REPUBLIQUE DU NIGER

Fraternité- Travail-Progrès

ASSEMBLEE NATIONALE

Loi n°

du

portant répression de la cybercriminalité au Niger

Vu la Constitution du 25 novembre 2010 ;

Vu la Directive C/DIR/1/08/11, portant lutte contre la cybercriminalité dans l'espace de la Communauté économique des Etats de l'Afrique de l'Ouest (CEDEAO) du 19 août 2011 ;

Vu la Convention du Conseil de l'Europe du 23 novembre 2001 sur la cybercriminalité ;

Vu la loi n° 61-27 du 15 juillet 1961, portant institution du Code pénal et ses textes modificatifs subséquents ;

Vu la loi n° 61-33 du 14 août 1961, portant institution du Code de procédure pénale et ses textes modificatifs subséquents **;**

Vu la loi uniforme n° 2008-48 du 3 septembre 2008 de l'UEMOA relative à la répression des infractions en matière de chèque, de carte bancaire et d'autres instruments et procédés électroniques de paiement **;**

Vu l'acte additionnel A/SA.2/01/11 du 16 février 2010 relatif à la protection des données à caractère personnel.

L'ASSEMBLEE NATIONALE A DELIBERE ET ADOPTE, EN SA SEANCE PLENIERE DU LUNDI 25 JUIN 2019, LA LOI DONT LA TENEUR SUIT :

TITRE I : DES INCRIMINATIONS ET DES PEINES

Chapitre premier – Dispositions générales

Article premier : Définitions

Au sens de la présente loi, on entend par :

« Cybercriminalité » : l'ensemble des infractions pénales qui se commettent au moyen ou sur réseau de télécommunication ou un système d'information ;

« Preuve électronique » : Tout écrit sous forme électronique, admis en preuve au même titre que l'écrit sur support papier et possédant la même force probante que celui-ci, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité et la pérennité ;

« Système informatique » : tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent en exécution d'un programme, un traitement automatisé de données.

« Communication électronique » : toute transmission, toute émission ou toute réception de signes, de signaux, d'écrits, d'images, de sons, de données ou de renseignements de toute nature par câble en cuivre, fibres optiques, radioélectricité ou autres systèmes électromagnétiques.

« Données informatiques » : toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction.

« Données relatives aux abonnés » : toute information, contenue sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de service et qui se rapporte aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir :

- le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;
- l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de service ;
- toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de service.

« Données relatives au trafic » : toutes données ayant trait à une communication passant par un système informatique, 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 du service sous-jacent.

« Fournisseur de service »: toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ;

Toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.

« Technologies de l'information et de la communication (TIC)» : les technologies employées pour recueillir, stocker, utiliser et transmettre des informations ainsi que celles qui impliquent l'utilisation des ordinateurs ou de tout système de communication y compris de télécommunication.

« Pornographie enfantine » : toute matière pornographique, quel que soit le support, notamment visuel ou sonore, représentant :

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

« Mineur » : toute personne âgée de moins de 18 ans.

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

Article 2 : objet et champ d'application

La présente loi a pour objet de fixer les règles applicables à la cybercriminalité ou à tout autre fait illégal commis au moyen d'un système informatique. A ce titre, elle prévoit les infractions et les procédures relatives aux technologies de l'information et de la communication, dans le respect des droits et libertés individuelles.

Chapitre II : incriminations et sanctions

Section 1 : Infractions spécifiques aux technologies de l'information et de la communication

Paragraphe premier : Infractions relatives aux systèmes informatiques

Article 3 : Accès illégal

Est puni d'une peine d'emprisonnement de un (1) à trois (3) ans et d'une amende de cinq cent mille (500 000) à un million (1 000 000) de francs CFA, quiconque accède, intentionnellement et sans droit, à tout ou partie d'un système informatique.

Lorsqu'il en résulte soit la suppression, la modification ou l'altération des données informatiques contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement est de trois (3) à cinq (5) ans et l'amende de deux millions (2 000 000) à cinq millions (5 000 000) de francs CFA.

