REPUBLIQUE DE GUINEE

Travail - Justice - Solidarité

Loi

N° L/ 2016/ 037/ AN,

Relative à la cyber-sécurité et la protection des données à caractère personnel en République de Guinée

L'Assemblée Nationale,

Vu la Constitution,

Après en avoir délibéré et adopté,

Le Président de la République promulgue la loi dont la teneur suit :

PREMIERE PARTIE : CYBER-SECURITE

TITRE I : DISPOSITIONS GENERALES

CHAPITRE Ier :TERMINOLOGIE

Article 1er : Au sens de la présente loi, les termes ci-dessous sont entendus de la manière suivante :

- ***Cybercriminalité :*** ensemble des infractions pénales qui se commettent au moyen ou sur un réseau de télécommunications ou un système d'information.
- ***Communication électronique*** : tout service ou moyen d' émission, de transmission ou de réception de signes, de signaux, d'écrits, de sons, d'images, ou de vidéos par voie électromagnétique, optique, ou par tout autre procédé, mis à la disposition du public ou d'une catégorie de public.
- ***Technologies de l'Information et de la Communications (Tics) :*** technologies employées pour recueillir, stocker, utiliser et envoyer des informations, et incluant celles qui impliquent l'utilisation des ordinateurs ou de tout autre système de communication y compris de télécommunications.

- ***Données informatiques ou données (tout court)*** : toute représentation de faits, d'informations ou de concepts, sous une forme assimilable à un traitement informatique, y compris un programme de nature à faire exécuter une fonction par un système d'information.
- ***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 ;
- ***Infrastructures critiques*** : les installations physiques et des technologies de l'information et de communications notamment électroniques, 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 social ou économique des citoyens, et/ou le fonctionnement correct ou continu des services de l'Etat.
- ***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 identifiée ou identifiable directement ou indirectement, à travers un numéro d'identification ou à un ou plusieurs éléments spécifiques, relatifs à son identité physique, physiologique, génétique, psychique, culturelle, sociale, ou économique.
- ***Données sensibles*** : toutes données à caractère personnel, relatives aux opinions ou activités religieuses, philosophiques, politique, syndicale, à la vie sexuelle ou raciale, à la santé, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives.
- ***Données relatives aux abonnés*** : toute information sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services notamment de communications électroniques/tics, 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 services de communication, les dispositions techniques prises à cet effet, et la durée du service ;
  - ✓ L'identité, l'adresse postale ou géographique, le numéro de téléphone ou tout autre numéro d'accès, l'adresse email, 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 relatives 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 service sous-jacent.
- ***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 ;
- ***Raciste et 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 race, de la couleur, de l'ascendance, de l'origine nationale,de l'ethnie 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 ;

- ***Mineur*** : toute personne âgée de moins de 18 ans au sens du Code Pénal guinéen.
- ***Pornographie infantile*** : toute donnée quelle qu'en soit la nature ou la forme, représentant de manière visuelle un mineur se livrant à un agissement sexuellement explicite ou des images représentant un mineur se livrant à un comportement sexuellement explicite ;
- ***Pays tiers*** : tout Etat non membre de la CEDEAO ;
- ***SMS*** : 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.
- ***Personne :*** toute personne physique ou morale, à l'exception des personnes morales de l'Etat et de ses services déconcentrés ou autres démembrements, des collectivités locales ou décentralisées, des établissements et des institutions publics.
- ***CERT*** :Centre de veille, d'alerte et de réponse aux attaques informatiques.

Pour les termes non définis par la présente loi, les définitions données par les instruments juridiques de la CEDEAO, de l'Union Africaine ou de l'Union Internationale des Télécommunications, prévalent sur toutes autres définitions.

CHAPITRE II : OBJET ET CHAMP D'APPLICATION

Article 2: La présente loi a pour objet, de définir les règles et mécanismes visant à lutter contre la cybercriminalité et créer ainsi un environnement favorable, propice et sécuritaire dans le cyber-espace, mais également de permettre à la République de Guinée de se conformer à ses engagements communautaires et internationaux en matière de cyber-sécurité.

Article 3: Sont soumises aux dispositions de la présente loi, les infractions relatives à la cybercriminalité commises sur le territoire de la République de Guinée, ainsi que les infractions pénales dont la constatation sur ledit territoire requiert la collecte d'une preuve électronique; et ce, quels que soient les auteurs des infractions, qu'il s'agisse de personnes physiques (citoyens guinéens ou étrangers) ou de personnes morales (à l'exception de l'Etat, des collectivités locales ou décentralisées, des établissements, des institutions ou administrations publics), dès lors que ces personnes se trouvent, exercent, ou évoluent sur le territoire national.

Toutefois, l'exception concernant l'Etat, les collectivités locales ou décentralisées, les établissements ou administrations publics, ne portent que sur la personne morale, et ne fait d'aucune manière, obstacle à l'application des dispositions de la présente loi aux agents de cette personne morale, qui commettraient des cyber-infractions.

En outre, la responsabilité pénale des personnes morales sujettes à l'application de la présente loi, n'exclut pas celle de leurs dirigeants ou représentants – personnes physiques, en cas de commission de l'une quelconque des infractions prévues par ladite loi.

TITRE II :

INFRACTIONS AUX TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION ET AUX COMMUNICATIONS ELECTRONIQUES OU COMMISES A TRAVERS CES TECHNOLOGIES ET COMMUNICATIONS

CHAPITRE III : ACCES ET MAINTIEN NON AUTORISES DANS LES SYSTEMES INFORMATIQUES

Article 4 : Quiconque accède ou tente d'accéder frauduleusement à tout ou partie d'un système informatique, pour quelles que raisons que soient, commet une infraction condamnée et punie par la loi.

Article 5:, Est puni d'un emprisonnement de un (1) an à cinq (5) ans et d'une amende de 60.000.000 à 130.000.000 Francs guinéens quiconque tente d'accéder frauduleusement à tout ou partie d'un système informatique.

Toute personne complice de la commission de cette infraction, sera punie des mêmes peines.

Article 6: Quiconque se maintient ou tente de se maintenir frauduleusement dans tout ou partie d'un système informatique, sera puni d'un emprisonnement de deux (2) ans à cinq (5) ans et d'une amende de 80.000.000 à 150.000.000 Francs guinéens.

Toute personne complice de la commission de cette infraction, sera punie des mêmes peines.

CHAPITRE IV: ENTRAVE AU FONCTIONNEMENT DES SYSTEMES INFORMATIQUES ET INTRODUCTION FRAUDULEUSE DE DONNEES DANS LES SYSTEMES INFORMATIQUES

Article 7: L'entrave au bon fonctionnement et/ou la falsification des données d'un système informatique constitue un acte de cybercriminalité et sera puni par la loi.

Article 8 : Quiconque entrave, fausse ou tente d'entraver ou de fausser le fonctionnement d'un système informatique, sera puni d'un emprisonnement de trois (3) ans à six (6) ans et d'une amende de 100.000.000 à 500.000.000 Francs Guinéens.

Toute personne complice de la commission de cette infraction, sera punie des mêmes peines.

Article 9 : Quiconque introduit ou tente d'introduire frauduleusement des données dans un système informatique, sera puni d'un emprisonnement de trois (3) ans à six (6) ans et d'une amende de 100.000.000 à 500.000.000 Francs Guinéens.

Toute personne complice pour la commission de cette infraction, sera punie des mêmes peines.

CHAPITRE V : INTERCEPTION FRAUDULEUSE, MODIFICATION ET FALSIFICATION DE DONNEES INFORMATIQUES

Article 10: L'interception frauduleuse et/ou la modification non autorisée des données informatiques constitue une infraction prévue et punie par la loi.

Article 11: 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 informatique, sera puni d'un emprisonnement de cinq (5) ans à dix (10) ans et d'une amende de 500.000.000 à 1.000.000.000 Francs Guinéens.

Toute personne complice de la commission de cette infraction, sera punie des mêmes peines.

Article 12: Quiconque altère ou tente d'altérer, modifie ou tente de modifier, supprime ou tente de supprimer frauduleusement des données informatisées, sera puni d'un emprisonnement de cinq (5) ans à dix (10) ans et d'une amende de 500.000.000 à 1.000.000.000 Francs Guinéens.

Toute personne complice de la commission de cette infraction, sera

punie des mêmes peines.

Article 13: 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, sera puni d'un emprisonnement de cinq (5) ans à dix (10) ans et d'une amende de 500.000.000 à 1.000. 000.000 Francs Guinéens.

Toute personne complice de la commission de cette infraction, sera punie des mêmes peines.

CHAPITRE VI: FRAUDE INFORMATIQUE, TRAITEMENT FRAUDULEUX DE DONNEES A CARACTERE PERSONNEL, USAGE DE DONNEES FALSIFIEES

Article 14: L'usage de données frauduleusement obtenues est puni par la loi.

Article 15: Quiconque fait usage ou tente de faire usage, en connaissance de cause, de données frauduleusement obtenues, sera puni d'un emprisonnement de deux (2) ans à cinq (5) ans et d'une amende de 300.000.000 à 600. 000.000 Francs Guinéens.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

Article 16 : 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 fonctionnement d'un système informatique, sera puni d'un emprisonnement de deux (2) ans à cinq (5) ans et d'une amende de 400.000.000 à 700.000.000 Francs Guinéens.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

CHAPITRE VII : DETENTION D'UN EQUIPEMENT POUR COMMETTRE DES INFRACTIONS CYBERCRIMINELLES ET COMMISSION DES INFRACTIONS INFORMATIQUES A TRAVERS DES ASSOCIATIONS SPECIFIQUEMENT FORMEES A CET EFFET OU PAR ENTENTE PREALABLE

Article 17: La détention frauduleuse d'un équipement de télécommunications à connecter sur un réseau ouvert au public ou un réseau privé constitue une infraction punie par la loi.

Article 18: La détention frauduleuse d'un mot de passe dans l'intention de s'introduire frauduleusement dans un système informatique est une infraction punie par la loi.

Article 19: Quiconque, dans l'intention de commettre l'une des infractions prévues par la présente loi, importe, vend, produit, 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,

Sera puni d'un emprisonnement de un (1) an à trois (03) ans et d'une amende de 150.000.000 à 550.000.000 Francs guinéens.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

Article 20: Quiconque participe, ou tente de participer à une association spécifiquement formée ou à une entente préalablement établie en vue de commettre ou de préparer l'une quelconque des infractions prévues par la présente loi ou assimilée, se rend coupable de 'délit', et sera puni d'un emprisonnement de trois (3) ans à cinq (5) ans et d'une amende de 1.000.000.000 à 1.500.000.000 Francs Guinéens.

CHAPITRE VIII : PRODUCTION, IMPORTATION OU EXPORTATION, POSSESSION, ET FACILITATION D'ACCES A DES IMAGES OU DES REPRESENTATIONS A CARACTERE PORNOGRAPHIQUE INFANTILE

Article 21: L'enregistrement, la diffusion, la transmission ou la représentation d'images à caractère de pornographie infantile constitue un délit et sera puni par la loi.

Article 22: Quiconque produit, enregistre, met à disposition, diffuse, transmet une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique ou d'un moyen de stockage de données informatiques, se rend coupable de 'délit', et sera puni d'un emprisonnement de cinq (5) ans à dix (10) ans et d'une amende de 700.000.000 à 1.000.000.000 Francs Guinéens.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines, mais également toute personne qui tenterait de commettre cette infraction.

Article 23: 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 informatique ou d'un moyen de stockage de données informatiques, sera puni d'un emprisonnement de cinq (5) ans à dix (10) ans et d'une amende de 700.000.000 à 1.000.000.000 Francs Guinéens.

Toute personne complice pour la commission de cette infraction, sera punie des mêmes peines, au même titre que toute personne qui tenterait de commettre cette infraction.

Article 24: Quiconque possède intentionnellement une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique ou d'un moyen de stockage de données informatiques, sera puni d'un emprisonnement de deux (2) ans à cinq (5) ans et d'une amende de 250.000.000 à 500.000.000 Francs Guinéens ou de l'une de ces deux peines seulement.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

Article 25: Quiconque facilite l'accès à des images, des documents, du son ou des représentations présentant un caractère pornographique à un mineur, sera puni d'un emprisonnement de deux (2) ans à cinq (5) ans et d'une amende de 250.000.000 à 500.000.000 Francs Guinéens.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines, au même titre que toute personne qui tenterait de commettre cette infraction.

CHAPITRE IX : DISPOSITION D'IMAGES OU D'ECRITS DE NATURE RACISTE OU XENOPHOBE PAR LE BIAIS D'UN SYSTEME INFORMATIQUE, INJURES, MENACES, ET NEGATIONNISME A TRAVERS LE SYSTEME INFORMATIQUE

Article 26: Le téléchargement, la diffusion et la mise à disposition de messages, de photos, d'écrits, de dessins ou toute autre représentation de théories ou d'idées, de nature raciste ou xénophobe, par le biais d'un système informatique, se rend coupable de délit puni par la loi.

Article 27: Quiconque crée, télécharge, diffuse ou met à disposition sous quelque forme que ce soit des messages, photos, écrits, dessins ou toute autre représentation de théories ou d'idées, de nature raciste ou xénophobe, par le biais d'un système informatique, se rend coupable de délit, et sera puni d'un emprisonnement de cinq (5) ans dix (10) ans et d'une amende de 100.000.000 à 300.000.000 Francs Guinéens.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

Article 28: Quiconque porte des menaces notamment de violence ou de mort par le biais d'un système informatique, sera puni d'un emprisonnement de un (01) an à cinq (5) ans et d'une amende de 30.000.000 à 100.000.000 Francs Guinéens.

