

RÉPUBLIQUE DE CÔTE D'IVOIRE

Union – Discipline – Travail

LOI N° 2013-451 DU 19 JUIN 2013 RELATIVE À LA LUTTE CONTRE LA CYBERCRIMINALITÉ

Sommaire :

Avant-propos ..... **I**

CHAPITRE 1 : ***Définitions*** **1**

Article premier **1**

CHAPITRE 2 : ***Objet et champ d'application*** **3**

Article 2 ..... **3**

Article 3 ..... **3**

CHAPITRE 3 : ***Infractions spécifiques aux technologies de l'information et de la communication*** **3**

Article 4 ..... **3**

Article 5 ..... **3**

Article 6 ..... **3**

Article 7 ..... **4**

Article 8 ..... **4**

Article 9 ..... **4**

Article 10 ..... **4**

Article 11 ..... **4**

Article 12 ..... **4**

Article 13 ..... **4**

Article 14 ..... **5**

Article 15 ..... **5**

Article 16 ..... **5**

Article 17 ..... **5**

Article 18 ..... **5**

Article 19 ..... **5**

Article 20 ..... **6**

Article 21 ..... **6**

Article 22 ..... **6**

Article 23 ..... **6**

Article 24 ..... **6**

Article 25 ..... **6**

Article 26 ..... **7**

Article 27 ..... **7**

Article 28 ..... **7**

Article 29 ..... **8**

Article 30 ..... **8**

Article 31 ..... **8**

Article 32 ..... **8**

CHAPITRE 4 : ***Atteintes à la propriété intellectuelle*** **9**

Article 33 ..... **9**

Article 34 ..... **9**

Article 35 ..... **10**

Article 36 ..... **11**

CHAPITRE 5 : ***Agissements illicites sur les réseaux de communication électronique*** **11**

Article 37 ..... **11**

Article 38 ..... **11**

Article 39 ..... **11**

Article 40 ..... **11**

Article 41 ..... **12**

CHAPITRE 6 : ***Responsabilité des prestataires techniques de service en ligne*** **12**

Article 42 12

Article 43 12

Article 44 12

Article 45 12

Article 46 13

Article 47 13

Article 48 13

Article 49 14

Article 50 14

Article 51 14

Article 52 14

Article 53 14

Article 54 15

Article 55 15

Article 56 15

Article 57 16

CHAPITRE 7 : ***Adaptation des infractions classiques aux technologies de l'information et de la communication*** **..... 16**

Article 58 16

Article 59 16

Article 60 17

Article 61 17

Article 62 17

Article 63 17

Article 64 17

Article 65 ..... **17**

Article 66 ..... **18**

Article 67 ..... **18**

Article 68 ..... **18**

Article 69 ..... **18**

Article 70 ..... **19**

CHAPITRE 8 : ***Procédure pénale en matière de cybercriminalité*** **19**

Article 71 ..... **19**

Article 72 ..... **19**

Article 73 ..... **19**

Article 74 ..... **19**

Article 75 ..... **20**

Article 76 ..... **20**

Article 77 ..... **20**

Article 78 ..... **21**

Article 79 ..... **21**

Avant-propos

À l'ère de la digitalisation accélérée, la Côte d'Ivoire, comme de nombreux pays, fait face à une hausse préoccupante des cybermenaces. Entre les fraudes en ligne, le piratage de données, les cyberescroqueries, les atteintes à la vie privée et la diffusion de fausses informations, les risques liés à la cybercriminalité pèsent sur la sécurité nationale, la stabilité économique et la confiance des citoyens dans le numérique.

Consciente de ces enjeux, la Côte d'Ivoire a renforcé son cadre juridique avec la **loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité (modifiée en ses articles 17, 33, 58, 60, 62, et 66 par la loi n° 2023-593 du 07 juin 2023)**.

Cette loi crée un cadre juridique solide pour encadrer et réprimer la cybercriminalité en Côte d'Ivoire. Elle couvre un large éventail d'infractions, responsabilise acteurs publics et privés, intègre des progrès techniques et judiciaires, et évolue pour rester dissuasive face aux nouvelles menaces numériques.

Mais le bémol, c'est que la loi ivoirienne relative à la lutte contre la cybercriminalité n'est pas assez vulgarisée, et donc, cette loi est encore peu connue, sinon méconnue de la plupart des citoyens, de bon nombre d'entrepreneurs dans le domaine du numérique, et même de certains professionnels ou futurs professionnels du Droit.

Or, une loi n'a de valeur que si elle est bien connue par ceux qu'elle protège. Il est essentiel que les citoyens connaissent leurs droits et leurs devoirs dans l'écosystème du numérique en Côte d'Ivoire.

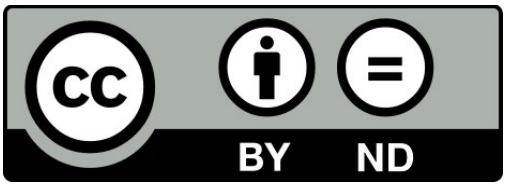
C'est donc pour contribuer à une meilleure vulgarisation de la loi ivoirienne relative à la lutte contre la cybercriminalité, que Jay Snyper Digital SARL vous propose cette copie propre, claire et bien structurée de cette loi fondamentale pour la confiance numérique en Côte d'ivoire.

En effet, la **loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité** définit les infractions spécifiques aux communications électroniques, notamment les atteintes aux systèmes informatiques, et les atteintes aux systèmes de traitement automatisé de données. Elle traite les agissements illicites sur les réseaux de communications électroniques concernant notamment :

- les accès illégaux (piratage de systèmes informatiques) ;
- les atteintes aux systèmes (virus, déni de service, altérations des données, etc.)
- le vol de données personnelles ;
- l'usurpation d'identité ;
- les atteintes à la vie privée ;
- les fraudes en ligne (arnaques financières, phishing, etc.) ;
- les atteintes à la propriété intellectuelle ;
- la diffusion de contenus illicites (pédopornographie, injures, outrages, désinformation, incitation à la haine, troubles à l'ordre public, etc.).

Avec la certitude que cette copie propre, claire et bien structurée de **loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité** vous soit fort utile, **Jay Snyper Digital SARL** vous souhaite une bonne lecture !