Article 4 : Maintien frauduleux

Est puni d'une peine d'emprisonnement de un (1) à trois (3) ans et d'une amende de cinq cent mille (500 000) à un million (1 000 000) de francs CFA, quiconque se maintient, intentionnellement et sans droit, dans tout ou partie d'un système informatique.

Lorsqu'il en résulte soit la suppression, la modification ou l'altération des données contenues dans le système informatique, soit une altération du fonctionnement de ce système, l'emprisonnement est de trois (3) à cinq (5) ans et l'amende de deux millions (2 000 000) à cinq millions (5 000 000) de francs CFA.

<u>Article 5</u> : Entrave et action de fausser le fonctionnement du système informatique

Est puni d'une peine d'emprisonnement de deux (2) à cinq (5) ans et d'une amende de cinq millions (5 000 000) à vingt millions (20 000 000) de francs CFA, quiconque entrave, intentionnellement et sans droit, le fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération et la suppression de données informatiques.

Est puni des mêmes peines, quiconque fausse le fonctionnement d'un système informatique.

<u>Article 6</u> : Introduction frauduleuse de données informatiques dans un système informatique

Est puni d'une peine d'emprisonnement de deux (2) à cinq (5) ans et d'une amende de cinq millions (5 000 000) à vingt millions (20 000 000) de francs CFA, quiconque introduit, intentionnellement et sans droit, des données informatiques dans un système informatique.

<u>Paragraphe 2</u> : Infractions relatives aux données informatiques

<u>Article 7</u> : Interception illégale

Est puni d'une peine d'emprisonnement de deux (2) à cinq (5) ans et d'une amende de un million (1 000 000) à cinq millions (5 000 000) de francs CFA, quiconque intercepte, intentionnellement et sans droit, par des moyens techniques, des données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques.

<u>Article 8</u> : Atteinte à l'intégrité des données

Est puni d'une peine d'emprisonnement de deux (2) à cinq (5) ans et d'une amende de cinq millions (5 000 000) à vingt millions (20 000 000) de francs CFA, quiconque endommage, efface, détériore, altère, modifie ou supprime, intentionnellement et sans droit, des données informatiques.

<u>Paragraphe 3</u> : Infractions informatiques

<u>Article 9</u> : Falsification informatique

Est puni d'une peine d'emprisonnement de cinq (5) à moins de dix (10) ans et d'une amende de cinq millions (5 000 000) à vingt millions (20 000 000) de francs CFA, quiconque introduit, altère, modifie, efface ou supprime, intentionnellement et sans droit, des données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles.

<u>Article 10</u> : Usage des données falsifiées

Est puni d'une peine d'emprisonnement de cinq (5) à moins de dix (10) ans et d'une amende de cinq millions (5 000 000) à vingt millions (20 000 000) de francs CFA, quiconque fait usage, intentionnellement et sans droit, des données obtenues dans les conditions prévues à l'article 9 de la présente loi.

<u>Article 11</u> : Fraude informatique

Est puni d'une peine d'emprisonnement de cinq (5) à moins de dix (10) ans et d'une amende de cinq millions (5 000 000) à vingt millions (20 000 000) de francs CFA, quiconque cause, intentionnellement et sans droit, un préjudice patrimonial à autrui par l'introduction, l'altération, la modification, l'effacement ou la suppression de données informatiques ou par toute forme d'atteinte au fonctionnement d'un système informatique, dans l'intention frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

<u>Paragraphe 4</u> : Autres abus

<u>Article 12</u> : Abus de dispositifs

Les peines applicables aux infractions prévues aux articles 3 à 8 de la présente loi sont encourues par, quiconque produit, vend, obtient pour utilisation, importe, diffuse ou met à disposition, intentionnellement et sans droit, sous quelque forme que ce soit :

- un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une de ces infractions ;
- un mot de passe, un code d'accès ou des 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 de ces infractions.

Les mêmes peines s'appliquent à quiconque possède, intentionnellement et sans droit, un dispositif, un mot de passe, un code d'accès ou des données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique en vue de commettre l'une ou l'autre des infractions visées par les articles 3 à 8 de la présente loi.

Les infractions prévues par le présent article ne sont pas établies lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition n'ont pas pour but de commettre une infraction prévue par les articles 3 à 8 de la présente loi, comme en cas d'essais autorisés ou de protection d'un système informatique.