Et lorsque ces menaces sont commises envers une personne en raison de son appartenance à un groupe donné, de sa race, de sa couleur, de son ascendance, de sa filiation, de sa religion, de son origine, de sa nationalité, de son ethnie, dans la mesure où cette appartenance sert

de prétexte à une telle menace, l'auteur de ces menaces sera puni d'un emprisonnement de trois (3) ans à huit (8) ans et d'une amende de 100.000.000 à 500.000.000 Francs Guinéens.

Toute personne complice de la commission de l'une de ces infractions sera punie des mêmes peines.

Article 29 : Quiconque émet une injure, une expression outrageante, tout terme de mépris ou toute invective qui ne renferme l'imputation d'aucun fait par le biais d'un système informatique, sera puni d'un emprisonnement de (6) mois à un (1) an et d'une amende de 40.000.000 à 120.000.000 Francs Guinéens.

Et lorsque ces infractions sont commises envers une personne en raison de son appartenance à un groupe donné, de sa race, de sa couleur, de son ascendance, de sa filiation, de sa religion, de son origine, de sa nationalité, de son ethnie, dans la mesure où cette appartenance sert de prétexte à une telle injure, son auteur sera puni d'un emprisonnement de trois (3) ans à huit (8) ans et d'une amende de 80.000.000 à 250.000.000 Francs Guinéens.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

Article 30: Quiconque nie, approuve, ou justifie de manière intentionnelle des faits constitutifs de génocide et/ou de crimes contre l'humanité par le biais d'un système informatique, se rend coupable de délit, et sera puni d'un emprisonnement de cinq (5) ans à dix (10) ans et d'une amende de 400.000.000 à 1.000.000.000 Francs Guinéens.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

CHAPITRE X : ATTEINTES ET MENACES A L'ORDRE ET A LA SECURITE PUBLICS; A LA SECURITE, L'INTEGRITE ET LA DIGNITE DES INDIVIDUS PAR LE BIAIS D'UN SYSTEME INFORMATIQUE,

Article 31: La production, la diffusion, la mise à disposition d'autrui des données de nature à troubler l'ordre ou la sécurité publics ou à porter atteinte à la dignité humaine par le biais d'un système informatique, se rend coupable de délit, et sera puni par la loi.

Article 32: Quiconque produit, diffuse ou met à disposition d'autrui des données de nature à troubler l'ordre ou la sécurité publics ou à porter atteinte à la dignité humaine par le biais d'un système informatique, se rend coupable de délit, et sera puni d'un emprisonnement de six (6) mois à cinq (5) ans et d'une amende de 20.000.000 à 300.000.000 Francs Guinéens.

Cette peine pourra être aggravée en fonction de l'ampleur de l'infraction et du préjudice causé. Toute personne complice pour la commission de cette infraction, sera punie des mêmes peines.

Article 33: Quiconque diffuse ou met à disposition d'autrui par le biais d'un système informatique, 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 humaine, aux biens, et/ou à l'environnement, se rend coupable d'acte de terrorisme, et sera puni d'un emprisonnement de trois (3) ans à un (05) ans et d'une amende de 500.000.000 à 1.000.000.000 Francs Guinéens.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

Article 34: Quiconque diffuse ou met à disposition d'autrui par le biais d'un système informatique, des informations ou procédés d'incitation au suicide, se rend coupable d'incitation au crime, et sera puni d'un emprisonnement de deux (2) ans à sept (7) ans et d'une amende de 100.000.000 à 350.000.000 Francs Guinéens.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

Article 35: Quiconque communique ou divulgue par le biais d'un système informatique, 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 sera puni d'un emprisonnement de six (6) mois à trois (3) ans et d'une amende de 20.000.000 à 100.000.000 Francs Guinéens ou de l'une de ces deux peines seulement.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

Quiconque communique ou divulgue par le biais d'un système informatique, une fausse information tendant à faire croire à un sinistre ou à toute autre situation d'urgence, sera au même titre que tout complice, puni des mêmes peines que celles prévues à l'alinéa 1er du présent Article.

Article 36: Quiconque menace de commettre par le biais d'un système informatique, une destruction, une dégradation ou une détérioration de biens ou une atteinte aux personnes, lorsqu'elle est matérialisée par un écrit, une image, une vidéo, un son ou toute autre donnée, se rend coupable de menace terroriste, et sera puni d'un emprisonnement de quatre (4) ans à dix (10) ans et d'une amende de 100.000.000 à 450.000.000 Francs Guinéens.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

Article 37: Est coupable de trahison et sera puni de l'emprisonnement à vie, tout citoyen de nationalité guinéenne, résidant sur le territoire de la République de Guinée ou en dehors, qui :

- ✓ Livre ou s'assure de la possession d'un renseignement, d'un document, d'un procédé ou d'une donnée informatique, devant pourtant être tenus « secret » dans l'intérêt de la défense nationale, en vue de les livrer à un pays étranger, à tout individu, ou à toute organisation qui porte atteinte ou viole ou est susceptible de porter atteinte ou de violer les intérêts fondamentaux de la république de Guinée, à travers les systèmes informatiques ;

- ✓ détruit ou laisse détruire un renseignement, un document, un procédé ou une donnée informatique, devant pourtant être tenus « secret » dans l'intérêt de la défense nationale, en vue de favoriser un pays étranger ou toute autre personne physique ou morale étrangère.

Article 38: Est coupable d'espionnage et sera puni de l'emprisonnement à vie, tout étranger (citoyen non guinéen) résidant sur le territoire de la République de Guinée ou en dehors, qui :

- ✓ Livre ou s'assure de la possession d'un renseignement, d'un document, d'un procédé ou d'une donnée informatique, devant pourtant être tenus « secret » dans l'intérêt de la défense nationale, en vue de les livrer à un pays étranger ou à une personne physique ou morale étrangère, par le biais d'un système informatique ;

- ✓ détruit ou laisse détruire un renseignement, un document, un procédé ou une donnée informatique, devant pourtant être tenus « secret » dans l'intérêt de la défense nationale, en vue de favoriser un pays étranger ou toute autre personne physique ou morale étrangère.

CHAPITRE XI : INFRACTIONS CLASSIQUES DE DROIT COMMUN COMMISES SUR OU PAR LE BIAIS DES SYSTEMES, LOGICIELS ET PROGRAMMES INFORMATIQUES

Article 39: Le fait d'utiliser ou de tenter d'utiliser les systèmes informatiques en vue de commettre des infractions de droit commun telles que le vol, l'escroquerie, le recel, l'abus de confiance, l'extorsion de fonds, le blanchiment de capitaux, constituent des circonstances aggravantes, et sont assimilées à des délits punis par la loi.

Article 40 Quiconque tente d'utiliser les systèmes informatiques en vue de commettre des infractions de droit commun telles que le vol, l'escroquerie, le recel, l'abus de confiance, l'extorsion de fonds, le blanchiment de capitaux sera puni d'un emprisonnement de un (1) an à deux (2) ans et d'une amende de 100.000.000à 1.000.000.000 Francs

Guinéens. Le montant de cette amende pourra toutefois, être revu à la hausse, selon l'ampleur de l'infraction et du préjudice qui en résulte.

Le fait d'utiliser ou de tenter d'utiliser les systèmes informatiques en vue de commettre des actes de terrorisme est lui, assimilable à un crime, entraînant selon l'ampleur de l'infraction, sera punie de (15) ans à la réclusion criminelle à perpétuité.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

Article 41: Quiconque commet ou tente de commettre un acte de terrorisme visant des données, logiciels et/ou programmes informatiques pourrait être assimilé à un crime, entraînant selon l'ampleur de l'infraction, un emprisonnement de cinq (05) ans à dix (10) ans et une amende de 500.000.000 à 3.000.000.000 Francs Guinéens.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

CHAPITRE XII: INFRACTIONS EN MATIERE DE DONNEES A CARACTERE PERSONNEL COMMISES SUR OU PAR LE BIAIS DES SYSTEMES INFORMATIQUES ET EN MATIERE DE CRYPTOLOGIE

Article 42: L'utilisation frauduleuse d'éléments d'identification d'une personne physique ou morale, du contenu d'une conversation électronique, même par omission ou négligence, constitue une violation de la vie privée et punie par la loi.

Article 43: Quiconque utilise ou tente d'utiliser frauduleusement un ou des éléments d'identification d'une personne physique ou morale ou procède ou fait procéder, même par omission ou négligence, à des traitements, à une conservation, à un détournement, à la mise à disposition ou divulgation à autrui de données à caractère personnel sans autorisation préalable de la personne concernée ou de l'autorité compétente ou en violation des règles et formalités prévues en la matière, par les dispositions relatives à la protection des données à caractère personnel, sera puni d'un emprisonnement de un (1) an à deux (2) ans et d'une amende de 75.000.000 à 300.000.000 Francs Guinéens.
Ces peines peuvent être aggravées selon l'ampleur de l'infraction et l'étendue du préjudice.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

Article 44: Lorsque la divulgation de données à caractère personnel sans autorisation de l'intéressé ou de l'autorité compétente, porte atteinte à la considération, à la dignité, à l'honneur de l'intéressé ou à l'intimité de sa vie privée, l'auteur de l'infraction, sera au même titre que tout complice, puni d'un emprisonnement de deux (2) ans à dix (10) ans et d'une amende de 100.000.000 à 400. 000.000 Francs Guinéens ou de l'une de ces deux peines seulement. Les mêmes peines sont applicables à la tentative de cette infraction.

La victime ou ses ayant-droits pourront en outre, engager une action civile (dommages-intérêts) pour la réparation du préjudice subi.

Toutefois, lorsque la divulgation prévue à l'alinéa précédent du présent article et ayant entraîné les conséquences mentionnées dans ledit article, a été commise par imprudence, omission, ou négligence, la peine d'emprisonnement et l'amende pour l'auteur ou tout complice, seront respectivement réduites de six (6) mois à cinq (5) ans et d'une amende de 20.000.000 à 75.000.000 Francs Guinéens.

Article 45: Quiconque utilise, possède, offre, vend, met à disposition, transmet en toute connaissance de cause par le biais d'un système informatique, de fausses données d'identification, sera puni de un (1) an à deux (2) ans et d'une amende de 80.000.000 à 175.000.000 Francs Guinéens.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

Article 46: Quiconque réalise ou tente de réaliser de fausses données d'identification par le biais d'un système informatique, se rend coupable de délit, et sera puni de un (1) an à deux (2) ans et d'une amende de 150.000.000 à 250.000.000 Francs Guinéens.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

Article 47: 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 par écrit son consentement préalable à recevoir de telles prospections ou qui s'y est formellement opposé, sera puni d'un emprisonnement de un (1) an à deux (2) ans et d'une amende de 30.000.000 à 200.000.000 Francs Guinéens.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

Article 48: Quiconque utilise des procédés illicites d'envoi de messages électroniques non sollicités en recourant à une collecte de données à caractère personnel, sera puni d'un emprisonnement de deux (2) ans à

cinq (5) ans et d'une amende de 60.000.000 à 230.000.000 Francs Guinéens.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

Article 49: Quiconque dissimule l'identité de la personne pour le compte de laquelle une offre commerciale est émise ou mentionne une offre sans rapport avec le service ou la prestation proposée, sera puni d'un emprisonnement de cinq (5) mois à deux (2) ans et d'une amende de 10.000.000 à 50.000.000 Francs Guinéens ou de l'une de ces deux peines seulement.

Article 50: Quiconque procède à un traitement de données à caractère personnel par un moyen frauduleux, déloyal ou illicite, se rend coupable de délit, et sera puni d'un emprisonnement de deux (2) ans à trois (3) ans et d'une amende de 75.000.000 à 900.000.000 Francs Guinéens.

La peine ne peut toutefois, être inférieure à 300.000.000 Francs Guinéens, lorsque le traitement frauduleux des donnéesa été fait en vue de l'envoi de messages électroniques non sollicités par une personne morale, à l'exception de l'Etat, des collectivités locales ou décentralisées et des établissements publics.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

Article 51: 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 emmener à communiquer des données à caractère personnelles ou des informations confidentielles, se rend coupable de délit, et sera puni d'un emprisonnement de un (1) an à deux (2) ans et d'une amende de 100.000.000 à 1.100.000.000 Francs Guinéens.

La peine d'emprisonnement ne saurait être cependant inférieure à deux (2) ans et l'amende inférieure à 500.000.000 Francs Guinéens, lorsque les données à caractère personnel ou les informations confidentielles communiquées, ont servi au détournement de fonds publics ou privés.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

Article 52: Quiconque prend ou tente de prendre frauduleusement connaissance d'une information à l'intérieur d'un système informatique, 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 se rend coupable de délit, et sera puni d'un emprisonnement de un (1) an à deux (2) ans et d'une amende de 75.000.000 à 150.000.000 Francs Guinéens.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

Article 53: La production, la vente, l'obtention pour utilisation, l'importation, la diffusion, ou d'autres formes de mise à disposition d'un dispositif, opérés de manière illégale, illicite et/ou intentionnelle, y compris d'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 informatique , 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 54: Lorsque les faits punis par la présente loi portent sur un système informatique ou un programme de traitement de données protégé par un code secret, la peine encourue ne peut être inférieure à cinq (05) ans d'emprisonnement.

Article 55: 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, sera puni d'un emprisonnement de un (1) an à cinq (5) ans et d'une amende de 40.000.000 à 180.000.000 Francs Guinéens.

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.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

Article 56: Quiconque, en dehors des cas prévus par la présente loi, met ou conserve sur support ou mémoire informatique, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître l'origine, la race, l'ethnie, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales, ou qui sont relatives à la santé ou à l'orientation sexuelle de celui-ci ou à toutes autres informations qui lui sont inhérentes et de nature sensible ou strictement personnelles, sera puni d'un emprisonnement d'un (1) an à sept (7) ans et d'une amende

de 30.000.000 à 150. 000.000 Francs Guinéens ou de l'une de ces deux peines seulement.