Ce document est diffusé sous la licence **Creative Commons 4.0 BY-ND** (Paternité - Pas de Modification)



Cette licence autorise la diffusion et la reproduction de ce document, à condition qu'il ne soit pas modifié sans l'autorisation préalable de l'auteur.

Jay Snyper Digital SARL

JAY SNYPER DIGITAL

Votre Référent Digital !

Jay Snyper Digital SARL est une société de services en ingénierie informatique (SSII), experte en solutions de transformation digitale.

Jay Snyper Digital SARL a pour mission d'aider les artisans, les commerçant·e·s, les professions libérales, les entreprises et les organismes des secteurs publics ou privés à atteindre leurs objectifs stratégiques, en leur fournissant les meilleures solutions numériques pour booster leurs performances.

Grâce à la diversité de son équipe composée de professionnels issus d'horizons complémentaires (Consultants en transformation digitale, Développeurs Web, Web designers, Web marketeurs, Infographistes, etc.), **Jay Snyper Digital SARL** vous accompagne de A à Z dans tous les domaines qui utilisent des ressources informatiques ou qui appliquent les Technologies de l'Information et de la Communication (TIC).

Nos services :

- **Transformation digitale et intégration de solutions numériques pour entreprises** ;
- **Création de sites Web** ;
- **Création d'applications mobiles** ;
- **Design et intégration de maquettes de sites Web ou d'applications mobiles** ;
- **Sécurité, protection et maintenance de sites WordPress** ;
- **Référencement SEO** ;
- **Stratégie digitale et marketing numérique** ;
- **Infographie et production audiovisuelle** ;
- **Vente, installation et maintenance de matériels informatiques**.

Plus d'informations à l'adresse : ***www.jaysnyper.com/services/***

Jay Snyper Digital SARL est une société par actions simplifiées au capital social de 1 000 000 F CFA, immatriculée au Registre du Commerce et du Crédit Mobilier du tribunal de commerce d'Abidjan (Côte d'Ivoire) sous le numéro **CI-ABJ-03-2022-B13-06372**.

RÉPUBLIQUE DE CÔTE D'IVOIRE

Union – Discipline – Travail

LA LOI N° 2013-451 DU 19 JUIN 2013 (MODIFIÉE EN SES ARTICLES 17, 33, 58, 60, 62, ET 66 PAR LA LOI N° 2023-593 DU 07 JUIN 2023) RELATIVE À LA LUTTE CONTRE LA CYBERCRIMINALITÉ

L'ASSEMBLÉE NATIONALE a adopté, le PRÉSIDENT DE LA RÉPUBLIQUE promulgue la loi dont la teneur suit :

CHAPITRE 1 :

Définitions

Article premier :

— Les définitions des instruments juridiques de la CEDEAO, de l'Union africaine ou de l'Union Internationale des Télécommunications prévalent pour les termes non définis par la présente loi.

Au sens de la présente loi, on entend par :

- ***cybercriminalité***, l'ensemble des infractions pénales qui se commettent au moyen ou sur un réseau de télécommunication ou un système d'information ;

- ***atteinte à la dignité humaine***, toute atteinte, hors les cas d'attentat à la vie, d'atteinte à l'intégrité ou à la liberté, qui a pour effet essentiel de traiter la personne comme une chose, comme un animal ou comme un être auquel serait dénié tout droit ;

- ***communication électronique***, toute émission, transmission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de vidéos par voie électromagnétique, optique ou par tout autre moyen ;

- ***données à caractère personnel***, toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique ;

- ***données informatiques ou données***, 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 exécuter une fonction par un système d'information ;

- ***données relatives 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 sur la base d'un contrat ou d'un arrangement de services :

  - le type de service de communication, les dispositions techniques prises à cet égard et la période de service ;

  - l'identité, l'adresse postale ou géographique, le numéro de téléphone et tout autre numéro d'accès, les informations relatives à la localisation, la facturation et à l'endroit où se trouvent les équipements de communication.

- ***données relatives 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 ;

- ***données sensibles***, toutes données à caractère personnel relatives aux opinions ou activités religieuse, philosophique, politique, syndicale, à la vie sexuelle ou raciale, à la santé, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives ;

- ***infrastructures critiques***, les installations physiques et des technologies de l'information, les réseaux, les services et les actifs qui, en cas d'arrêt ou de destruction, peuvent avoir de graves incidences sur la santé, la sécurité ou le bien-être économique et social des citoyens ou encore le fonctionnement continu des services de l'État ;

- ***mineur***, toute personne figée de moins de dix-huit (18) ans, conformément au Code pénal ;

- ***pays tiers***, tout État non membre de la CEDEAO ;

- ***personne concernée***, toute personne physique qui fait l'objet d'un traitement de données à caractère personnel ;

- ***pornographie infantile***, toute donnée quelle qu'en soit la nature ou la forme représentant de manière visuelle un enfant de moins de dix-huit (18) ans se livrant à un agissement sexuellement explicite ou des images représentant un enfant de moins de quinze (15) ans se livrant à un comportement sexuellement explicite ;

- ***racisme et xénophobie en matière des TIC***, 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 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 à l'autre de ces éléments ou qui incite à de tels actes ;

- ***SMS***, le sigle anglo-saxon signifiant « short message service » (en français : service de message court) ;

- ***surveillance***, toute activité faisant appel à des moyens techniques ou électroniques en vue de détecter, d'observer, de copier ou d'enregistrer les mouvements, images, paroles, écrits, ou l'état d'un objet ou d'une personne fixe ou mobile ;

- ***système d'information ou système informatique***, tout dispositif isolé ou non, tout ensemble de dispositifs interconnectés assurant en tout ou partie, un traitement automatisé de données en exécution d'un programme.

CHAPITRE 2 :

Objet et champ d'application

Article 2 :

— La présente loi a pour objet de lutter contre la cybercriminalité.

Article 3 :

— Sont soumis aux dispositions de la présente loi, les infractions relatives à la cybercriminalité, ainsi que les infractions pénales dont la constatation requiert la collecte d'une preuve électronique.