Article 13 : Association de malfaiteurs informatiques

Est puni d'une peine d'emprisonnement de cinq (5) à moins de dix (10) ans et d'une amende de cinquante millions (50 000 000) à cent millions (100 000 000) de francs CFA, quiconque participe, intentionnellement et sans droit, à une association formée ou à une entente établie en vue de préparer ou de commettre une ou plusieurs infractions prévues par la présente loi.

Article 14 : Usurpation d'identité numérique

Est puni d'une peine d'emprisonnement de deux (2) à cinq (5) ans et d'une amende de cinq millions (5 000 000) à vingt millions (20 000 000) de francs CFA, quiconque usurpe, intentionnellement et sans droit, l'identité numérique d'un tiers ou fait usage d'une ou de plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou de porter atteinte à son honneur, à sa vie privée, à son patrimoine ou à celui d'un tiers.

Paragraphe 5 : Infractions relatives à la pornographie enfantine

Article 15 : Production, offre, diffusion de pornographie enfantine

Est puni d'une peine d'emprisonnement de cinq (5) à moins de dix (10) ans et d'une amende de cinq millions (5 000 000) à dix millions (10 000 000) de francs CFA, quiconque produit, offre ou diffuse, intentionnellement et sans droit, de la pornographie enfantine en vue de sa diffusion, offre ou met à disposition, diffuse ou transmet de la pornographie enfantine par le biais d'un système informatique.

Article 16 : Importation, exportation de la pornographie enfantine

Est puni d'une peine d'emprisonnement de cinq (5) à moins de dix (10) ans et d'une amende de cinq millions (5 000 000) à dix millions (10 000 000) de francs CFA, quiconque se fait procurer ou procure à autrui, importe, se fait importer ou exporte ou se fait exporter de la pornographie enfantine, intentionnellement et sans droit, par le biais d'un système informatique.

Article 17 : Détention ou possession de la pornographie enfantine

Est puni d'une peine d'emprisonnement de cinq (5) à moins de dix (10) ans et d'une amende de cinq millions (5 000 000) à dix millions (10 000 000) de francs CFA, quiconque, intentionnellement et sans droit, possède ou détient de la pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques.

Article 18 : Facilitation de l'accès des mineurs à des contenus pornographiques

Est puni d'une peine d'emprisonnement de cinq (5) à moins de dix (10) ans et d'une amende de cinq millions (5 000 000) à dix millions (10 000 000) de francs CFA,

quiconque facilite, intentionnellement et sans droit, l'accès à des images, des documents, du son ou une représentation présentant un caractère de pédopornographie.

Article 19 : Consultation habituelle de sites de pornographie enfantine

Est puni d'une peine d'emprisonnement de cinq (5) à moins de dix (10) ans et d'une amende de cinq millions (5 000 000) à dix millions (10 000 000) de francs, quiconque, intentionnellement et sans droit, consulte habituellement ou en contrepartie d'un paiement un service de communication au public en ligne mettant à disposition des images ou vidéos pédopornographiques.

Article 20 : Sollicitations sexuelles d'un mineur de moins de quinze ans

Est puni d'une peine d'emprisonnement de un (1) à trois (3) ans et d'une amende de cinq cent mille (500 000) à un million (1 000 000) de francs CFA, toute personne majeure faisant des propositions sexuelles à un mineur de moins de quinze ans ou à une personne se présentant comme telle en utilisant un moyen de communication électronique.

Lorsque les propositions ont été suivies d'une rencontre, les peines prévues à l'alinéa premier du présent article sont portées au double.

Section 2 : Infractions adaptées aux technologies de l'information et de la communication

Paragraphe premier : Infractions portant sur les données informatiques

Article 21 : Reproduction, extraction, copiage de données informatiques

Est puni d'une peine d'emprisonnement de un (1) à cinq (5) ans et d'une amende de trois millions (3 000 000) à dix millions (10 000 000) de francs CFA, quiconque reproduit, extrait ou copie intentionnellement et sans droit des données informatiques appartenant à autrui.