Article 57: Quiconque ne respecte pas l'interdiction d'exercer la profession de prestataire de cryptologie ou l'obligation de retrait des moyens de cryptologie, sera puni d'un emprisonnement de un (1) an à cinq (5) ans et d'une amende de 150.000.000 à 600.000.000 Francs Guinéens ou de l'une de ces deux peines seulement.

CHAPITRE XIII : INFRACTIONS EN MATIERE DE PROPRIETE INTELLECTUELLE DANS ET A TRAVERS LES SYSTEMES INFORMATIQUES

Article 58: Quiconque commet une atteinte à la propriété intellectuelle au moyen d'un système informatique, sera puni d'un emprisonnement de deux (2) ans à dix (10) ans et d'une amende de 100.000.000 à 900.000.000 Francs Guinéens ou de l'une de ces deux peines seulement. Ces peines pourront être alourdies selon l'ampleur de l'infraction et l'étendue du préjudice.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

Constitue une atteinte à la propriété intellectuelle :

- ✓ Le fait, sans autorisation de l'auteur ou de ses ayant-droits, de reproduire, de représenter ou de mettre à la disposition du public sur un système informatique ou un support numérique ou analogique, intégralement ou partiellement, une œuvre de l'esprit protégée par un droit d'auteur ou un droit voisin ;
- ✓ Le fait, sans autorisation de l'auteur ou de ses ayant-droits, de traduire ou d'adapter une œuvre de l'esprit par le biais d'un programme informatique ou de mettre cette traduction ou adaptation sur un système informatique ou un support numérique ou analogique à la disposition du public ;
- ✓ Le fait, sans autorisation de l'auteur ou de ses ayant-droits, 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 informatique 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 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, et sans droit, de vendre, de mettre à disposition du public par reproduction ou représentation, un bien ou un produit protégé par un brevet d'invention.

Article 59: 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'œuvre de l'esprit strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective, à

l'exception des copies des œuvres d'art destinées à être utilisées pour des fins identiques ou similaires à celles pour lesquelles l'œuvre d'art a été créée ;

- ✓ Les analyses et courtes citations, sous réserve que soient clairement indiqués les noms 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 accessoires 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 informatique ou électronique ;
- ✓ La reproduction et la représentation réalisées à des fins non lucratives par des personnes morales de droit public et par des établissements ouverts au public, telles que les bibliothèques, les services d'archives, les musées, les centres de documentation et les espaces culturels multimédias , en vue d'une consultation de l'œuvre à titre strictement personnel par des personnes atteintes d'une ou plusieurs déficiences de leurs fonctions motrices, physiques, sensorielles, mentales, cognitives ou psychiques, et dont le niveau d'incapacité est reconnu dans un certificat médical dûment établi à cet effet ;
- ✓ 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 chercheurs et enseignants directement concernés, sous réserve que cette reproduction ou représentation ne donne lieu à une exploitation commerciale ou lucrative.

Article 60: L'auteur d'une œuvre de l'esprit ou ses ayant-droits peuvent faire obstacle à la copie de l'œuvre en limitant le droit de copie reconnu 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 entraîne un préjudice injustifié aux intérêts de l'auteur.

Il est entendu par mesures techniques de protection, toute technologie, technique, 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 concernée.

Toutefois, l'usager doit être clairement informé de l'existence des mesures techniques de protection qu'il acquière 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 informatiques ou d'exploitation.

Article 61: 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 des ayant-droits.
A défaut, il se rend coupable de complicité par fourniture de moyen, et par conséquent répréhensible.

CHAPITRE XIV : INFRACTIONS EN MATIERE DE JEUX, TRANSFERTS D'ARGENT ET AUTRES AGISSEMENTS ILLICITES SUR LES RESEAUX DE COMMUNICATIONS ELECTRONIQUES

Article 62: L'organisation des jeux d'argent sur les réseaux de communications électroniques, est placée sous un régime de règlementation et de régulations strictes de l'Etat, impliquant la fourniture d'une licence ou d'une autorisation préalable à toute activité de cette nature.

A ce titre, Quiconque, sans autorisation préalable de l'Etat ou de ses services concernés, organise des jeux d'argent illicites en ligne notamment les jeux de hasard, de loterie illicite, de publicité de loterie prohibée, de prise de paris illicites ou de tous autres jeux dont la mise en œuvre requiert une autorisation préalable, sera puni d'un emprisonnement de un (1) an à cinq (5) ans et d'une amende de 75.000.000 à 1.000.000.000 Francs Guinéens.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

Article 63: Sont interdits sur les réseaux de communications électroniques, 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.

Les établissements bancaires et financiers opérant sur le territoire Guinéen, doivent veiller au respect de cette interdiction, et notifier à ce titre aux autorités compétentes.

Article 64: Quiconque ne respecte pas l'interdiction de transfert d'argent mentionnée à l'Article 63 précédent, sera puni d'un emprisonnement de un (1) an à deux (2) ans et d'une amende de 75.000.000 à 1.500.000.000 Francs Guinéens. Ces peines pourront être alourdies selon l'ampleur de l'infraction et l'étendue du préjudice.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

Lorsque cette interdiction est violée par une personne morale (à l'exception de l'Etat, des collectivités locales ou décentralisées, des établissements et institutions publics – leurs agents restent quant à eux responsables), la peine d'emprisonnement et l'amende encourues sont portées au double. Les mêmes peines sont applicables à tout complice.

Si le transfert est effectué à destination de l'étranger, ce fait est également constitutif d'une infraction à la règlementation régissant les transactions financières notamment internationales et le contrôle des changes, et assimilable à un délit, sans préjudice de l'application des sanctions prévues par ladite règlementation.

La personne (physique ou morale) auteur de cette infraction tout comme son complice, sera punie d'un emprisonnement de deux (2) ans à cinq (5) ans et d'une amende de 200.000.000 à 2.000.000.000 Francs Guinéens. Cette amende pourra être aggravée en fonction de l'ampleur de l'infraction et du préjudice qui en résulte.

Article 65: Outre la structure guinéenne en charge de la lutte contre la cybercriminalité (pour les sanctions pécuniaires), les juridictions nationales sont compétentes, pour constater et/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 communications électroniques 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 communications 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 XV :RESPONSABILITE DES PRESTATAIRES TECHNIQUES DE SERVICE EN LIGNE

Article 66 : L'ouverture d'un cyber-café est, conformément aux dispositions de la loi relative aux Télécommunications et aux Technologies de l'Information en République de Guinée, soumise à l'Agrément ou un acte de reconnaissance d'activités préalable de l'Autorité de Régulation des Postes et Télécommunications.

Article 67 : L'accès au service internet à partir de cyber-cafés est soumis à l'identification préalable des usagers. Les exploitants de cyber-cafés sont tenus de procéder à cette identification préalable, dont les modalités seront fixées par Arrêté du Ministre en charge des Postes, des Télécommunications et de l'Economie Numérique.

Article 68 : Tout mineur de moins de douze (12) ans ne peut accéder à un cyber-café, qu'accompagné d'un adulte.

Article 69 : L'accès de tout mineur de moins de dix-huit (18) ans à un cyber-café, doit être un accès limité, qui exclue l'accès aux sites web à caractère pornographique, violent, raciste, haineux ou dégradant et de manière générale, tous les sites web portant atteinte à la dignité humaine ou incitant à l'incivisme.

Article 70 : Les personnes dont l'activité est d'offrir un service de communication en ligne doivent rendre possible l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner, et d'informer leurs abonnés ou leurs usagers de l'existence de ces moyens.

Article 71 : Quiconque ne respecte pas cette obligation de rendre possible l'existence des moyens visés à l'Article 70 précédent, et/ou viole l'obligation d'information de l'existence de ces moyens à ses abonnés ou usagers, sera puni d'une amende de 20.000.000 à 100.000.000 Francs Guinéens. Et le dirigeant ou le(s) propriétaire(s) de cet opérateur ou prestataire de services de communications en ligne, sont passibles de six (6) mois à trois (3) ans d'emprisonnement.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

En outre, le fournisseur de services offrant un accès à des services de communication ou assurant à titre gratuit ou onéreux le stockage permanent pour mise à disposition de contenus, est tenu sur décision de l'autorité compétente, de suspendre immédiatement l'accès auxdits services ou contenus.

Article 72 : 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 et/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, de bonne foi et en aucun moment, pas eu connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ;
- ✓ Si dès le moment où elles ont eu connaissance de ce caractère illicite, 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 l'autorité compétente.

Article 73 : La connaissance des faits litigieux est présumée acquise par les personnes indiquées à l'article 72 précédent, dès lors qu'il leur est

notifié par la victime ou par toute personne intéressée, les activités illicites ou les faits et circonstances faisant apparaître ce caractère d'illicéité.

Cependant, pour être prise en considération, la notification par les personnes précitées, doit comporter les éléments suivants :

- ✓ Si la personne auteur de la notification est une personne physique : ses nom, prénom, profession, domicile, nationalité, date et lieu de naissance, et ses coordonnées téléphonique et électronique (email).
- ✓ Si la personne auteur de la notification est une personne morale : sa dénomination, son siège social, et ses coordonnées téléphonique et électronique (email, site web).
- ✓ les nom, prénom, domicile, et dans la mesure du possible la profession, nationalité, date et lieu de naissance, et les coordonnées téléphonique et électronique (email). du destinataire du service en cause et s'il s'agit d'une personne morale, sa dénomination, son siège social, et ses coordonnées téléphonique et électronique (email, site web) ;
- ✓ la description des faits litigieux et leur localisation précise sur le réseau ;
- ✓ les droits et motifs pour lesquels le retrait du contenu litigieux est requis ;
- ✓ 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 modification, ou la justification que l'auteur ou l'éditeur n'a pas pu être contacté.

Article 74: La procédure de notification des faits ou activités illicites prévue à l'article 73 de la présente loi, n'a pas pour effet d'engager la responsabilité d'une des personnes concernées par les exceptions visées audit article.

Article 75: Quiconque présente de mauvaise foi, aux personnes visées à l'Article 73 de la présente loi, un contenu ou une activité, comme étant illicite, dans le but d'en obtenir le retrait ou de faire en cesser la diffusion, sera puni d'un emprisonnement de un (1) an à cinq (5) ans et d'une amende de 15.000.000 à 75.000.000 Francs Guinéens ou de l'une de ces deux peines seulement.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

Article 76: Les personnes mentionnées à l'Article 73 de la présente loi, ne sont pas obligées de surveiller les informations qu'elles transmettent ou stockent, ni de rechercher des faits ou circonstances révélant des activités illicites. Toutefois, l'autorité compétente, peut requérir de ces

personnes, de procéder à une surveillance ciblée et temporaire des activités réalisées par le biais de leurs services.

Article 77: Les fournisseurs d'accès internet ont l'obligation de mettre en place un dispositif facilement accessible et visible sur leur site internet, permettant à toute personne intéressée, de porter à leur connaissance, ce type d'activités illicites. Ils sont aussi tenus de rendre publics, les moyens dédiés à cette lutte.

En outre, ils ont l'obligation d'informer sans délai et par tous moyens admissibles l'autorité compétente et éventuellement l'autorité judiciaire compétente ou toute autre autorité compétente, de toutes activités illicites exercées par des destinataires de leurs services, qui leur sont signalées par des tiers ou qu'ils auraient eux-mêmes constaté ou soupçonné.

Tout manquement à l'une quelconque des obligations mentionnées aux alinéas 1er et 2 du présent Article, expose son auteur, au même titre que son complice, à un emprisonnement de un (1) an à cinq (5) ans et d'une amende de 15.000.000 à 100.000.000 Francs Guinéens.

Article 78 : Les autorités compétentes, peuvent prescrire ou ordonner à toute personne mentionnée à l'Article 73 de la présente loi, la mise en œuvre de toutes mesures ou solutions propres à prévenir ou à faire cesser un dommage occasionné par le contenu d'un service de communication électronique, notamment la collecte ou l'enregistrement des faits ou données répréhensibles.

Toute violation de cette prescription ou de cet ordre, expose son auteur et tout complice, à un emprisonnement de un (1) an à cinq (5) ans et à une amende de 60.000.000 à 300.000.000 Francs Guinéens.

Article 79: Les personnes mentionnées à l'Article 73 de la présente loi , sont tenues de détenir et de conserver sur une durée comprise entre trois (3) et cinq (05) ans en fonction de l'importance des données, les données informatiques pouvant permettre d'identifier 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 règlementaires relatives à la protection des données à caractère personnel.

Toutefois, au cas où la durée mentionnée à l'alinéa 1er ci-dessus est contraire ou en violation des prescriptions prévues en la matière par la législation ou la règlementation relative à la protection des données à caractère personnel, les règles prévues par cette législation ou cette règlementation auront la primauté.

Article 80 : Les personnes mentionnées à l'Article 73 de la présente loi, ont l'obligation de mettre en ligne à la disposition du public, 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 communications en ligne dudit territoire.

Ces données d'identification doivent comporter les éléments suivants :

- ✓ s'il s'agit de personnes physiques : leurs nom, prénom(s), domicile, date et lieu de naissance, nationalité, adresse postale et géographique, numéro de téléphone, adresse électronique (email) ; et si elles sont assujetties à l'inscription au Registre du Commerce et du Crédit mobilier ou au répertoire des métiers, les références de cette inscription.
- ✓ S'il s'agit de personnes morales : leur dénomination sociale et l'adresse postale et géographique du siège social, leur numéro de téléphone, leur adresse électronique (email, site web) ; et si elles sont assujetties à l'inscription au Registre du Commerce et du Crédit mobilier ou au répertoire des métiers, les références de cette inscription, ainsi que le montant et la répartition de leur capital social. En outre, si elle est assujettie à la Direction Nationale des Impôts et à la taxe sur la valeur ajoutée, son numéro d'identification fiscal (code NIF) et sa clé TVA.
- ✓ Si son activité est soumise à un régime d'autorisation, le nom et l'adresse de l'autorité ayant délivré celle-ci. Si elle est membre d'une profession réglementée, la référence aux règles professionnelles applicables, son titre professionnel, l'Etat membre dans lequel il a été octroyé ainsi que le nom de l'ordre ou de l'organisme professionnel auprès duquel elle est inscrite.