CHAPITRE 3 :

Infractions spécifiques aux technologies de l'information et de la communication

Article 4 :

— Est puni de un (1) à deux (2) ans d'emprisonnement et de 5 000 000 à 10 000 000 de francs CFA d'amende, quiconque accède ou tente d'accéder frauduleusement à tout ou partie d'un système d'information.

Article 5 :

— Est puni de un (1) à deux (2) ans d'emprisonnement et de 5 000 000 à 10 000 000 de francs CFA d'amende, quiconque se maintient ou tente de se maintenir frauduleusement dans tout ou partie d'un système d'information.

Article 6 :

— Est puni de un (1) à cinq (5) ans d'emprisonnement et de 10 000 000 à 40 000 000 de francs CFA d'amende, quiconque entrave, fausse ou tente d'entraver ou de fausser frauduleusement le fonctionnement d'un système d'information.

Article 7 :

— Est puni de un (1) à cinq (5) ans d'emprisonnement et de 10 000 000 à 40 000 000 de francs CFA d'amende, quiconque introduit ou tente d'introduire frauduleusement des données dans un système d'information.

Article 8 :

— Est puni de cinq (5) à dix (10) ans d'emprisonnement et de 40 000 000 à 60 000 000 de francs CFA d'amende, quiconque intercepte ou tente d'intercepter frauduleusement par des moyens techniques des données informatiques lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système d'information.

Article 9 :

— Est puni de cinq (5) à dix (10) ans d'emprisonnement et de 40 000 000 à 60 000 000 de francs CFA d'amende, quiconque altère ou tente d'altérer, modifie ou tente de modifier, supprime ou tente de supprimer frauduleusement des données informatiques.

Article 10 :

— Est puni de cinq (5) à dix (10) ans d'emprisonnement et de 40 000 000 à 60 000 000 de francs CFA d'amende, quiconque produit ou fabrique un ensemble de données par l'introduction, la modification, l'altération ou la suppression frauduleuse de données informatiques, engendrant des données contrefaites, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient originales.

Article 11 :

— Est puni de un (1) à cinq (5) ans d'emprisonnement et de 20 000 000 à 40 000 000 de francs CFA d'amende, quiconque fait usage, en connaissance de cause, de données informatiques frauduleusement obtenues.

Article 12 :

— Est puni de un (1) à cinq (5) ans d'emprisonnement et de 30 000 000 à 50 000 000 de francs CFA d'amende, quiconque obtient frauduleusement, pour soi-même ou pour autrui, un avantage quelconque, par l'introduction, l'utilisation, la modification, l'altération ou la suppression de données informatiques ou par toute forme d'atteinte au système d'information.

Article 13 :

— Est puni de un (1) an à deux (2) ans d'emprisonnement et de 10 000 000 à 50 000 000 de francs CFA d'amende, quiconque, dans l'intention de commettre l'une des infractions prévues par la présente loi produit, vend, importe, détient, diffuse, offre, cède ou met à disposition, en connaissance de cause :

- un équipement, un dispositif ou un programme informatique ;

- un mot de passe, un code d'accès ou des données informatiques similaires.

Article 14 :

— Est puni de dix (10) à vingt (20) ans d'emprisonnement et de 75 000 000 à 100 000 000 de francs CFA d'amende, quiconque participe à une association formée ou à une entente établie en vue de préparer ou de commettre une ou plusieurs des infractions prévues dans la présente loi.

L'infraction ci-dessus définie est un délit.

Article 15 :

— Est puni de deux (2) à cinq (5) ans d'emprisonnement et de 75 000 000 à 100 000 000 de francs CFA d'amende, quiconque produit, enregistre, offre, met à disposition, diffuse, transmet une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système d'information ou d'un moyen de stockage de données informatiques.

Article 16 :

— Est puni de deux (2) à cinq (5) ans d'emprisonnement et de 75 000 000 à 100 000 000 de francs CFA d'amende, quiconque se procure ou procure à autrui, importe ou fait importer, exporte ou fait exporter une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système d'information ou d'un moyen de stockage de données informatiques.

Article 17 :

— Est puni de un (1) à six (6) ans d'emprisonnement et de 20 000 000 à 40 000 000 de francs CFA d'amende, quiconque possède intentionnellement une image ou une représentation présentant un caractère de pornographie infantile dans un système d'information ou dans un moyen de stockage de données informatiques.

Article 18 :

— Est puni de un (1) à cinq (5) ans d'emprisonnement et de 20 000 000 à 40 000 000 de francs CFA d'amende, quiconque facilite l'accès à des images, des documents, du son ou une représentation présentant un caractère de pornographie à un mineur.

Article 19 :

— Est puni de deux (2) à cinq (5) ans d'emprisonnement et de 5 000 000 à 10 000 000 de francs CFA d'amende, quiconque utilise frauduleusement un ou des éléments d'identification d'une personne physique ou morale par le biais d'un système d'information.

Quiconque utilise, possède, offre, vend, met à disposition, transmet en toute connaissance de cause de fausses données d'identification est puni de deux (2) à cinq (5) ans d'emprisonnement et de 5 000 000 à 10 000 000 de francs CFA d'amende.

Quiconque réalise ou tente de réaliser de fausses données d'identification est puni de deux (2) à cinq (5) ans d'emprisonnement et de 5 000 000 à 10 000 000 de francs CFA d'amende.

Article 20 :

— Est puni d'une peine d'emprisonnement de un (1) à cinq (5) ans et d'une amende de 10 000 000 à 100 000 000 de francs CFA, quiconque ne respecte pas l'interdiction d'exercer la profession de prestataire de cryptologie ou l'obligation de retrait des moyens de cryptologie.

Article 21 :

— Est puni d'une peine d'emprisonnement de un (1) à cinq (5) ans et d'une amende de 1 000 000 à 10 000 000 de francs CFA, quiconque procède à la prospection directe à l'aide de tout moyen de communication utilisant, sous quelque forme que ce soit, les données à caractère personnel d'une personne physique qui n'a pas exprimé son consentement préalable par écrit à recevoir de telles prospections.