Article 22 : Escroquerie portant sur des données informatiques

Est puni d'une peine d'emprisonnement de deux (2) à cinq (5) ans et d'une amende correspondante au triple de la valeur mise en cause sans qu'elle ne soit inférieure à un million (1 000 000) de francs, quiconque, intentionnellement et sans droit, par des manœuvres frauduleuses quelconques au sens du Code pénal, se fait remettre ou délivrer ou tente de se faire remettre ou délivrer des données informatiques et escroque ou tente d'escroquer tout ou partie de la fortune d'autrui.

Lorsque l'escroquerie aura été commise par une personne ayant fait appel au public, en vue de l'émission d'actions, obligations, bons, parts ou titres quelconques, soit d'une société, soit d'une entreprise commerciale ou industrielle, l'emprisonnement sera de cinq

(5) à moins de dix (10) ans et l'amende correspondante au quintuple de la valeur mise en cause sans qu'elle soit inférieure à deux millions (2 000 000) de francs CFA.

Si l'escroquerie a été commise soit en prenant le titre de fonctionnaire ou agent de l'autorité publique, soit en portant indûment un uniforme, costume ou insigne, soit en alléguant un faux ordre de l'autorité publique, la peine d'emprisonnement sera de cinq (5) à moins de dix (10) ans et l'amende correspondante au quintuple de la valeur mise en cause sans qu'elle ne soit inférieure à deux millions (2 000 000) de francs CFA.

Dans tous les cas, la juridiction saisie peut prononcer l'interdiction d'exercice des droits civiques et/ou l'interdiction de séjour, pour une durée qui ne peut excéder cinq (5) ans.

Article 23 : Abus de confiance portant sur les données informatiques

Est puni d'une peine d'emprisonnement de deux (2) à cinq (5) ans et d'une amende de un million (1 000 000) à cinq millions (5 000 000) de francs CFA, quiconque détourne ou dissipe intentionnellement et sans droit des données informatiques qui lui auront été volontairement remises à un titre quelconque, à charge de les restituer ou d'en faire un usage déterminé.

Si l'abus de confiance a été commis par une personne faisant appel au public, afin d'obtenir soit pour son propre compte, soit comme directeur, administrateur ou agent d'une société ou d'une entreprise commerciale ou industrielle, la remise de fonds ou de valeurs, à titre de dépôt, de mandat ou de nantissement, la peine d'emprisonnement sera de cinq (5) à moins de dix (10) ans et l'amende de cinq millions (5 000 000) à vingt millions (20 000 000) de francs CFA.

Si l'abus de confiance a été commis par un officier public ou ministériel, ou par un salarié, les peines seront d'un emprisonnement de cinq (5) à moins de dix (10) ans et l'amende de cinq millions (5 000 000) à vingt millions (20 000 000) de francs.

Article 24 : Recel portant sur des données informatiques

Est puni d'une peine d'emprisonnement de deux (2) à moins de dix (10) ans et d'une amende de cinq millions (5 000 000) à vingt millions (20 000 000) de francs CFA, quiconque détient sciemment, à un titre quelconque, des données informatiques obtenues à l'aide d'un crime ou d'un délit.

Article 25 : Extorsion portant sur des données informatiques

Est puni d'une peine d'emprisonnement de deux (2) à moins de dix (10) ans et d'une amende de cinq millions (5 000 000) à vingt millions (20 000 000) de francs CFA quiconque, intentionnellement et sans droit, extorque ou tente d'extorquer par force, violence ou contrainte des données informatiques.

Article 26 : Chantage portant sur des données informatiques

Est puni d'une peine d'emprisonnement de deux (2) à sept (7) ans et d'une amende de cinq millions (5 000 000) à vingt millions (20 000 000) de francs CFA, quiconque, à l'aide de la menace, écrite ou verbale, de révélations ou d'imputations diffamatoires, extorque ou tente d'extorquer des données informatiques.