Toutefois, les personnes exerçant à titre non professionnel un service de communication électronique, sont autorisées à ne fournir au public, afin de préserver leur anonymat, que le nom, la dénomination sociale, et l'adresse des personnes visées à l'Article 73 de la présente loi sous réserve toutefois d'avoir satisfait au préalable auprès de ces dernières, à son obligation d'identification dans les conditions ci-dessus énumérées.

Article 81: Quiconque, personne physique – dirigeant de droit ou de fait d'une personne morale exerçant l'une des activités énumérées à l'Article 73 de la présente loi, ne satisfait pas aux obligations prévues aux Articles 78 et 80 de cette loi, sera puni d'un emprisonnement de six (6) mois à quatre (4) ans et d'une amende de 10.000.000 à 100.000.000 Francs Guinéens.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

Article 82: 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 et/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 transmission.

Article 83: Toute personne assurant dans le 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 et/ou pénale engagée en 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 entravé l'utilisation licite et usuelle de la technologie utilisée pour obtenir des données ;
- ✓ Elle n'a pas agi avec promptitude pour retirer des 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 l'autorité compétente a prescrit ou ordonné de retirer du réseau les contenus transmis initialement ou d'en rendre l'accès impossible.

CHAPITRE XVI: SANCTIONS RELATIVES AUX REFUS DE COMMUNICATIONS REQUISES PAR LES AUTORITES COMPETENTES

Article 84: Le refus de communication à la structure guinéenne en charge de la Cyber-sécurité, à l'autorité judiciaire compétente ou toute autorité publique des données d'identification ou en général de toute information mentionnée ou requise en vertu des dispositions de la présente loi ou de ses textes d'application subséquents, expose l'auteur et tout complice, à 2.000.000 Francs Guinéens par jour de retard (montant qui sera porté au double au bout d'une semaine), et à une peine d'emprisonnement de un (1) an à cinq (5) ans, ou à l'une de ces deux peines seulement.

CHAPITRE XVII: SANCTIONS SPECIFIQUES AUX INFRACTIONS A LA PRESENTE LOI COMMISES PAR LES PERSONNES MORALES

Article 85: Lorsque les infractions à la présente loi sont commises par les personnes morales (à l'exception de l'Etat et ses services déconcentrés, des collectivités locales ou décentralisée et des institutions et établissements publics), les amendes et peines d'emprisonnement prévues par ladite loi, sont portées :

- ✓ du double au quintuple pour l'amende, selon l'ampleur de l'infraction et l'étendue du préjudice, et
- ✓ au double en ce qui concerne la peine d'emprisonnement du représentant ou dirigeant de la personne morale ou de son propriétaire ou de ses actionnaires, au cas où cette aggravation de sanction n'aurait pas été initialement et explicitement prévue.

CHAPITRE XVIII : SANCTIONS COMPLEMENTAIRES AUX INFRACTIONS A LA PRESENTE LOI, RECIDIVE, ET PUBLICATION DES SANCTIONS

Article 86: Sans préjudice de l'application des dispositions prévues en la matière par le Code pénal guinéen ou par les lois sur la protection des données à caractère personnel, sur les transactions électroniques, sur la cryptologie et/ou par leurs textes d'application, les personnes (physiques ou morales) condamnées ou sanctionnées (amendes ou peines de prison) pour les infractions prévues par la présente loi, encourent également sur ordonnance du juge compétent, les peines complémentaires et non exhaustives suivantes:

- ✓ L'interdiction pour une durée de cinq (5) ans d'exercer une fonction publique, ou d'exercer l'activité sociale ou professionnelle dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ou de toutes autres activités sociales ou professionnelles, l'auteur de l'infraction ou son complice, serait raisonnablement susceptible de commettre à nouveau l'une quelconque des infractions prévues par la présente loi;
- ✓ L'interdiction temporaire ou définitive de séjour sur le territoire de la république de Guinée;
- ✓ La privation de ses droits, notamment l'inéligibilité pour toutes fonctions de représentation syndicale, locale ou nationale ;
- ✓ L'exclusion provisoire ou définitive de toute possibilité de concourir ou d'être recrutée à tout processus (appel d'offres, consultations ou manifestations d'intérêt), relatif à un marché public ;
- ✓ L'interdiction temporaire ou définitive de procéder à un appel public à l'épargne ;

- ✓ l'interdiction d'émettre des messages de communication numérique ou électronique ;
- ✓ l'interdiction à titre provisoire ou définitif de l'accès au site ayant servi à commettre une infraction au système informatique, voire l'interdiction d'héberger ce site ;
- ✓ L'interdiction d'émettre des chèques autres que ceux qui permettent de procéder à des retraits de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;
- ✓ L'interdiction d'utiliser des cartes bancaires ou toutes autres formes de paiement électroniques ;
- ✓ La dissolution de la société ou de l'organisation, dans le cadre des personnes morales.

Article 87: En cas de récidive aux infractions prévues dans le cadre de la présente loi, les peines et amendes prévues aux Articles 4 à 77 seront alourdies, et pourront aller du double au quintuple pour les amendes, et au double pour les peines d'emprisonnement.

Les sanctions complémentaires suscitées et non exhaustives, pourront également être appliquées et aggravées au niveau de leur teneur, à la discrétion de l'autorité judiciaire compétente.

La récidive est entendue au sens de la présente loi, comme la commission à nouveau d'une infraction déjà commise par le passé ou d'une autre des infractions prévues par ladite loi (qui n'aurait pas obligatoirement été déjà commise).

Article 88: Les sanctions (pécuniaires, de prison, ou administratives) prononcées à l'encontre des auteurs (personnes morales ou physiques) d'infractions aux dispositions de la présente loi ou de leurs complices, devront être publiées au moins au journal officiel de la République.

TITRE III

DISPOSITIONS INSTITUTIONNELLES

CHAPITRE XIX : ORGANE(S) OU INSTITUTION(S) RESPONSABLES DE LA LUTTE CONTRE LA CYBERCRIMINALITE ET DE LA BONNE APPLICATION DE LA PRESENTE LOI

Article 89: Le Centre de sécurité des systèmes d'information (CERT) est chargé de la prévention (veille), de l'alerte, des investigations, de la recherche, de la détection, de la riposte, du déferrement des suspects, auteurs et

leurs complices, de la certification, de la sensibilisation et de la formation en matière de lutte et de répression contre les menaces et infractions aux technologies de l'information et de la communications notamment les systèmes informatiques et les communications électroniques en République de Guinée.

Cette structure est l'organe principalement responsable de la lutte et de la répression contre la cybercriminalité en République de Guinée et dispose à cet égard de tous les pouvoirs requis à cet effet.

Des dispositions règlementaires fixeront les modes de fonctionnement du CERT.

Article 90: La politique stratégique, les objectifs, les plans d'actions et les programmes de lutte contre la cyber-délinquance sont soumis à l'appréciation et à la validation conjointes des Ministres en charge des Postes, des Télécommunications, de l'Economie Numérique, de la Justice et de la Sécurité et si besoin est, de la Défense Nationale, de l'Economie et des Finances, du Commerce et du Gouverneur de la Banque Centrale.

Article 91: Chaque agent ou collaborateur de l'autorité compétente, doit préalablement à sa prise de fonction, prêter serment devant le Premier Président de la Cour d'Appel.

CHAPITRE XX :AUTRES MECANISMES ET ACTEURS IMPORTANTS DANS LA LUTTE CONTRE LA CYBERCRIMINALITE

Article 92: Le Ministre des Postes, des Télécommunications et de l'Economie Numérique, en collaboration avec les autres départements concernés devra prendre toutes mesures, décisions utiles et nécessaires, visant à favoriser l'installation et l'opérationnalisation dans de brefs délais à compter de la promulgation de la présente loi, d'une Plateforme de lutte contre la cybercriminalité (CERT) au sein de chaque secteur socio-économique de la Guinée (Opérateurs de Téléphonie, Fournisseurs d'Accès Internet, Banques, Assurances, Universités publiques ou privées, Hôpitaux, Industries d'extraction ou autres Industries de production et de services etc.), afin de leur permettre de renforcer les synergies et mutualiser leurs efforts pour une meilleure lutte contre la cybercriminalité au sein de leurs secteurs d'activités respectifs.

Article 93: Ces plateformes sectorielles de lutte contre la cybercriminalité, vectrices d'efficacité dans la lutte contre la cybercriminalité à l'échelle du territoire national, seront placées sous la coordination du Centre National de sécurité des systèmes d'information.

TITRE IV
REGLES PROCEDURALES EN MATIERE DE CYBERCRIMINALITE ET MOYENS DE PREUVES

Article 94: Les Agents assermentés du centre pour la sécurité des systèmes d'information ou les officiers de police judiciaire sur réquisition ou mandat du parquet et sur décision de l'autorité judiciaire compétente selon le cas, peuvent en cas de soupçon fondé ou d'infraction avérée :

- ✓ procéder à des perquisitions ou accéder à tout système informatique, en vue de la manifestation de la vérité ;
- ✓ procéder à la saisie conservatoire ou à la confiscation définitive des équipements, supports, matériels, logiciels, programmes, données, documents, ayant servi à la commission de l'infraction ou qui étaient destinés à la commission d'une infraction (tentative);
- ✓ procéder à la mise sous scellés des locaux ayant abrité la commission de l'infraction ou qui étaient destinés à la commission d'une infraction (tentative).

En l'absence de volonté, ou en cas d'inutilité ou d'impossibilité de procéder à la saisie du support électronique, les données de même nature que celles qui sont nécessaires à la compréhension du système, devront néanmoins faire l'objet de copies sur des supports de stockage informatique et être placées sous scellés.

Les actions précitées, ne sauraient cependant être mises en œuvre, en violation des dispositions du code de procédure pénale qui seraient prévues en la matière.

Si les copies évoquées à l'alinéa 2 du présent Article sont réalisées notamment dans le cadre des actions visées par ledit Article, il peut être procédé sur décision du juge compétent, à l'effacement définitif sur le support qui n'a pas été placé sous-main de justice, des données informatiques dont la détention ou l'usage est illégal (notamment au regard des impératifs de protection des données à caractère personnel) ou dangereux pour la sécurité des personnes et des biens.

Article 95: Lorsque des systèmes informatiques, des supports informatiques, ou des locaux ayant servi à la commission d'une infraction ou d'une tentative d'infraction au sens de la présente loi, sont mis sous scellés, ils ne peuvent être rouverts que selon les modalités prévues par le code de procédure pénale.

Article 96: Les perquisitions, enquêtes ou accès par les agents ou services compétents à tout système d'information, ne peuvent être opérés en violation des règles prescrites par le Code Pénal et de Procédure Pénale en vigueur en République de Guinée, à l'exception des cas ou situations consécutifs d'un risque ou d'un péril imminent et/ou d'une atteinte grave pour la santé, la sécurité et/ou le bon fonctionnement de l'Etat, ou d'un citoyen.

Les Agents assermentés peuvent à cet effet, librement procéder, seuls ou avec le concours d'autres officiers de police judiciaire ou des forces de défense et de sécurité en général, à des contrôles inopinés, investigations, perquisitions, saisies, arrestations, déferrements de suspects et de leurs complices ou plus généralement, exercer tous pouvoirs de police administrative et judiciaire dans le cyber-espace, dont la mise en œuvre pourrait s'avérer utile ou fondamentale pour la défense des intérêts fondamentaux de la nation, ou la sécurité, la tranquillité et la santé des citoyens.

Toutefois, ces agents demeureront pénalement et civilement responsables de tous abus qu'ils commettraient au cours de l'exercice de ces mesures d'exception.

Article 97: Lorsque les nécessités de l'information l'exigent et lorsqu'il y a des raisons sérieuses de craindre la disparition de données informatiques archivées valant preuve ou commencement de preuve, l'autorité compétente, peut faire injonction à toute personne intéressée, de conserver et de protéger dans le secret l'intégrité des données en sa possession ou sous son contrôle, dans un délai maximum de dix (10) ans à compter de la date de notification de l'injonction.

Article 98: L'écrit électronique est admis comme preuve en matière de cybercriminalité, à condition toutefois que la personne dont émane l'écrit puisse être dûment identifiée, et que l'écrit soit établi et conservé, dans des conditions de nature à en garantir l'intégrité.

Article 99: Les données relatives aux abonnés doivent être conservées par les opérateurs de systèmes informatiques ou les prestataires de services de communications électroniques et protégées dans leur intégrité, pendant une durée minimale de cinq (5) ans.

Lorsqu'il est impossible de retrouver l'auteur d'une communication électronique pour défaut de conservation des données relatives aux abonnés ou pour perte de l'intégrité desdites données, l'opérateur du système informatique ou le prestataire du service de communications électroniques, encourt une amende de 150.000.000 à 700.000.000 Francs Guinéens.

Article 100: Lorsque dans le cadre d'une enquête ou d'une instruction, il existe 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 informatique, sont susceptibles de perte ou de modification, l'autorité compétente peut procéder ou faire procéder à la conservation immédiate desdites données. Une telle décision peut être également ordonnée par l'autorité judiciaire compétente.

La personne physique ou morale à qui injonction est faite, doit conserver et protéger l'intégrité desdites données pendant une durée

aussi longue que le temps nécessaire pour l'instruction ou pour l'enquête.

Article 101: l'autorité publique compétente 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 informatique ou un support de stockage informatique ;
- ✓ d'un opérateur de systèmes informatiques ou d'un prestataire de services de communications électroniques, de communiquer les données spécifiées relatives au trafic et aux abonnés en sa possession ou sous son contrôle.