Article 22 :

— Est puni d'une peine d'emprisonnement de un (1) à cinq (5) ans et d'une amende de 1 000 000 à 10 000 000 de francs CFA, quiconque utilise des procédés illicites d'envoi de messages électroniques non sollicités sur la base de la collecte de données à caractère personnel.

Article 23 :

— Est puni d'une peine d'emprisonnement de un (1) mois à un (1) an et d'une amende de 500 000 à 1 000 000 de francs CFA, quiconque dissimule l'identité de la personne pour le compte de laquelle une offre commerciale est émise ou mentionne une offre sans rapport avec la prestation ou le service proposé.

Article 24 :

— Est puni d'une peine d'emprisonnement de un (1) à cinq (5) ans et de 5 000 000 à 100 000 000 de francs CFA d'amende, quiconque procède au traitement de données à caractère personnel par un moyen frauduleux, déloyal ou illicite.

La peine d'amende ne peut être inférieure à 10 000 000 de francs CFA lorsque le traitement frauduleux, déloyal ou illicite a été faite en vue de l'envoi de messages électroniques non sollicités par une personne morale, autre que l'État.

Article 25 :

— Est puni d'une peine d'emprisonnement de un (1) à cinq (5) ans et d'une amende de 5 000 000 à 100 000 000 de francs CFA, quiconque utilise les éléments d'identification d'une personne physique ou morale dans le but de tromper les destinataires d'un message électronique ou les usagers d'un site Internet en vue de les amener à communiquer des données à caractère personnel ou des informations confidentielles.

La peine d'emprisonnement ne peut être inférieure à cinq (5) ans et la peine d'amende ne peut être inférieure à 20 000 000 de francs CFA, lorsque les données à caractère personnel ou les informations confidentielles communiquées ont servi au détournement de fonds publics ou privés.

Article 26 :

— Quiconque prend frauduleusement connaissance d'une information à l'intérieur d'un système d'information électronique, ou copie frauduleusement une information à partir d'un tel système, ou encore soustrait frauduleusement le support physique sur lequel se trouve une information, est coupable de vol d'information.

Quiconque commet un vol d'information est puni d'une peine d'emprisonnement de cinq (5) à dix (10) ans et de 3 000 000 à 5 000 000 de francs d'amende.

La tentative est punissable.

L'infraction ci-dessus définie est un délit.

Article 27 :

— La peine est d'un emprisonnement de dix (10) à vingt (20) ans et d'une amende de 5 000 000 à 10 000 000 de francs CFA si le vol d'information ou la tentative de vol d'information a été commis accompagné d'une au moins des circonstances ci-après :

- avec des violences ayant entraîné des blessures ;
- avec effraction, escalade ou usage de fausse clé ;
- en réunion par au moins deux personnes ;
- avec usage frauduleux, soit d'un uniforme ou d'un costume d'un fonctionnaire public, civil ou militaire, soit d'un titre d'un fonctionnaire, soit d'un faux ordre d'une autorité civile ou militaire ;
- dans une maison habitée ou servant d'habitation ou dans les locaux professionnels ;
- avec l'usage d'un masque ;
- avec l'usage d'un véhicule pour faciliter son entreprise ou sa fuite ;
- la nuit.

Article 28 :

— Le vol d'information ou la tentative de vol d'information est puni de vingt (20) ans d'emprisonnement et de 10 000 000 de francs CFA d'amende, s'il est accompagné de l'une des circonstances ci-après :

- lorsque l'auteur ou le complice est porteur d'une arme apparente ou cachée ;

- lorsque l'auteur ou le complice a fait usage d'une arme ayant entraîné des blessures ou la mort de la victime.

Article 29 :

— Lorsqu'elle est faite intentionnellement et sans droit, la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission d'un vol d'information, ou l'usage d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système d'information, dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions prévues par la présente loi, est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée d'entre elles.

Article 30 :

— Lorsque les faits punis par la présente loi portent sur un système d'information ou un programme de traitement de données protégé par un code d'accès secret, la peine encourue ne peut être inférieure à dix ans d'emprisonnement.

Article 31 :

— Est puni d'une peine d'emprisonnement de un (1) à cinq (5) ans et de 1 000 000 de francs CFA d'amende, quiconque de mauvaise foi, ouvre, supprime, retarde ou détourne des correspondances électroniques arrivées ou non à destination et adressées à un tiers, ou en prend frauduleusement connaissance.

Est puni des mêmes peines, quiconque de mauvaise foi, intercepte, détourne, utilise ou divulgue des correspondances électroniques émises, transmises ou reçues par la voie des télécommunications ou procède à l'installation d'appareils conçus pour réaliser de telles interceptions.

Article 32 :

— Les personnes condamnées pour les délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

- l'interdiction, pour une durée de cinq ans, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;

- la confiscation du moyen qui a servi à commettre l'infraction ou qui était destiné à la commission de l'infraction ou du bien qui en est le produit ;

- la fermeture, pour une durée de cinq (5) ans s'il y a lieu, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

- l'exclusion, pour une durée de cinq (5) ans, des marchés publics ;

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

- l'affichage ou la diffusion de la décision prononcée, aux frais du condamné.

CHAPITRE 4 :

Atteintes à la propriété intellectuelle

Article 33 :

— Sont punies d'une peine d'emprisonnement de un (1) à vingt (20) ans et d'une amende de 500 000 à 100 000 000 de francs CFA, les atteintes à la propriété intellectuelle commises au moyen d'un système d'information.

Constitue une atteinte à la propriété intellectuelle :

- le fait, sans autorisation de l'auteur ou de ses ayants droit, de reproduire, de représenter ou de mettre à la disposition du public sur un système d'information un support numérique ou analogique, intégralement ou partiellement, une œuvre de l'esprit protégée par le droit d'auteur ou un droit voisin ;

- le fait, sans autorisation de l'auteur ou de ses ayants droit, de traduire ou d'adapter une œuvre de l'esprit par le biais d'un programme informatique ou de mettre cette traduction ou adaptation par un système d'information ou un support numérique ou analogique la disposition du public ;

- le fait, sans autorisation de l'auteur ou de ses ayants droit, de reproduire, d'utiliser, de vendre, de dénaturer, de dénigrer une marque, une raison sociale, un nom commercial, un nom de domaine Internet ou tout autre signe distinctif appartenant à un tiers par le biais d'un système d'information ouvert au public ou par le biais d'un programme informatique ou sur un support numérique ou analogique ;

- le fait, en toute connaissance de cause, d'exploiter par reproduction ou par représentation une œuvre de l'esprit mise de façon illicite à disposition du public sur un réseau de communication électronique ;

- le fait, en toute connaissance de cause, sans droit, de vendre ou de mettre à disposition d'un public par reproduction ou par représentation un bien ou un produit protégé par un brevet d'invention.

