles concernées, sous peine des sanctions pénales encourues en matière de violation du secret professionnel.

SECTION IV : DE LA COLLECTE EN TEMPS REEL DES DONNEES RELATIVES AU TRAFIC

Art.134 : Lorsque les nécessités de l'enquête l'exigent, le Procureur de la République ou le Juge d'instruction peut utiliser les moyens techniques appropriés pour collecter ou enregistrer, en temps réel, les données relatives au trafic associées à des communications spécifiques, transmises au moyen d'un Système d'Information.

Le Procureur de la République ou le Juge d'instruction peut également obliger un fournisseur de services à collecter ou à enregistrer, en application des moyens techniques existants, ou à prêter aux Autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données visées à l'alinéa premier du présent article.

Art.135 : Le fournisseur de service désigné à l'alinéa 2 de l'article 134 ci-dessus est tenu de garder le secret sur les informations reçues.

Toute violation du secret professionnel est punie, conformément aux dispositions du Code Pénal.

SECTION V : DE L'UTILISATION DE LOGICIELS A DISTANCE

Art.136 : Lorsque les nécessités de l'enquête l'exigent, le Juge compétent peut, sur réquisition du parquet, autoriser l'Officier de Police Judicaire, ou les agents habilités de l'ANCY d'utiliser un logiciel d'accès à distance et à l'installer dans le Système d'Information du mis en cause afin de recueillir les éléments de preuve pertinents.

Cette demande contient les informations suivantes :

- nom prénom et adresse ;
- description du Système d'Information ciblé ;
- description de la mesure envisagée ;
- étendue et durée de l'utilisation ;
- raison de la nécessité de l'utilisation du logiciel.

Art.137 : Seuls peuvent être utilisés des programmes informatiques spéciaux qui génèrent un procès-verbal complet et inaltérable de la surveillance. Le procès-verbal est joint au dossier de la procédure.

Le transfert des données du système informatique surveillé à l'autorité de poursuite pénale compétente est sécurisé.

Les agents habilités de l'ANCY s'assurent que le code source peut être contrôlé, dans le but de vérifier que le programme ne contient que des fonctions admises par la loi.

TITRE V : DE LA COOPERATION ET DE L'ENTRAIDE JUDICIAIRE INTERNATIONALE

CHAPITRE I : DE LA COOPERATION INTERNATIONALE

Art.138 : Les modalités d'établissement des conventions de coopération en matière de cybersécurité et de lutte contre la cybercriminalité sont déterminées par voie réglementaire.

CHAPITRE II : DE L'ENTRAIDE JUDICIAIRE

Art.139 : La demande d'entraide judiciaire en matière d'infraction commise par voie de Technologies de l'Information et de la Communication, sont émises et exécutées conformément aux dispositions du Code de Procédure Pénale.

TITRE VI : DES DISPOSITIONS DIVERSES, TRANSITOIRES ET FINALES

Art.140 : La présente Loi complète les dispositions de la Loi 18.002 du 17 janvier 2018, régissant les Communications Electroniques en République Centrafricaine, complète les dispositions du Code Pénal et les autres textes législatifs et réglementaires en vigueur en République Centrafricaine.

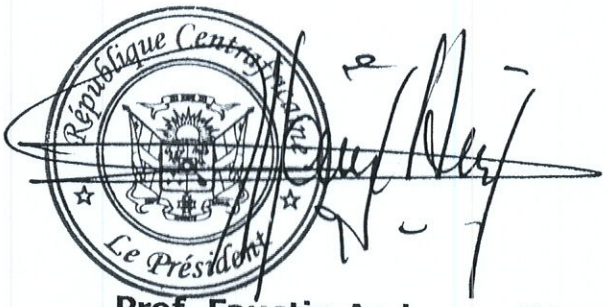
Art.141 : Les Ministères chargés de la Sécurité Publique et de l'Economie Numérique assurent les missions de l'ANCy en attendant la mise en place de ses organes.

Art.142 : Le Gouvernement, en collaboration avec toutes les parties prenantes et par le biais des Ministères chargés de l'Economie Numérique et de la Sécurité Publique, définit la politique nationale en matière de cybersécurité et de lutte contre la cybercriminalité.

Art.143 : Des textes règlementaires fixent, en tant que de besoin, les modalités d'application de la présente loi.

Art.144 : La présente loi qui prend effet à compter de la date de sa promulgation, est enregistrée et publiée au Journal Officiel.

Fait à Bangui, le 21 FEV 2024



Prof. Faustin Archange TOUADERA