Article 102: l'autorité publique compétente peut au cours d'une perquisition ou d'investigations, accéder à un système informatique ou à un support de stockage numérique et à des données relatives à l'enquête en cours et stockées dans ledit système ou ledit support se trouvant sur les lieux de la perquisition ou des investigations.

Cet accès peut également porter sur des données relatives à l'enquête en cours et stockées dans un autre système informatique n'étant pas forcément sur les lieux de la perquisition ou des investigations, 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 informatique situé hors du territoire de la République de Guinée, elles peuvent et doivent être recueillies par l'autorité publique compétente, sous réserve cependant du respect des engagements internationaux de la République de Guinée.

Cet accès ne devrait en outre pas se faire, en violation des dispositions du code de procédure pénale qui seraient prévues en la matière.

Article 103: l'autorité publique compétente peut, sous réserve du respect de toutes dispositions du code de procédure pénale qui seraient prévues à cet effet :

- ✓ collecter ou enregistrer par tout moyen technique les données relatives au trafic ou au contenu associées à des communications spécifiques transmises sur le territoire guinéen au moyen d'un système informatique ;
- ✓ obliger un opérateur de systèmes informatiques ou un prestataire de services de communications électroniques, dans le cadre de ses capacités techniques existantes, à collecter ou enregistrer par tout moyen technique ou prêter auxdites Autorités son concours et son assistance pour collecter et enregistrer en temps réel, les données relatives au trafic ou au contenu associées à des communications

transmises sur le territoire guinéen au moyen d'un système informatique.

Article 104: Les surcoûts identifiables et spécifiques, nécessaires à la mise en œuvre par l'opérateur d'un système informatique ou un prestataire de services de communications électroniques de l'assistance précisée aux articles précédents de la présente loi, et éventuellement exposés par ledit opérateur ou prestataire, devront faire l'objet d'une compensation financière par l'autorité financière compétente.

Article 105: Quiconque refuse de déférer aux demandes et réquisitions légales et régulières (en vertu des dispositions de la présente loi et de ses textes d'application) de l'autorité publique et de ses agents assermentés et aux demandes et réquisitions des autorités judiciaires compétentes (Procureur de la République, Juge d'Instruction) sera puni d'un emprisonnement de six (6) mois à deux (2) ans et d'une amende de 15.000.000 à 100.000.000 Francs Guinéens.

Lorsque l'auteur de cette infraction est une personne morale, elle encourt une amende de 150.000.000 à 800.000.000 Francs Guinéens, sans préjudice de l'application des autres sanctions.

TITRE V
COOPERATION TECHNIQUE, POLICIERE, ET JUDICIAIRE POUR LA LUTTE CONTRE LA CYBERCRIMINALITE

Article 106: Le Cyber-espace n'ayant pas de frontière et entraînant de nombreux et complexes défis pour la recherche et la riposte aux infractions qui la caractérisent, et qui constituent en outre de sérieuses menaces à la sécurité, à l'ordre public et au développement économique national ainsi qu'à la quiétude et à la sécurité des citoyens nécessitant par là-même une coopération accrue entre les différents intervenants dans cette lutte (Etats, Organisations régionales ou internationales, instituts de standardisation ou de normalisation...), une collaboration accrue est nécessaire entre les Ministères de la Justice, de la Sécurité, des Postes, Télécommunications et de l'Economie Numérique, ainsi que l'Autorité de Régulation des Postes et Télécommunications.

TITRE VI
PRESCRIPTIONS EN MATIERE D'INFRACTIONS CYBERCRIMINELLES

Article 107: Les prescriptions concernant les infractions relatives au cyber-espace et définies dans la présente loi, suivent le même régime que ceux prévus par les Codes Pénal et de Procédure Pénale en vigueur en République de Guinée.

TITRE VII
DISPOSITIONS FINALES

Article 108: Les infractions prévues par la présente loi ne sont pas exhaustives en matière de cybercriminalité et pourront à cet égard, pour celles non prévues par ladite loi, être définies, et sanctionnées dans le cadre des textes subséquents qui seront pris pour son application.

Les sanctions prévues dans le cadre de la présente loi, pourront aussi, en tant que de besoin, être élargies ou aggravées.

Les sanctions en matière de cybercriminalité seront en outre complétées et renforcées par les sanctions prévues par les lois spécifiques sur les transactions électroniques, sur la protection des données à caractère personnel, sur la cryptologie et/ou par leurs textes d'application.

Article 109: Les modalités d'application de la présente loi, seront prises par Décret ou arrêté du Ministre en charge des Postes, des Télécommunications et de l'Economie numérique.

DEUXIEME PARTIE : LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

TITRE I : DISPOSITIONS GENERALES

CHAPITRE Ier : TERMINOLOGIE

Article 1er: Au sens de la présente loi, les termes ci-dessous sont entendus de la manière suivante :

- ***Activité de cryptologie :*** toute activité ayant pour but, la production, l'utilisation, l'importation, l'exportation, ou la commercialisation des moyens de cryptologie.
- ***Agrément*** : la reconnaissance formelle par un organisme agréé, que le produit ou le système évalué peut protéger jusqu'à un niveau déterminé.
- ***Archivage électronique sécurisé :*** l'ensemble des modalités de conservation et de gestion des archives électroniques, destinées à garantir leur valeur juridique pendant toute la durée nécessaire.
- ***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.
- ***Autorité de Protection***: l'Autorité Administrative chargée de veiller à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente loi.

- ***Chiffrement:*** toute technique qui consiste à transformer des données numériques en un format inintelligible en employant des moyens de cryptologie.

- ***Code de conduite*** : la charte d'utilisation élaborée par le responsable du traitement des données à caractère personnel, afin d'instaurer un usage et régulier des ressources informatiques, de l'internet et des communications électroniques de la structure concernée, et qui est préalablement homologuée par l'Autorité de protection.

- ***Commerce électronique*** : l'activité économique par laquelle, une personne propose ou assure, à distance et par voie électronique, la fourniture de biens et la prestation de services.

  Entrent également dans le champ du commerce électronique, les activités de fourniture de services telles que celles consistant à fournir des informations en ligne, des communications commerciales, des outils de recherches, d'accès et de récupération de données, d'accès à un réseau de communication ou d'hébergement d'informations, même s'ils ne sont pas rémunérés par ceux qui les reçoivent.

- ***Communications électroniques :*** 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.

- ***Consentement de la personne concernée*** : toute manifestation de volonté expresse, non équivoque, libre, spécifique et informée, par laquelle la personne concernée ou son représentant légal, judiciaire ou conventionnel, accepte que ses données à caractère personnel fassent l'objet d'un traitement manuel ou électronique.

- ***Conventions secrètes*** : toutes clés non publiées, nécessaires à la mise en œuvre d'un moyen ou d'une prestation de cryptologie pour des opérations de chiffrement ou de déchiffrement.

- ***Courrier électronique*** : tout message, sous forme de texte, de voix, de son ou d'image, envoyé à travers un réseau public de communication, stocké sur un serveur du réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier le récupère.

- ***Cryptologie*** : la science relative à la protection et à la sécurité des informations, notamment pour la confidentialité, l'authentification l'intégrité et la non-répudiation.

- ***Cybercriminalité :*** ensemble des infractions pénales qui se commettent au moyen ou sur un réseau de télécommunications ou un système d'information.

- ***Destinataire d'un traitement de données à caractère personnel*** : toute personne habilitée à recevoir une communication de ce type de données, autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter ces données.

- ***Document :*** le résultat d'une série de lettres, de caractères, de chiffres, de figures ou de tous autres signes ou symboles, qui a une signification intelligible, quel que soient leur média et leurs modalités de transmission.

- ***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 (tout court)*** : toute représentation de faits, d'informations ou de concepts, sous une forme assimilable 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 notamment de communications électroniques/tics, 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 services de communication*** **:** les dispositions techniques prises à cet effet, et la durée du service.

- ***L'identité :*** l'adresse postale ou géographique, le numéro de téléphone ou tout autre numéro d'accès, l'adresse email, 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 relatives 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 service sous-jacent.

- ***Données sensibles*** : toutes données à caractère personnel, relatives aux opinions ou activités religieuses, philosophiques, politique, syndicale, à la vie sexuelle ou raciale, à la santé, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives.

- ***Echange de Données Informatisées (EDI)*** **:** tout transfert électronique d'une information d'un système électronique, à un autre mettant en œuvre une norme convenue pour structurer l'information.

- ***Ecrit :*** toute suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles, ayant une signification intelligible, quelque soient leurs supports et leurs modalités de transmission.

- ***Fichier de Données à Caractère Personnel :*** tout ensemble structuré de données accessibles selon des critères définis, que cet ensemble soit centralisé, décentralisé, ou réparti de manière fonctionnelle ou géographique, afin de permettre l'identification d'une personne déterminée.

- ***Fournisseur de Services :*** Toute personne morale qui fournit au public des services de communications électroniques notamment internet ou des prestations informatiques.

- ***Information :*** tout élément de connaissance, susceptible d'être représenté à l'aide de conventions afin d'être utilisé, conservé, traité ou communiqué. L'information peut être exprimée sous forme écrite, visuelle, sonore, numérique, etc.

- ***Infrastructures critiques*** : les installations physiques et des technologies de l'information et de communications notamment électroniques, 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 social ou économique des citoyens, et/ou le fonctionnement correct ou continu des services de l'Etat.

- ***Interconnexion des Données à Caractère Personnel*** : tout mécanisme de connexion consistant en la mise en relation de données traitées pour une finalité déterminée avec d'autres données traitées pour des finalités identiques ou non, ou liées par un ou plusieurs responsables du traitement desdites données.

- ***Message Electronique :*** Toute information créée, envoyée,reçue ou conservée à travers des moyens électroniques ou optiques ou des moyens analogues, notamment, mais non exclusivement, l'échange de données informatisées (EDI), la messagerie électronique, le télégraphe, le télex, et la télécopie.

- ***Mineur*** : toute personne âgée de moins de 18 ans au sens du Code Pénal guinéen.

- ***Moyens de Cryptologie*** : l'ensemble des outils scientifiques et techniques (matériel ou logiciel) qui permettent de chiffrer et/ou de déchiffrer.
  On entend également par moyens de Cryptologie, tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'écrits ou de signaux, à l'aide de conventions secrètes, ou pour réaliser l'opération inverse avec ou sans convention secrète.

- ***Pays tiers*** : tout Etat non membre de la CEDEAO.

- ***Personne concernée :*** toute Personne physique, qui fait l'objet d'un traitement de données à caractère personnel.

- ***Prestation de Cryptologie*** : toute prestation ou opération, visant à la mise en œuvre, pour le compte de soi-même ou pour autrui, des moyens de cryptologie.

- ***Prestataire de Services de Cryptologie*** : toute Personne, physique ou morale, qui fournit une prestation de cryptologie.

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

- ***Prospection directe*** : tout envoi de message, quel qu'en soit le support ou la nature, notamment commercial, politique ou caritative, destiné à promouvoir,

directement ou indirectement, des biens, des services, ou l'image d'une personne vendant des biens ou fournissant des services.

- ***Racisme et xénophobie en matière de technologies de l'information et de la communication (TICs)*** : 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.

- ***Responsable du traitement :*** la personne physique ou morale, publique ou privée, ou tout autre organisme ou association qui, seul ou conjointement avec d'autres, prend la décision de collecter et de traiter des données à caractère personnel, et en détermine les finalités.

- ***Signature Electronique :*** toute donnée qui résulte de l'usage d'un procédé fiable d'identification, et de nature à garantir son lien avec l'acte auquel elle s'attache.

- ***SMS*** : Sigle anglo-saxon, signifiant 'Short Message Service' (en Français : Service de messagerie court).

- ***Sous-traitant :*** toute personne physique ou morale, publique ou privée, ou tout autre organisme ou association, qui traite des données à caractère personnel pour le compte du responsable du traitement desdites données.

- ***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.

- ***Tiers*** : toute personne physique ou morale, publique ou privée, ou tout autre organisme ou association, autre que la personne concernée, le responsable du traitement, et les personne qui, placés sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilités à traiter les données caractère personnel.

- ***Traitement des données à caractère personnel*** : toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés ou non, et appliquées à des données à caractère personnel, telles que la collecte, l'exploitation, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la sauvegarde, la copie, la consultation, l'utilisation, la communication par la transmission, la diffusion ou toute autre fore de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, le cryptage, l'effacement ou la destruction desdites données ;

- ***Copies temporaires*** : données copiées temporairement dans un espace dédié, pour une durée limitée dans le temps, pour les besoins du fonctionnement du logiciel de traitement ;
- ***Donnée génétique*** : toute donnée concernant les caractères héréditaires d'un individu ou d'un groupe d'individus apparentés ;
- ***Service à distance*** : toute prestation de service à valeur ajoutée, s'appuyant sur les télécommunications et/ou sur l'informatique, visant à permettre, de manière interactive et à distance, à une personne physique ou morale, publique ou privée, la possibilité d'effectuer des activités, démarches ou formalités, etc.

Pour les termes non définis par la présente loi, les définitions données par les instruments juridiques de la CEDEAO, de l'Union Africaine ou de l'Union Internationale des Télécommunications, prévalent sur toutes autres définitions.

CHAPITRE II: OBJET ET CHAMP D'APPLICATION

Article 2: La présente loi a pour objet, de garantir la protection des données à caractère personnel en République de Guinée, en définissant notamment les règles, mécanismes et outils de protection et de gestion desdites données, ainsi que les sanctions aux violations desdites règles, en sus des sanctions prévues par la loi relative à la cybercriminalité.