Article 34 :

— Ne constituent pas une atteinte à la propriété intellectuelle lorsqu'elles sont réalisées par le biais d'un système ou un programme informatique ou électronique :

- les copies ou reproductions d'œuvres de l'esprit strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective, à l'exclusion des copies des œuvres d'art destinées à être utilisées pour des fins identiques ou similaires à celles pour lesquelles l'œuvre originale a été créée ;

- les analyses et courtes citations, sous réserve que soient clairement indiqués le nom de l'auteur de l'œuvre et de la source, justifiées par le caractère critique, polémique, pédagogique, scientifique ou d'information de l'œuvre à laquelle elles sont incorporées ;

- la parodie et la caricature de l'œuvre originale réalisée sans intention de nuire à l'image et à l'honorabilité de l'auteur de ladite œuvre ;

- les copies ou reproductions provisoires présentant un caractère transitoire et accessoire lorsqu'elles sont une partie intégrante et essentielle d'un procédé technique et qu'elles ont pour objet de permettre la transmission ou l'utilisation licite de l'œuvre sur un système d'information ou électronique ;

- la reproduction et la représentation réalisée à des fins non lucratives par des personnes morales de droit public et par des établissements ouverts au public, tels que les bibliothèques, les services d'archives, les musées, les centres de documentation et les espaces culturels multimédias, en vue d'une consultation strictement personnelle de l'œuvre par des personnes atteintes d'une ou de plusieurs déficiences des fonctions motrices, physiques, sensorielles, mentales, cognitives ou psychiques dont le niveau d'incapacité est reconnu dans un certificat médical dûment établi ;

- la reproduction d'une œuvre, effectuée à des fins de conservation ou destinée à préserver les conditions de sa consultation sur place par des bibliothèques accessibles au public, par des musées ou par des services d'archives, sous réserve que ceux-ci ne recherchent aucun avantage économique ou commercial ;

- la reproduction et la représentation d'œuvre de l'esprit réalisée à des fins exclusivement pédagogiques par les enseignants et les chercheurs dans le cadre strict de leurs enseignements ou de leurs recherches pour leurs élèves et étudiants ou pour d'autres enseignants et chercheurs directement concernés, sous réserve que cette reproduction ou représentation ne donne lieu à aucune exploitation commerciale ou lucrative.

Article 35 :

— L'auteur d'une œuvre de l'esprit ou ses ayants droit peuvent faire obstacle à la copie de l'œuvre en limitant le droit de copie reconnue par la présente loi, notamment, par la mise en œuvre de mesures techniques de protection lorsque la mise en œuvre du droit de copie porte atteinte à l'exploitation normale de l'œuvre ou cause un préjudice injustifié aux intérêts de l'auteur.

On entend par mesure technique de protection, toute technologie, dispositif, composant qui, dans le cadre normal de son fonctionnement, accomplit la fonction de contrôle des utilisations de l'œuvre ou de limitation des copies de l'œuvre considérée. L'usager doit être clairement informé de l'existence des mesures techniques de protection sur l'œuvre qu'il acquiert ou utilise et sur les fonctions de ces mesures techniques, notamment si elles interdisent ou non l'usage de l'œuvre sur d'autres systèmes d'information ou d'exploitation.

Article 36 :

— Le titulaire d'un service d'accès à internet ou à tout réseau de communication électronique est tenu de veiller à ce que cet accès ne soit pas utilisé à des fins manifestement illicites, notamment de reproduction ou de représentation d'œuvres de l'esprit sans l'autorisation de leurs auteurs ou leurs ayants droit. En cas de non-respect de cette obligation, il peut être poursuivi pour complicité par fourniture de moyen.

CHAPITRE 5 :

Agissements illicites sur les réseaux de communication électronique

Article 37 :

— L'organisation des jeux d'argent sur les réseaux de communication électronique est placée sous un régime de droits exclusifs de l'État concédés à un nombre restreint d'opérateurs.

Article 38 :

— Est puni d'une peine d'emprisonnement de un (1) à cinq (5) ans et d'une amende de 5 000 000 à 100 000 000 de francs CFA, quiconque sans autorisation, organise des jeux d'argent illicites en ligne caractérisés par la tenue de jeux de hasard, de loterie illicite, de publicité de loterie prohibée, de prise de paris illicite sur les réseaux de communication électronique.

Article 39 :

— Sont interdits les transferts d'argent par cartes de paiement ou par virement ou par tout autre moyen de paiement effectués par des personnes physiques ou morales dans le cadre de jeux d'argent illicites sur les réseaux de communication électronique.

Les établissements bancaires ou financiers exerçant sur le territoire national veillent au respect de cette interdiction. Ces établissements notifient aux autorités compétentes toute violation constatée ou tentative de violation de cette interdiction.

Article 40 :

— Est puni d'une peine d'emprisonnement de cinq (5) ans et d'une d'amende de 5 000 000 à 10 000 000 de francs CFA, quiconque ne respecte pas l'interdiction de transfert d'argent.

La peine encourue par la personne morale responsable est le double de l'amende prévue pour la personne physique ayant commis l'infraction.

Si le transfert est effectué à destination de l'étranger, l'infraction commise constitue également une infraction à la réglementation régissant les relations financières extérieures et elle est punie sans préjudice des dispositions de la loi relative au contentieux des infractions au contrôle des changes.

Article 41 :

— Les juridictions nationales sont compétentes pour constater ou punir les infractions lorsque les activités de jeux d'argent illicites sont offertes à partir du territoire national ou sont accessibles aux utilisateurs des réseaux de communication électronique à partir du territoire national et qu'il existe un lien suffisant, substantiel ou significatif entre la prestation illicite offerte aux utilisateurs des réseaux de communication en ligne et le territoire national, notamment, par la langue utilisée, la monnaie employée, les produits proposés, le nom de domaine utilisé par le site proposant ladite prestation.