Article 3: Sont soumises aux dispositions de la présente loi :

- ✓ Toute collecte, tout traitement, toute transmission, tout stockage et toute utilisation des données à caractère personnel par une personne physique, l'Etat, les collectivités locales ou décentralisées, les établissements et Institutions publics, ou par les personnes morales de droit privé ;
- ✓ Tout traitement automatisé ou non de données contenues ou appelées à figurer dans un fichier ;
- ✓ Tout traitement de données mis en œuvre sur le territoire de la République de Guinée ;
- ✓ Tout traitement de données qui concerne la sécurité publique ou nationale, la défense, la recherche et la poursuite d'infractions pénales ou liées à la sûreté de l'Etat, sous réserve des dérogations expressément prévues par des dispositions particulières fixées par d'autres textes de lois en vigueur, en matière de traitement desdites données.

Article 4: Sont exclus du champ d'application de la présente loi :

- ✓ Les traitements de données à caractère personnel mis en œuvre par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques, à condition toutefois que lesdites données ne soient pas destinées à une communication systématique à des tiers ou à la diffusion ;

- ✓ Les copies temporaires faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données à caractère personnel, et à la seule fin de permettre à d'autres destinataires du service, le meilleur accès possible aux informations transmises.

TITRE II :
REGLES RELATIVES AU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

CHAPITRE III : FORMALITES PREALABLES ET NECESSAIRES AU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

Article 5: Le traitement des données à caractère personnel est soumis à une déclaration préalable auprès de l'Autorité compétente désignée par voie règlementaire.

La déclaration doit comporter l'engagement selon lequel, la protection satisfait aux exigences de la présente loi et de tous autres règlementaires ou lois en vigueur en République de Guinée en matière de protection de données à Caractère Personnel.

A l'issue de cette déclaration, l'Autorité compétente délivre un récépissé et le cas échéant, par voie électronique.

Le demandeur peut ensuite mettre en œuvre le traitement dès réception du récépissé. Il n'est toutefois exonéré d'aucune de ses responsabilités.

Les traitements relevant d'un même organisme et ayant des finalités identiques ou liées entre elles, peuvent faire l'objet d'une déclaration unique. Les informations requises au titre de la déclaration, ne sont fournies pour chacun des traitements, que dans la mesure où elles sont propres à ladite déclaration.

CHAPITRE IV:DISPENSE DE FORMALITES PREALABLES POUR LE TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

Article 6: Sont dispensés des formalités de déclaration préalable pour le traitement des données à caractère personnel :

- ✓ Le traitement de données utilisées par une personne physique dans le cadre exclusif de ses activités personnelles, domestiques, ou familiales ;
- ✓ Le traitement de données concernant une personne physique, et dont la publication est prescrite par une disposition légale ou réglementaire ;
- ✓ Le traitement de données, ayant pour seul objet, la tenue d'un registre qui est destiné à un usage exclusivement privé ;

- ✓ Le traitement pour lequel le responsable du traitement a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer de manière indépendante, le respect des obligations prévues dans la présente loi ainsi que tous autres lois ou règlements en vigueur en République de Guinée en matière de protection de données à caractère personnel, à l'exception des cas ou un transfertde données à caractère personnel à destination d'un pays tiers serait envisagé.

CHAPITRE V: MATIERES OU AGISSEMENTS SOUMIS A UNE AUTORISATION PREALABLE AVANT TOUTE MISE EN ŒUVRE

Article 7: Sont soumis à l'Autorisation préalable de l'Autorité compétente avant toute mise en œuvre :

- ✓ Le traitement des données à caractère personnel portant sur des données génétiques, médicales et sur la recherche scientifique dans ces domaines ;
- ✓ Le traitement des données à caractère personnel portant sur des données relatives aux infractions, aux condamnations, ou aux mesures de sûreté prononcées par les juridictions compétentes ;
- ✓ Le traitement des données à caractère personnel portant sur un numéro national d'identification ou tout autre identifiant de la même nature, notamment les numéros de téléphone ;
- ✓ Le traitement des données à caractère personnel comportant des données biométriques ;
- ✓ Le traitement des données à caractère personnel ayant un motif d'intérêt public, notamment à des fins historiques, statistiques ou scientifiques ;
- ✓ Le transfert de données à caractère personnel envisagé à destination d'un pays tiers.

Les demandes de traitement sont présentées par le responsable du traitement ou son représentant légal. Toutefois, l'autorisation n'exonère pas son titulaire (Responsable du traitement) ou le mandataire de celui-ci, de leur responsabilité à l'égard des tiers.

CHAPITRE VI:TRAITEMENT DES DEMANDES D'AVIS, DE DECLARATIONS, ET D'AUTORISATIONS

Article8: Pour les catégories les plus courantes de traitement des données à caractère personnel, notamment celles dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés, l'Autorité compétente peut établir des normes et procédures destinées à simplifier ou à exonérer le responsable du traitement des données à caractère personnel de l'obligation de déclaration préalable.

Article9: La demande d'avis, la déclaration, et la demande d'autorisation, doivent être adressées à l'Autorité compétente, et contenir au minimum les mentions suivantes :

- ✓ L'identité, le domicile, l'adresse géographique et l'adresse postale, le numéro de téléphone, et l'adresse électronique (email, site web) du responsable du traitement des données à caractère personnel ou au cas où celui-ci ne serait pas établi sur le territoire guinéen, celles de son représentant dûment mandaté à cet effet ; et s'il s'agit d'une personne morale, sa dénomination sociale, son siège social, ses coordonnées téléphoniques et adresses électroniques (email, site web), l'identité du dirigeant social, ainsi que celle des associés ou actionnaires, le numéro d'inscription au Registre du commerce et du Crédit Mobilier, son numéro de déclaration ou d'immatriculation fiscale, son numéro d'immatriculation ou de déclaration à la Caisse Nationale de Sécurité Sociale;
- ✓ La ou les finalités du traitement, ainsi que la description détaillée de ses fonctions ;
- ✓ Les interconnexions envisagées ou toutes autres formes de mise en relation avec d'autres traitements ;
- ✓ Les données à caractère personnel traitées, leur origine, ainsi que les catégories de personnes concernées par le traitement ;
- ✓ La durée de conservation des données à caractère personnel traitées ;
- ✓ Le ou les service(s) chargé(s) de mettre en œuvre le traitement ainsi que les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données collectées ;
- ✓ Les destinataires habilités à recevoir la communication des données à caractère personnel traitées ;
- ✓ La fonction de la personne ou le service auprès duquel, s'exerce le droit d'accès;
- ✓ Les dispositions prises pour assurer la sécurité des traitements des données à caractère personnel, la protection et la confidentialité desdites données ;
- ✓ L'indication du recours ou non à un sous-traitant ou du transfert ou non des données à caractère personnel à destination d'un pays tiers.

En cas de changement intervenu dans les mentions précitées à renseigner par le demandeur, que ce soit au cours de l'instruction de la demande ou après la délivrance du récépissé ou de l'autorisation notamment lors de la mise en œuvre du traitement, le responsable du traitement est tenu d'informer immédiatement l'Autorité compétente.

Article10: Les conditions de la présentation de la demande d'autorisation et les procédures d'octroi des autorisations seront fixées par voie règlementaire.

L'Autorité en charge de la Protection des données à caractère personnel pourra toutefois, par décision, exiger des conditions

complémentaires relatives à la présentation de la demande d'autorisation ou de déclaration et aux procédures d'octroi des autorisations.

Article 11: La déclaration ou la demande d'autorisation peut être adressée à l'Autorité en charge de la Protection des Données à Caractère Personnel, par voie Postale, en mains propres dans les locaux de ladite Autorité ou par tout autre moyen contre la remise d'un accusé de réception en bonne et due forme.

Article 12: L'Autorité en charge de la Protection des Données à Caractère Personnel dispose d'un délai de deux (02) mois pour se prononcer (accord ou refus) sur toute Déclaration ou demande d'Autorisation, qui lui est soumise ou adressée.

Ce délai court à compter de la date de réception de la Déclaration et du dépôt de la demande d'Autorisation, ainsi que de la fourniture des pièces, documents, informations exigés pour tout demandeur en vertu des dispositions de la présente loi.

Il peut toutefois être prorogé de deux (02) mois supplémentaires, à condition que l'Autorité en charge de la Protection des Données à Caractère Personnel puisse motiver sa décision ou justifier cette prorogation.

Tout motif ne pouvant être considéré comme valable ou recevable, qu'au regard de manquements ou insuffisances avérés pour la protection des données à caractère personnel de la personne concernée par le traitement, au vu du dossier fourni.

Au-delà de ces délais, toute absence de réponse expresse de la part de l'Autorité en charge de la Protection des Données à Caractère Personnel, équivaut à une acceptation implicite de la déclaration ou à une autorisation tacite accordée au demandeur par ladite Autorité de protection.

En cas de refus par l'Autorité en charge de la Protection des Données à Caractère Personnel à la déclaration ou à la demande d'autorisation présentée par le demandeur (le responsable du traitement des données à caractère personnel), celui-ci peut exercer un recours administratif ou devant la juridiction compétente.

Ce recours n'est toutefois pas suspensif.

Article 13: Les modalités de dépôt des déclarations ou d'octroi des autorisations pour le traitement des données à caractère personnel en conformité avec les dispositions de la présente de la loi, seront fixées par Décret du Président de la République.

CHAPITRE VII:DU CORRESPONDANT A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Article 14: Le correspondant à la Protection des Données à Caractère Personnel, doit être une personne bénéficiant des qualifications requises pour exercer de telles missions. Il doit tenir une liste des traitements effectués immédiatement accessible à toute personne qui en fait la demande, et ne peut faire l'objet d'aucune sanction de la part de son employeur, du fait de l'accomplissement de ses missions.

A défaut, il peut saisir l'Autorité en charge de la Protection des Données à Caractère Personnel en raison des difficultés qu'il rencontre dans l'exercice de ses missions.

Article 15: La désignation du correspondant à la Protection des Données à Caractère Personnel par le responsable du traitement desdites données, doit être notifiée à l'Autorité en charge de la Protection des Données à Caractère Personnel.

Cette désignation doit également être portée à la connaissance des instances représentatives du personnel de l'Employeur.

Article 16: Le profil et les conditions de rémunération du correspondant à la Protection des Données à Caractère Personnel seront fixés par Arrêté du Ministre en charge des Postes, des Télécommunications et de l'Economie Numérique.

En cas de manquement(s) constaté(s) à ses devoirs, correspondant à la Protection des Données à Caractère Personnel, les conditions seront fixées par Arrêté du Ministre en charge des Postes, Télécommunications et de l'Economie Numérique.

Article 17: Les traitements de données à caractère personnel opérés pour le compte de l'Etat, d'une personne morale de droit public ou de droit privé gérant un service public, peuvent être autorisés par voie réglementaire, après avis motivé de l'Autorité en charge de la Protection des Données à Caractère Personnel.

Ces traitements portent notamment sur :

- ✓ la sûreté de l'Etat, la défense nationale ou la sécurité publique;
- ✓ la prévention, la recherche, la constatation, ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté;
- ✓ le recensement de la population;
- ✓ le traitement de salaires, pensions, impôts, taxes, et autres liquidations.

CHAPITRE VIII:PRINCIPES DIRECTEURS DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

Article 18: Le traitement des données à caractère personnel est considéré comme légitime, si la personne concernée donne expressément son consentement préalable.

Toutefois, il peut être dérogé à cette exigence du consentement préalable, lorsque le responsable du traitement est dûment autorisé et que le traitement est nécessaire :

- ✓ soit au respect d'une obligation légale, à laquelle le responsable du traitement est soumis ;
- ✓ soit à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées ;
- ✓ soit à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à sa demande ;
- ✓ soit à la sauvegarde de l'intérêt ou des droits et libertés fondamentaux de la personne concernée.

Article 19: La collecte, l'enregistrement, le traitement, le stockage, la transmission et l'interconnexion des fichiers de données à caractère personnel, doivent se faire de manière licite et loyale.

Article 20: Les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne peuvent être traitées ultérieurement de manière incompatible avec ces finalités.

Elles doivent être adéquates, pertinentes, et non excessives, au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement.

Elles doivent aussi être conservées pendant une durée qui n'excède pas la période nécessaire aux finalités pour lesquelles, elles ont été collectées ou traitées.

Au-delà de cette période requise, les données ne peuvent faire l'objet de conservation, qu'en vue de répondre spécifiquement à un traitement desdites données à des fins historiques, statistiques ou de recherches, en vertu des dispositions de la présente loi ou de toutes autres lois ou règlementations en vigueur en matière de protection de données à caractère personnel.

Article 21: Les données collectées doivent être exactes, et si nécessaire, mises à jour.

Toute mesure ou solution raisonnable doit être mise en œuvre, afin que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement, soient effacées ou rectifiées.

Article 22: Le principe de transparence implique une information obligatoire et claire de la part du responsable du traitement des données à caractère personnel.

Article 23: Les données à caractère personnel doivent être traitées de manière confidentielle et être protégées, notamment lorsque le traitement de ces données comporte des transmissions de données dans un réseau.

Article 24: Lorsque le traitement des données à caractère personnel est mis en œuvre pour le compte du responsable du traitement desdites données, celui-ci doit choisir un sous-traitant qui soit en mesure d'apporter des garanties pour la protection et la confidentialité des données.

Il incombe au responsable du traitement des données à caractère personnel ainsi qu'au sous-traitant, de veiller au respect des dispositions de la présente loi.

Article 25: Le traitement des données à caractère personnel réalisé aux fins de journalisme, de recherche, d'expression artistique ou littéraire est admis lorsqu'il est mis en œuvre aux seules fins d'expression littéraire et artistique ou d'exercice, à titre professionnel, de l'activité de journaliste ou de chercheur, dans le respect des règles déontologiques de ces professions.

Article 26: Les dispositions de la présente loi, ne font pas obstacle à l'application des dispositions des lois relatives à la presse écrite ou au secteur de l'audiovisuel et du Code Pénal en vigueur en République de Guinée, qui auraient prévu les conditions d'exercice du droit de réponse et qui préviennent, limitent, réparent et, le cas échéant, répriment les atteintes à la vie privée et à la réputation des personnes physiques.

Article 27: Aucune décision de justice impliquant une appréciation sur le comportement d'une personne physique ne peut avoir pour fondement, un traitement automatisé des données à caractère personnel destiné à évaluer certains aspects de sa personnalité.

Aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement, un traitement automatisé des données à caractère personnel donnant une définition du profil ou de la personnalité de l'intéressé.

Article 28: Le responsable d'un traitement des données à caractère personnel ne peut être autorisé à transférer lesdites données vers un pays tiers, que si l'Etat assure un niveau de protection supérieur ou équivalent de la vie privée, des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font ou peuvent faire l'objet .

Avant tout transfert effectif des données à caractère personnel vers ce pays tiers, le responsable du traitement desdites données doit obtenir au

préalable l'autorisation de l'Autorité de Protection des Données à Caractère Personnel.

Tout transfert de données à caractère personnel vers un pays tiers fait l'objet d'un contrôle strict et régulier par l'Autorité de Protection des Données à Caractère Personnel, au regard de leur finalité.

Article 29: L'interconnexion des fichiers n'est autorisée, que si elle permet d'atteindre les objectifs légaux ou statutaires présentant un intérêt légitime pour les responsables des traitements des données à caractère personnel.

Elle ne peut et ne doit pas entraîner de discrimination ou de réduction des droits, libertés et garanties pour les personnes concernées, ni être assortie de mesures de sécurité inappropriées.

Elle doit en outre tenir compte du principe ou de l'exigence de pertinence des données faisant l'objet de l'interconnexion.

CHAPITRE IX: DROITS DE LA PERSONNE CONCERNEE PAR LE TRAITEMENT DES DONNEES A CARACTERE PERSONNEL ET EXCEPTIONS A CES DROITS

Article 30: Le responsable du traitement des données à caractère personnel est tenu de fournir à la personne dont les données font l'objet d'un traitement, au plus tard à l'occasion de la collecte et quels que soient les moyens et supports employés, les informations suivantes :

- ✓ son identité et, le cas échéant, celle de son représentant dûment mandaté ;
- ✓ la ou les finalité(s) déterminée(s) du traitement auquel les données sont destinées ;
- ✓ les catégories de données concernées ;
- ✓ le ou les destinataire(s) au(x) quel(s), les données sont susceptibles d'être communiquées ;
- ✓ la possibilité de refuser de figurer sur le fichier en cause ;
- ✓ l'existence d'un droit d'accès aux données qui concernent la personne, et d'un droit de rectification de ces données ;
- ✓ la durée de conservation des données ;
- ✓ l'éventualité de tout transfert des données, à destination d'un pays tiers.

Article 31: Toute personne physique dont les données à caractère personnel font l'objet d'un traitement, peut demander sous forme de questions et obtenir du responsable de ce traitement :

- ✓ les informations permettant de connaître et de contester le traitement ;
- ✓ la confirmation que des données à caractère personnel qui la concernent, font ou ne font pas l'objet de ce traitement ;

- ✓ la communication des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;
- ✓ des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires, auxquels les données sont communiquées.

En cas d'impossibilité d'accès de la personne concernée, le droit d'accès peut être exercé par l'Autorité en charge de la Protection des Données à Caractère Personnel qui dispose d'un pouvoir d'investigation en la matière, et qui peut ordonner la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme aux exigences de la présente loi

L'Autorité en charge de la Protection des Données à Caractère Personnel doit ensuite communiquer à la personne concernée, les résultats de ses investigations.

Le responsable du traitement des données à caractère personnel peut néanmoins, s'opposer aux demandes manifestement abusives émanant de la même personne concernée ; abus matérialisés par le nombre, le caractère répétitif ou systématique des demandes.

En cas de contestation, la charge de la preuve du « caractère manifestement abusif » des demandes, incombe au responsable du traitement des données, auprès duquel elles sont adressées.

Article 32: Toute personne physique concernée par un traitement de ses données à caractère personnel a le droit :

- ✓ de s'opposer, pour des motifs légitimes tenant à sa situation particulière, à ce que des données à caractère personnel qui la concernent fassent l'objet d'un traitement, sauf en cas de dispositions légales prévoyant expressément le traitement.
- ✓ En cas d'opposition légitime, le traitement mis en œuvre par le responsable du traitement des données, ne peut porter sur les données en cause ;
- ✓ de s'opposer, sur sa demande et gratuitement, au traitement de données à caractère personnel qui la concernent, et destinées à des fins de prospection ;
- ✓ d'être informée avant que des données à caractère personnel qui la concernent, ne soient pour la première fois, communiquées à des tiers ou utilisées pour le compte de tiers, à des fins de prospection, et de se voir accorder expressément le droit de s'opposer, gratuitement, à ladite communication ou utilisation.

Article 33: Toute personne physique justifiant, de son identité, peut exiger du responsable d'un traitement de données à caractère personnel, que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou supprimées les données à caractère personnel qui la concernent, et qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation, est interdite.

Article 34: Les ayant-droits d'une personne décédée justifiant de leur identité, peuvent, si des éléments portés à leur connaissance les laissent présumer que les données à caractère personnel qui la concernent et faisant l'objet d'un traitement, n'ont pas été actualisées, exiger du responsable du traitement desdites données, qu'il prenne en considération le décès et procède aux mises à jour qui doivent être conséquemment faites.

Lorsque les ayant-droits en font la demande, le responsable du traitement des données à caractère personnel doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations requises en vertu de l'Alinéa 1er du présent Article.

Article 35: La personne concernée par le traitement des données à caractère personnel a le droit d'obtenir du responsable du traitement desdites données, l'effacement des données qui la concernent, et la cession de la diffusion de ces données, en particulier en ce qui concerne des données à caractère personnel, que la personne concernée avait rendues disponibles lorsqu'elle était mineure, ou pour l'un des motifs suivants :

- ✓ les données ne sont plus nécessaires, au regard des finalités pour lesquelles elles ont été collectées ou traitées ;
- ✓ la personne concernée par le traitement des données à caractère personnel a retiré le consentement sur lequel est fondé le traitement ou lorsque le délai de conservation autorisé a expiré, et qu'il n'existe pas d'autre motif légal au traitement des données ;
- ✓ la personne concernée par le traitement des données à caractère personnel s'oppose au traitement desdites données qui la concernent, lorsqu'il n'existe pas de motif légal audit traitement ;
- ✓ le traitement des données à caractère personnel n'est pas conforme aux dispositions de la présente loi ; ou
- ✓ pour tout autre motif légitime.

Article 36: Lorsque le responsable du traitement des données à caractère personnel a rendues publiques les données à caractère personnel de la personne concernée par le traitement, il doit prendre toutes les mesures raisonnables, y compris les mesures techniques, en ce qui concerne les données publiées sous sa responsabilité, en vue d'informer les tiers qui traitent lesdites données, qu'une personne concernée par leur traitement, leur demande d'effacer tous liens vers ces données à caractère personnel, ou toute copie ou reproduction de celles-ci.

Lorsque le responsable du traitement a autorisé un tiers à publier des données à caractère personnel de la personne concerne par le traitement, il est réputé responsable de cette publication, et doit à cet effet, prendre toutes les mesures appropriées, pour mettre en œuvre le

droit à l'oubli numérique et à l'effacement des données à caractère personnel.

Article 37: Le responsable du traitement des données à caractère personnel doit procéder, sans délai, à l'effacement, sauf lorsque la conservation des données à caractère personnel est nécessaire :

- ✓ soit, à l'exercice du droit à la liberté d'expression ;
- ✓ soit, pour des motifs d'intérêt général dans le domaine de la santé publique, conformément à la loi ;
- ✓ soit, au respect d'une obligation légale de conserver les données à caractère personnel, prévue en vertu de la présente loi ou de toutes autres lois régissant les données à caractère personnel en République de Guinée, et à laquelle le responsable du traitement des dites données est soumis.

Article 38: Le responsable du traitement des données à caractère personnel doit mettre en place des mécanismes appropriés, visant à assurer la mise en œuvre du respect du droit à l'oubli numérique et à l'effacement desdites données.

Il doit également examiner de manière périodique, la nécessité ou non de conserver les données à caractère personnel, conformément aux dispositions de la présente loi.

Lorsque l'effacement des données à caractère personnel est effectué, le responsable du traitement desdites données ne doit procéder à aucun autre traitement de ces données.

Article 39: L'Autorité de Protection des données à caractère personnel doit adopter des mesures et des lignes directrices, aux fins de préciser :

- ✓ les conditions de la suppression des liens vers ces données à caractère personnel, des copies ou des reproductions de celles-ci existant dans les services de communications électroniques accessibles au public ;
- ✓ les conditions et critères applicables à la limitation du traitement des données à caractère personnel.

Article 40: Lorsque les données à caractère personnel font l'objet d'un traitement automatisé dans un format structuré et couramment utilisé, la personne concernée par le traitement des données a le droit d'obtenir du responsable du traitement desdites données, une copie des données faisant l'objet du traitement automatisé, dans un format électronique structuré qui est couramment utilisé et qui permet la réutilisation de ces données par la personne concernée.

Lorsque la personne concernée par le traitement des données à caractère personnel a fourni lesdites données, et que le traitement est fondé sur son consentement préalable ou sur un contrat, elle a le droit de transmettre ces données à caractère personnel et toutes autres informations qu'elle a

fournies et qui sont conservées par un système de traitement automatisé à un autre système dans un format électronique qui est couramment utilisé, sans que le responsable du traitement auquel les données à caractère personnel sont retirées, n'y fasse obstacle.

L'Autorité en charge de la Protection des Données à Caractère Personnel peut préciser le format électronique, ainsi que les normes techniques, les modalités et les procédures relatives à la transmission de données à caractère personnel.

CHAPITRE X: OBLIGATIONS DES RESPONSABLES DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL, ET DE LEURS SUBORDONNES ET PREPOSES

Article 41: Le traitement des données à caractère personnel est confidentiel. Il doit être effectué exclusivement par des personnes qui agissent sous l'autorité du responsable du traitement desdites données, et seulement sur ses instructions.

Article 42: Le responsable du traitement des données à caractère personnel est tenu de prendre toutes les précautions utiles, au regard de la nature des données, et notamment, pour empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

Lorsque le traitement des données à caractère personnel est mis en œuvre pour le compte du responsable du traitement desdites données, celui-ci doit choisir un sous-traitant qui apporte ou satisfait à toutes les exigences de garantie, au regard des mesures de sécurité technique et d'organisation relatives au traitement à effectuer.

Il incombe au responsable du traitement des données, ainsi qu'au sous-traitant, de veiller au respect de ces mesures.

Article 43: Le responsable du traitement des données à caractère personnel est tenu :

- ✓ d'empêcher toute personne non autorisée, d'accéder aux installations utilisées pour le traitement des données ;
- ✓ d'empêcher que des supports de données puissent être lus, copiés, modifiés ou déplacés par une personne non autorisée ;
- ✓ d'empêcher l'introduction non autorisée de toute donnée dans le système d'information, ainsi que toute prise de connaissance, toute modification ou tout effacement non autorisés de données enregistrées ;
- ✓ d'empêcher que des systèmes de traitement de données puissent être utilisés par des personnes non autorisées, à l'aide d'installations de transmission de données ;

- ✓ d'empêcher que des systèmes de traitement de données soient utilisés à des fins de blanchiment de capitaux et de financement du terrorisme, ou d'infractions à la sûreté de l'Etat ou à l'ordre et à la sécurité publics ;
- ✓ de garantir que, lors de l'utilisation d'un système de traitement automatisé de données, les personnes autorisées ne puissent accéder qu'aux données relevant ou couvertes par leur autorisation ;
- ✓ de garantir que puisse être vérifiée et constatée, l'identité des tiers auxquels des données peuvent être transmises par des installations de transmission ;
- ✓ de garantir que puisse être vérifiée et constatée à posteriori, l'identité des personnes ayant eu accès au système d'information contenant des données à caractère personnel, la nature des données qui ont été introduites, modifiées, altérées, copiées, effacées ou lues dans le système, le moment auquel ces données ont été manipulées ;
- ✓ d'empêcher que lors de la communication de données et du transport de support de données, les données puissent être lues, copiées, modifiées, altérées ou effacées, sans autorisation préalable ;
- ✓ de sauvegarder les données par la constitution de copies de sécurité protégées. Le responsable du traitement doit mettre en œuvre toutes les mesures techniques et l'organisation appropriées, afin d'assurer la protection des données à caractère personnel qu'il traite contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés des données, notamment lorsque le traitement des données comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.

Article 44: Le responsable du traitement des données à caractère personnel est tenu d'établir un rapport annuel à l'attention de l'Autorité en charge de la Protection des Données à Caractère Personnel sur le respect des dispositions énoncées pertinentes de la présente loi.

Article 45: Les données à caractère personnel doivent être conservées pendant une durée fixée par l'Autorité en charge de la Protection des Données à Caractère Personnel en fonction des finalités de chaque type de traitement pour lesquelles elles ont été recueillies, conformément aux textes en vigueur.

Article 46: Le responsable du traitement des données à caractère personnel est tenu de prendre toute mesure utile pour s'assurer que les données à caractère personnel traitées, peuvent être exploitées, quel que soit le support technique utilisé.

TITRE III
DISPOSITIONS INSTITUTIONNELLES

CHAPITRE XI:DE L'AUTORITE CHARGEE DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Article 47: L'Autorité en charge de la protection des données à caractère personnel sera créée par voie règlementaire.

Article 48: Cette Autorité en charge de la Protection des Données à Caractère Personnel devra veiller à ce que le traitement des données à caractère personnel soit mis en œuvre conformément aux dispositions de la présente loi ou de toutes autres législations et réglementations en vigueur en République de Guinée en matière de protection de données à caractère personnel.

Elle devra, en outre, s'assurer que l'usage des technologies de l'information et de la communication ne porte pas atteinte ou ne comporte pas de menaces pour les libertés et la vie privée pour l'ensemble des utilisateurs desdites technologies à l'échelle du territoire de la République de Guinée.