CHAPITRE 6 :

Responsabilité des prestataires techniques de service en ligne

Article 42 :

— L'accès au service internet à partir d'un cybercafé situé sur le territoire national est soumis à l'identification préalable des usagers.

Les exploitants de cybercafé sont tenus de procéder à cette identification suivant les modalités fixées par décret.

Article 43 :

— Le mineur de moins de dix (10) ans ne peut accéder à un cybercafé qu'accompagné d'un adulte.

L'accès à internet dans un cybercafé pour un mineur de moins de dix-huit (18) ans est un accès limité, qui exclut les sites web à caractère pornographique, violent, raciste ou dégradant et de manière générale tous les sites web portant atteinte à la dignité humaine ou incitant à l'incivisme.

Article 44 :

— Les personnes dont l'activité est d'offrir un accès à des services de communication en ligne 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.

Article 45 :

— Est puni d'une peine d'amende de 1 000 000 à 10 000 000 de francs CFA, quiconque ne respecte pas l'obligation d'information et de mise à disposition de moyens techniques de filtrage.

Le fournisseur de services offrant un accès à des services de communication ou assurant à titre gratuit ou onéreux le stockage direct et permanent pour mise à disposition de contenus, est tenu, sur décision du juge compétent, de suspendre immédiatement l'accès auxdits services ou contenus.

Article 46 :

— Les personnes physiques ou morales qui offrent un accès à des services de communication en ligne ou qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent voir leur responsabilité civile ou pénale engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services :

- si elles n'avaient effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ;
- si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible ;
- si le retrait de ces données n'a pas été ordonné par un tribunal.

Article 47 :

— La connaissance des faits litigieux est présumée acquise par les personnes mentionnées à l'article précédent, lorsqu'il leur est notifié par la victime ou par une personne intéressée, les activités illicites ou les faits et circonstances faisant apparaître ce caractère. Pour être prise en compte la notification doit comporter les éléments suivants :

- si l'auteur de la notification est une personne physique : ses nom, prénoms, profession, domicile, nationalité, date et lieu de naissance ;
- si l'auteur de la notification est une personne morale : sa dénomination et son siège social ;
- les nom, prénoms et domicile du destinataire du service en cause ou s'il s'agit d'une personne morale, sa dénomination et son siège social ;
- la description des faits litigieux et leur localisation précise sur le réseau ;
- les droits et les motifs pour lesquels le retrait du contenu litigieux est demandé ;
- la copie de la correspondance adressée à l'auteur ou à défaut à l'éditeur des informations ou activités litigieuses demandant leur interruption, leur retrait ou leur modification, ou la justification de ce que l'auteur ou l'éditeur n'a pu être contacté.

Article 48 :

— La procédure de notification des faits ou d'activités illicites prévue à l'article précèdent n'a pas pour effet d'engager la responsabilité d'une des personnes concernées par les exceptions prévues à l'article 47 de la présente loi.

Article 49 :

— Est puni d'une peine d'emprisonnement de un (1) à cinq (5) ans et d'une amende de 1 000 000 à 5 000 000 de francs CFA, le fait, pour toute personne de présenter de mauvaise foi aux personnes mentionnées à l'article 47 de la présente loi, un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion.

Article 50 :

— Les personnes mentionnées à l'article 47 de la présente loi ne sont pas soumises à une obligation de surveillance des informations qu'elles transmettent ou stockent, ni à une obligation de recherche des faits ou des circonstances révélant des activités illicites.

Toutefois, l'autorité judiciaire peut requérir de ces personnes une surveillance ciblée et temporaire des activités exercées par le biais de leurs services.

Article 51 :

— Les fournisseurs d'accès internet sont tenus de mettre en place un dispositif facilement accessible et visible sur leur site internet permettant à toute personne de porter à leur connaissance ce type d'activités illicites et sont tenus de rendre publics les moyens consacrés à cette lutte.

Les fournisseurs d'accès internet sont tenus également d'informer promptement les autorités publiques compétentes de toutes activités illicites qui leur sont signalées et qu'exercent les destinataires de leurs services.

Tout manquement aux obligations définies ci-dessus est puni d'une peine d'emprisonnement de un (1) à cinq (5) ans et d'une amende de 1 000 000 à 5 000 000 de francs CFA.

Article 52 :

— L'autorité judiciaire peut prescrire, à toute personne mentionnée à l'article 47 de la présente loi, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication électronique.

Tout manquement aux prescriptions judiciaires définies ci-dessus est puni d'une peine d'emprisonnement de un (1) à cinq (5) ans et d'une amende de 1 000 000 à 5 000 000 de francs CFA.

Article 53 :

— Les personnes mentionnées à l'article 47 de la présente loi sont tenues de détenir et de conserver sur une période de trois ans les données informatiques de nature à permettre l'identification de quiconque a contribué à la création d'un contenu ou de l'un des contenus des services dont elles sont prestataires conformément aux dispositions légales ou réglementaires relatives à la protection des données à caractère personnel.

L'autorité judiciaire peut requérir auprès de ces personnes la communication des données d'identification des destinataires des services dont elles sont prestataires.

Article 54 :

— Les personnes mentionnées à l'article 47 de la présente loi sont tenues de mettre à la disposition du public en ligne leurs propres données permettant de les identifier lorsque leurs services sont offerts à partir du territoire national ou sont accessibles à partir de ce territoire et destinés aux utilisateurs des réseaux de communication en ligne dudit territoire.

Ces données d'identification doivent comporter les éléments suivants :

- s'il s'agit de personnes physiques : leurs nom, prénoms, domicile, date et lieu de naissance, numéro de téléphone, adresse postale, adresse électronique et, si elles sont assujetties aux formalités d'inscription au registre de commerce et du crédit mobilier ou au répertoire des métiers, le numéro de leur inscription.