A ce titre, elle sera notamment chargée :

- ✓ d'informer les personnes concernées par le traitement de leurs données à caractère personnel ainsi que les responsables du traitement desdites données de leurs droits et obligations ;
- ✓ de répondre à toute demande d'avis portant sur un traitement de données à caractère personnel ;
- ✓ d'établir un règlement intérieur qui précise, notamment les règles relatives aux délibérations, à l'instruction et à la présentation des dossiers ;
- ✓ de recevoir les déclarations, et d'octroyer les autorisations pour la mise en œuvre des traitements de données à caractère personnel, ou de les retirer, selon les cas prévus par la présente loi ;
- ✓ de recevoir les réclamations et les plaintes relatives à la mise en œuvre des traitements de données à caractère personnel, et d'informer les auteurs, de la suite accordée à ces plaintes ou réclamations ;
- ✓ d'informer, sans délai, l'autorité judiciaire compétente des infractions dont elle a connaissance dans le cadre de ses missions ;
- ✓ de déterminer les garanties indispensables et les mesures appropriées pour la protection des données à caractère personnel ;
- ✓ de procéder, par le biais d'agents assermentés, à des vérifications relatives à tout traitement de données à caractère personnel ;
- ✓ de prononcer des sanctions administratives et pécuniaires, à l'égard des responsables de traitement de données et/ou à leurs préposés, subordonnés ou sous-traitants qui ne se conforment pas aux dispositions de la présente loi ;

- ✓ de mettre à jour et à la disposition du public pour consultation, un répertoire des traitements de données à caractère personnel ;
- ✓ de conseiller les personnes et organismes qui font les traitements de données à caractère personnel ou qui procèdent à des essais ou expérimentations en la matière ;
- ✓ de donner son avis sur tout projet de texte juridique, notamment de loi, de règlement, traité, convention, en rapport avec la protection des libertés et de la vie privée ;
- ✓ d'élaborer des règles de conduites relatives au traitement et à la protection des données à caractère personnel ;
- ✓ de participer aux activités de recherche scientifique, de formation et d'étude, en rapport avec la protection des données à caractère personnel, et de manière générale, les libertés et la vie privée ;
- ✓ d'autoriser, à certaines conditions déterminées par Décret du Président de la République, les transferts transfrontaliers de données à caractère personnel ;
- ✓ de faire des propositions susceptibles de simplifier et d'améliorer le cadre législatif et réglementaire régissant le traitement et la protection des données à caractère personnel ;
- ✓ d'initier et mettre en œuvre tous les mécanismes nécessaires et utiles afin de renforcer la coopération avec les Autorités de la protection des données à caractère personnel d'autres pays et/ou les organisations sous-régionales, continentales ou internationales compétentes dans ce domaine ;
- ✓ de participer aux réunions, séminaires, conférences et autres cadres de négociations internationales en matière de traitement et de protection des données à caractère personnel ;
- ✓ d'établir et de remettre un rapport au Ministre des Postes, des Télécommunications et de l'Economie Numérique, au Ministre de la Justice, au Ministre de la Sécurité, à toute autre institution légitimement ou légalement intéressée, et éventuellement à la disposition du public ;

Article 49: Le Prestataire de services de cryptologie ne peut opposer à l'Autorité de la Protection des Données à Caractère Personnel, le secret professionnel auquel il est soumis en vertu des dispositions légales ou conventionnelles.

De même, le responsable du traitement de données à caractère personnel services ne peut opposer à l'Autorité de la Protection des Données à Caractère Personnel, le secret professionnel auquel il est assujetti.

TITRE IV
SANCTIONS ADMINISTRATIVES ET PENALES AUX VIOLATIONS DES DISPOSITIONS DE LA PRESENTE LOI ET EN CAS DE RECIDIVE

CHAPITRE XII: SANCTIONS ADMINISTRATIVES

Article 50: L'Autorité en charge de la Protection des Données à Caractère Personnel peut prononcer à l'encontre du responsable du traitement de données à caractère personnel les mesures suivantes :

- ✓ un avertissement à l'égard dudit responsable qui ne respecte pas les obligations résultant de la présente loi à laquelle il est assujetti ;
- ✓ une mise en demeure ou sommation de cesser ou faire cesser les manquements constatés et ce, dans le délai que ladite Autorité de Protection aura fixé.

Article 51: Lorsque la mise en œuvre d'un traitement de données à caractère personnel entraîne une violation des droits et libertés, l'Autorité en charge de la Protection des Données à Caractère Personnel peut, à l'issue d'une procédure contradictoire, décider :

- ✓ de l'interruption de la mise en œuvre dudit traitement de données à caractère personnel ;
- ✓ du verrouillage de certaines données à caractère personnel déjà traitées ;
- ✓ de l'interdiction temporaire ou définitive d'un traitement contraire aux dispositions de la présente loi.

Article 52: L'Autorité en charge de la Protection des Données à Caractère Personnel peut, après avoir entendu le responsable du traitement ou son sous-traitant qui ne se conforme pas aux dispositions prévues de la présente loi et à la mise en demeure qui lui a été adressée, prononcer à son encontre, les sanctions suivantes :

- ✓ le retrait provisoire de l'autorisation accordée ;
- ✓ le retrait définitif de l'autorisation accordée ;
- ✓ une sanction pécuniaire (amende), dont le montant devra toutefois être proportionnel à la gravité des manquements commis et aux avantages tirés de ce manquement.

Article 53: Les modalités de retrait de l'autorisation précitée, seront fixées par Décret du Président de la République.

CHAPITRE XIII: SANCTIONS PENALES

Article 54: Est interdit et puni de la réclusion criminelle de dix (10) ans à vingt (20) ans et d'une amende de 300.000.000 à 600.000.000. Francs Guinéens, le fait de procéder ou tenter de procéder à la collecte et à tout traitement de données à caractère personnel qui révèlent l'origine ethnique, raciale, ou régionale, la filiation, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la vie sexuelle, les données génétiques ou plus généralement celles relatives à l'état de santé de la personne concernée. Cette infraction est constitutive d'un délit.

La tentative de commission de cette infraction et la complicité de sa commission sont punies des mêmes peines.

Toutefois, cette interdiction ne s'applique pas :

- ✓ lorsque le traitement des données à caractère personnel porte sur des données manifestement rendues publiques par la personne concernée ;
- ✓ lorsque le traitement des données génétiques ou relatives à l'état de santé est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée, se trouve dans l'incapacité physique ou juridique de donner son consentement ;
- ✓ lorsque le traitement, notamment des données génétiques, est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice de la personne concernée ;
- ✓ lorsqu'une procédure judiciaire ou une enquête pénale est ouverte. Dans ce cas, le traitement des données à caractère personnel n'est poursuivi, que pour la constatation des faits ou la manifestation de la vérité ;
- ✓ lorsque le traitement est effectué dans le cadre des activités légitimes d'une fondation, d'une association, ou de tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse, mutualiste, ou syndicale.
- ✓ Mais, le traitement doit concerner les seuls membres de cet organisme ou les personnes entretenant avec celui-ci, des contacts réguliers liés à sa finalité.
- ✓ Aussi, les données ne doivent pas être communiquées à des tiers, sans le consentement des personnes concernées.

Tous ces cas de traitement de données à caractère personnel doivent être autorisés et contrôlés dans leur conception et leur mise en œuvre par l'Autorité en charge de la Protection des Données à Caractère Personnel.

Article 54: Est interdit et puni d'une peine d'emprisonnement de un (1) an à cinq (5) ans et d'une amende de 30.000.000 à 200.000.000 Francs Guinéens, le fait de procéder ou tenter de procéder 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 par écrit son consentement préalable à recevoir de telles prospections ou qui s'y est formellement opposée.

La tentative de commission de cette infraction et la complicité pour sa commission, sont punies des mêmes peines.

Article 55: Est puni d'une peine d'emprisonnement de six (6) mois à trois (3) ans et d'une amende de 20.000.000 à 150.000.000 Francs Guinéens, quiconque entrave ou tente d'entraver l'action de l'Autorité en charge de la Protection des Données à Caractère Personnel, ou ne se conforme pas aux décisions et injonctions prises par ladite Autorité, notamment en :

- ✓ s'opposant à l'exercice des missions confiées aux membres ou aux agents habilités de l'Autorité en charge de la Protection, en application des dispositions de la présente loi ;
- ✓ en refusant de communiquer aux membres ou aux agents habilités de l'Autorité en charge de la Protection, les renseignements ou documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître ;
- ✓ communiquant des informations qui ne sont pas conformes au contenu des enregistrements tel qu'il était au moment où la demande a été formulée ou qui ne présente pas ce contenu sous une forme directement accessible.

Tout complice de la commission ou de la tentative de commission de cette infraction sera puni des mêmes peines.

Le Procureur de la République ou le Juge compétent doit être informé, sans délai, des entraves aux actions notamment des décisions de l'Autorité en charge de la Protection des Données à Caractère Personnel, et celui-ci, dès que saisi, doit prendre toutes les mesures appropriées pour mettre fin à ces entraves, et de poursuivre l'auteur et tout complice.

Article 56 : Tout responsable de traitement de données ou son sous-traitant, subordonné ou préposé qui ne respecte pas les dispositions de la présente loi, sera puni d'une amende de 50.000.000 à 150.000.000 Francs Guinéens.

En cas de récidive dans les cinq (5) années suivant la date à laquelle l'amende indiquée à l'alinéa 1er du présent Article est devenue définitive, cette amende est portée à un montant qui ne peut excéder 1.500.000.000 Francs Guinéens; et s'il s'agit d'une entreprise, cette amende est portée à un montant qui ne peut excéder 7% du chiffre d'affaire hors taxes du dernier exercice clos de l'entreprise.

Article 57: Les modalités de recouvrement des sanctions pécuniaires décidées par l'Autorité en charge de la Protection des Données à Caractère Personnel seront fixées par voie réglementaire.

CHAPITRE XIII: SANCTIONS EN CAS DE RECIDIVE

Article 58: En cas de récidive aux infractions prévues dans le cadre de la présente loi, les sanctions administratives et pénales prévues par ladite loi ou selon le cas par la loi sur la cybercriminalité pour les infractions liées aux données à caractère personnel, pourront être aggravées à la discrétion de l'Autorité en charge de la Protection des Données à Caractère Personnel ou de l'autorité judiciaire compétente.

Selon la nature de l'infraction, les peines d'emprisonnement et les amendes prévues par l'une des lois précitées, pourront être portées au double pour la peine de prison, et les amendes seront alourdies, au double si l'auteur de l'infraction ou tout complice est une personne physique, et du double au quintuple, s'il s'agit d'une personne morale.

CHAPITRE XIV: SANCTIONS ADDITIONNELLES ET PUBLICATION DES SANCTIONS

Article 59: Selon la gravité de l'infraction et l'ampleur du préjudice, des sanctions additionnelles de même nature ou du même ordre que celles prévues par la loi sur la cybercriminalité, pourront être prononcées par l'Autorité de Protection des Données à Caractère Personnel ou de l'autorité judiciaire compétente.

Article 60 : Les sanctions (pécuniaires, de prison, ou administratives) prononcées à l'encontre des auteurs (personnes morales ou physiques) d'infractions aux dispositions de la présente loi ou de leurs complices ou des dispositions de la loi sur la cybercriminalité relatives aux infractions en matière de données à caractère personnel devront être publiées au moins au journal officiel de la République, sur le site internet de l'Autorité de Protection des Données à Caractère Personnel, de la structure chargée de la lutte contre la cybercriminalité (CERT), dans un journal d'information ou d'annonces légales, au greffe de la juridiction compétente et sur tout autre support électronique; et ce, aux frais de la personne condamnée (pour les deux derniers supports).

Article 61: Outre les sanctions prévues par la présente loi, les infractions en matière de données à caractère personnel peuvent également être réprimées par les sanctions pertinentes prévues en la matière par la loi sur la cybercriminalité en vigueur en République de Guinée.

L'Autorité en charge de la Protection des Données à Caractère Personnel peut au-delà des sanctions prévues par la présente loi, et sans que cela ne constitue une atteinte aux prérogatives du Centre national de sécurité des systèmes d'information (CERT), également prononcer toutes sanctions pécuniaires ou administratives prévues par la loi sur la cybercriminalité en matière d'infractions aux données à caractère personnel, à l'encontre de tout auteur et complice de violation des règles prévues en cette matière par ladite loi, au seul cas où l'unité ou l'institution guinéenne en charge de la lutte contre la cybercriminalité (CERT) ou l'autorité judiciaire compétente, n'aurait pas encore prononcé les sanctions prévues pour l'infraction commise.

TITRE V

PRESCRIPTIONS EN MATIERE D'INFRACTIONS

Article 62 : Les délais de prescription concernant les infractions ou atteintes en matière de données à caractère personnel, suivent le même régime que ceux prévus par les Codes Pénal et de Procédure Pénal en vigueur en République de Guinée. A défaut, ceux-ci seront déterminés par un Décret du Président de la République.

TITRE VI

DISPOSITIONS FINALES

Article 63 : Les responsables du traitement des données à caractère personnel disposent d'un délai maximum d'un (1) an, à compter de la date de promulgation de la présente loi, pour se mettre en conformité avec les dispositions de ladite loi.

Article 64 : Les modalités d'application non précisées pour les autres dispositions de la présente loi seront précisées par des textes d'application (Décrets, Arrêtés, Décisions...) pris par l'autorité compétente.

Article 65 : La présente loi qui abroge toutes dispositions antérieures contraires et entre en vigueur à compter de la date de sa promulgation, sera enregistrée et publiée au Journal Officiel de la République de Guinée, et exécutée comme loi de l'Etat.

Conakry, le 28 JUIL. 2016 **.....2016**

Prof. Alpha CONDE