- s'il s'agit de personnes morales : leur dénomination sociale et l'adresse de leur siège social, leur numéro de téléphone et, si elles sont assujetties aux formalités d'inscription au registre de commerce et du crédit mobilier ou au répertoire des métiers, le numéro de leur inscription, leur capital social et leur adresse électronique.

Toutefois, les personnes éditant à titre non professionnel un service de communication électronique peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination sociale et l'adresse de la personne mentionnée à l'article 47 de la présente loi, sous réserve d'avoir satisfait auprès de cette dernière à son obligation d'identification telle que prévue ci-dessus.

Article 55 :

— Est puni d'une peine d'emprisonnement de un (1) an à cinq (5) ans et d'une amende de 1 000 000 à 5 000 000 de francs CFA le fait pour une personne physique ou le dirigeant de droit ou de fait d'une personne morale exerçant l'une des activités mentionnées à l'article 47 de la présente loi, de ne pas satisfaire aux obligations définies aux articles 53 et 54 ci-dessus.

Article 56 :

— Toute personne assurant une activité de transmission de contenus sur un réseau de télécommunications ou de fourniture d'accès à un réseau de télécommunications ne peut voir sa responsabilité civile ou pénale engagée en raison de ces contenus que dans l'un des cas suivants :

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

- lorsqu'elle sélectionne le destinataire de la transmission ;

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

Article 57 :

— Toute personne assurant dans le seul but de rendre plus efficace leur transmission ultérieure, une activité de stockage automatique, intermédiaire et temporaire des contenus qu'un prestataire transmet ne peut voir sa responsabilité civile ou pénale engagée à raison de ces contenus que si :

- elle a modifié ces contenus et 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 des données ;

- elle n'a pas agi avec promptitude pour retirer les contenus qu'elle a stockés ou pour en rendre l'accès impossible, dès qu'elle a effectivement eu connaissance soit du fait que les contenus transmis initialement ont été retirés du réseau, soit du fait que l'accès aux contenus transmis initialement a été rendu impossible, soit du fait que les autorités judiciaires ont ordonné de retirer du réseau les contenus transmis initialement ou d'en rendre l'accès impossible.

CHAPITRE 7 :

Adaptation des infractions classiques aux technologies de l'information et de la communication

Article 58 :

— Est puni de dix (10) à vingt (20) ans d'emprisonnement et de 10 000 000 à 20 000 000 de francs CFA d'amende, le fait pour toute personne de créer, de diffuser ou de mettre à disposition, sous quelque forme que ce soit, des écrits, messages, photos, sons, vidéos, dessins ou toute autre représentation d'idées ou de théories, de nature raciste ou xénophobe, par le biais d'un système d'information.

L'infraction ci-dessus définie est un délit.

Article 59 :

— Est puni de deux (2) à cinq (5) ans d'emprisonnement et de 5 000 000 à 20 000 000 de francs CFA d'amende, le fait pour toute personne de menacer autrui de mort ou de violence par le biais d'un système d'information.

Lorsque la menace a un caractère raciste, xénophobe, ethnique, religieux ou fait référence à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, la peine d'emprisonnement est de dix (10) à vingt (20) ans et l'amende est de 20 000 000 à 40 000 000 de francs CFA.

L'infraction ci-dessus définie est un délit.

Article 60 :

— Est puni de un (1) à dix (10) ans d'emprisonnement et de 5 000 000 à 10 000 000 de francs CFA d'amende, le fait pour toute personne de proférer ou d'émettre toute expression outrageante, tout terme de mépris ou toute invective qui ne renferme l'imputation d'aucun fait, par le biais d'un système d'information.

Article 61 :

— Est puni de trois (3) à cinq (5) ans d'emprisonnement et de 75 000 000 à 100 000 000 de francs CFA d'amende, le fait pour toute personne de nier, d'approuver ou de justifier, intentionnellement, des actes constitutifs de génocide ou de crimes contre l'humanité par le biais d'un système d'information.

Article 62 :

— Est puni de un (1) mois à dix (10) ans d'emprisonnement et de 5 000 000 à 20 000 000 de francs CFA d'amende, le fait pour une personne de produire, de mettre à la disposition d'autrui ou de diffuser des données de nature à troubler l'ordre public ou à porter atteinte à la dignité humaine par le biais d'un système d'information.

Article 63 :

— Est puni de un (1) à cinq (5) ans d'emprisonnement et de 5 000 000 à 20 000 000 de francs CFA d'amende, le fait pour toute personne de diffuser ou de mettre à disposition d'autrui par le biais d'un système d'information, sauf à destination des personnes autorisées, un mode d'emploi ou un procédé permettant la fabrication de moyens de destruction de nature à porter atteinte à la vie, aux biens ou à l'environnement.

Article 64 :

— Est puni de un (1) à cinq (5) ans d'emprisonnement et de 5 000 000 à 20 000 000 de francs CFA d'amende, le fait pour toute personne de diffuser ou de mettre à disposition d'autrui, par le biais d'un système d'information, des procédés ou des informations d'incitation au suicide.

Article 65 :

— Est puni de six (6) mois à deux (2) ans d'emprisonnement et de 1 000 000 à 5 000 000 de francs CFA d'amende, le fait pour toute personne de communiquer ou de divulguer par le biais d'un système d'information, une fausse information tendant à faire croire qu'une destruction, une dégradation ou une détérioration de biens ou une atteinte aux personnes a été commise ou va être commise.

Est puni des mêmes peines, le fait de communiquer ou de divulguer par le biais d'un système d'information, une fausse information faisant croire à un sinistre ou à toute autre situation d'urgence.

Article 66 :

— Est puni de cinq (5) à vingt (20) ans d'emprisonnement et de 5 000 000 à 20 000 000 de francs CFA d'amende, le fait pour toute personne de menacer de commettre par le biais d'un système d'information, une destruction, une dégradation ou une détérioration de biens ou une atteinte aux personnes, lorsqu'elle est matérialisée par un écrit, une image, un son, une vidéo ou toute autre donnée.

Article 67 :

— Est coupable de trahison et puni de l'emprisonnement à vie, le fait pour un Ivoirien :

- de livrer ou de s'assurer de la possession en vue de la livraison à un pays étranger ou à une personne physique ou morale étrangère par le biais d'un système d'information, un renseignement, un document, un procédé ou une donnée informatique qui doit être tenu*(e)* secret dans l'intérêt de la Défense nationale ;

- de détruire ou de laisser détruire un renseignement, un document, un procédé ou une donnée informatique qui doit être tenu*(e)* secret dans l'intérêt de la Défense nationale, en vue de favoriser un pays étranger ou une personne physique ou morale étrangère.

Article 68 :

— Est coupable d'espionnage et puni de l'emprisonnement à vie, le fait pour un étranger :

- de livrer ou de s'assurer de la possession en vue de la livraison à un pays étranger ou à une personne physique ou morale étrangère par le biais d'un système d'information, un renseignement, un document, un procédé ou une donnée informatique qui doit être tenu*(e)* secret dans l'intérêt de la Défense nationale ;

- de détruire ou de laisser détruire un tel renseignement, un document, un procédé ou une donnée informatique qui doit être tenu*(e)* secret dans l'intérêt de la Défense nationale, en vue de favoriser un pays étranger ou une personne physique ou morale étrangère.

Article 69 :

— Toute personne morale, à l'exception de l'État est pénalement responsable des infractions prévues par la présente loi, lorsqu'elles sont commises pour son compte par ses représentants.

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

La peine encourue par les personnes morales responsables est le double de l'amende prévue pour la personne physique ayant commis l'infraction.

Article 70 :

— En cas de condamnation au titre de la présente loi, outre la publicité de la condamnation ordonnée et exécutée, conformément à l'article 75 du Code pénal, le juge peut prononcer à titre complémentaire, la confiscation spéciale la privation des droits et l'interdiction de séjour prévues respectivement aux articles 63, 66 et 80 du Code pénal.

CHAPITRE 8 :

Procédure pénale en matière de cybercriminalité

Article 71 :

— Les officiers de police judiciaire définis à l'article 16 nouveau du Code de Procédure pénale, les experts agréés auprès des tribunaux et toute autre personne dont les compétences sont requises, serment préalablement prêté, peuvent procéder aux opérations prévues par la présente loi.

Les autorités compétentes visées ci-dessus n'ayant pas la qualité d'officier de Police judiciaire ne peuvent procéder à une perquisition qu'en présence de ces officiers.

Article 72 :

— Les données relatives aux abonnés doivent être conservées par les fournisseurs de services. Cette obligation impose aux fournisseurs de services de conserver et de protéger l'intégrité desdites données pendant une durée de dix ans.

Lorsqu'il est impossible de retrouver l'auteur d'une communication électronique pour défaut de conservation des données relatives aux abonnés, le fournisseur de services encourt une peine d'amende de 10 000 000 à 50 000 000 de francs CFA.

Article 73 :

— Lorsque dans le cadre d'une enquête ou d'une instruction, il y a des raisons de penser que des données informatiques spécifiées, y compris des données relatives aux abonnés et au trafic, stockées au moyen d'un système d'information, sont susceptibles de perte ou de modification, l'autorité compétente procède ou fait procéder à la conservation immédiate desdites données.

La personne physique ou morale à qui injonction est faite, conserve et protège l'intégrité desdites données pendant une durée aussi longue que nécessaire pour les besoins de l'enquête ou l'instruction.

Article 74 :

— L'autorité compétente, sur réquisition du procureur ou ordonnance du juge d'instruction, peut requérir :

- de toute personne physique ou morale, l'obligation de communiquer des données spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système d'information ou un support de stockage informatique ;

- d'un fournisseur de services, de communiquer les données spécifiées relatives au trafic et aux abonnés en sa possession ou sous son contrôle.

Article 75 :

— L'autorité compétente peut, au cours d'une perquisition effectuée dans les conditions prévues par le Code de Procédure pénale, accéder à un système d'information ou à un support de stockage numérique et à des données intéressant l'enquête en cours et stockées dans ledit système ou ledit support se trouvant sur les lieux de la perquisition.

L'autorité compétente peut également accéder à des données intéressant l'enquête en cours et stockées dans un autre système d'information, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.

S'il est avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système d'information situé hors du territoire national, elles sont recueillies par l'autorité compétente, sous réserve du respect des engagements internationaux.

Article 76 :

— L'autorité compétente peut, dans les conditions prévues par le Code de Procédure-pénale, procéder à la saisie des systèmes informatiques, des supports de stockage informatique ou procéder à la copie des données informatiques nécessaires à la manifestation de la vérité.

Si une copie est réalisée dans le cadre de cette procédure, il peut être procédé, sur décision du juge, à l'effacement définitif sur le support physique qui n'a pas été placé sous-main de justice, des données informatiques dont la détention ou l'usage est illégal ou dangereux pour la sécurité des personnes ou des biens.

Lorsque les systèmes informatiques ou les supports de stockage informatique sont mis sous scellés, ils ne peuvent être ouverts que selon les modalités prévues par le Code de Procédure pénale.

Article 77 :

— L'autorité compétente, sur réquisition du procureur ou ordonnance du juge d'instruction, est habilitée :

- à collecter ou enregistrer par tout moyen technique les données relatives au trafic ou au contenu associées à des communications spécifiques transmises sur son territoire au moyen d'un système d'information ;

- à obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à collecter ou enregistrer par tout moyen technique ou prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer en temps réel, les données relatives au trafic ou au contenu associées à des communications spécifiques transmises sur son territoire au moyen d'un système d'information.

Les surcoûts identifiables et spécifiques éventuellement exposés par les fournisseurs de services pour répondre à ces demandes font l'objet d'une compensation financière de l'État.

Article 78 :

— Est puni d'une peine d'emprisonnement de trois (3) à six (6) mois et de 1 000 000 à 5 000 000 de francs CFA d'amende, quiconque refuse de déférer à la demande du procureur ou du juge d'instruction.

Lorsqu'il s'agit d'une personne morale, elle encourt une peine d'amende de 10 000 000 à 100 000 000 de francs CFA.

Article 79 :

— La présente loi sera publiée au Journal officiel de la République de Côte d'Ivoire et exécutée comme loi de l'État.

Fait à Abidjan, le 19 juin 2013

Alassane OUATTARA