Paragraphe 2 : Infractions commises par un moyen de communication électronique

Article 27 : Escroquerie par un moyen de communication électronique

Est puni d'une peine d'emprisonnement de deux (2) à cinq (5) ans et d'une amende correspondante au triple de la valeur mise en cause sans qu'elle ne soit inférieure à un million (1 000 000) de francs CFA quiconque, intentionnellement et sans droit, par des manœuvres frauduleuses quelconques au sens du Code pénal, à l'aide d'un moyen de communication électronique se sera fait remettre ou délivrer, ou aura tenté de se faire remettre ou délivrer des fonds, des meubles ou des obligations, dispositions, billets, promesses, quittances ou décharges et escroque ou tente d'escroquer tout ou partie de la fortune d'autrui.

Article 28 : Chantage par un moyen de communication électronique

Est puni d'une peine d'emprisonnement de deux (2) à sept (7) ans et d'une amende de cinq millions (5 000 000) à vingt millions (20 000 000) de francs CFA, quiconque, au moyen de la menace d'atteintes à la confidentialité, à l'intégrité des données informatiques ou par toute forme d'atteintes à la confidentialité ou au fonctionnement du système informatique, extorque ou tente d'extorquer, soit la remise de fonds ou valeurs, soit la signature ou la remise des écrits.

Article 29 : Diffamation par un moyen de communication électronique

Est puni d'une peine d'emprisonnement de six (6) mois à trois (3) ans et d'une amende de un million (1 000 000) à cinq millions (5 000 000) de francs CFA, quiconque commet une diffamation par le biais d'un moyen de communication électronique.

Article 30 : Injure par un moyen de communication électronique

Est puni d'une peine d'emprisonnement de six (6) mois à trois (3) ans et d'une amende de un million (1 000 000) à cinq millions (5 000 000) de francs CFA, quiconque profère ou émet toute expression outrageante, tout terme de mépris ou toute invective qui ne renferme l'imputation d'aucun fait, par le biais d'un moyen de communication électronique.

<u>Article 31 :</u> Diffusion de données de nature à troubler l'ordre public ou à porter atteinte à la dignité humaine

Est puni d'une peine d'emprisonnement de six (6) mois à trois (3) ans et de un million (1.000.000) à cinq millions (5.000.000) de francs CFA d'amende, le fait pour une personne de produire, de mettre à la disposition d'autrui ou de diffuser des données de nature à troubler l'ordre public ou à porter atteinte à la dignité humaine par le biais d'un système d'information.

<u>Article 32</u> : Propos à caractère raciste, régionaliste, ethnique, religieux ou xénophobe

Est puni d'une peine d'emprisonnement de un (1) à cinq (5) ans et de un million (1.000.000) à cinq millions (5.000.000) de francs CFA d'amende, quiconque crée, diffuse ou met à disposition, sous quelque forme que ce soit, des écrits, messages, photos, sons, vidéos, dessins ou toute autre représentation d'idées ou de théories de nature raciste, régionaliste, ethnique, religieux ou xénophobe, par le biais d'un système d'information.

<u>Article 33</u> : Peines complémentaires

S'il y a condamnation pour une infraction commise par le biais d'un moyen de communication électronique, la juridiction compétente prononce la confiscation des matériels, des équipements, des instruments, des programmes informatiques ou des données objets ou produits de l'infraction.

La juridiction peut également prononcer l'interdiction d'émettre des messages de communication électronique, l'interdiction à titre provisoire ou définitif de l'accès au site ayant servi à commettre l'infraction ou l'interdiction d'hébergement du site par tous moyens techniques disponibles.

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

La violation des interdictions prononcées en vertu du présent article est punie d'un emprisonnement de six (6) mois à trois (3) ans et d'une amende de cinq cent mille (500 000) à cinq millions (5 000 000) de francs CFA.

En cas de condamnation à une infraction commise par le biais d'un moyen de communication électronique, le juge ordonne à titre complémentaire la publication au frais du condamné, par extrait, de la décision sur ce même support.

La publication prévue à l'alinéa précédent du présent article est exécutée dans les quinze (15) jours suivant le jour où la condamnation est devenue définitive.

Si dans le délai de quinze (15) jours après que la condamnation est devenue définitive, le condamné n'a pas diffusé ou fait diffuser cet extrait, il sera condamné à un emprisonnement de un (1) à cinq (5) ans et d'une amende de un million (1 000 000) à dix millions (10 000 000) de francs CFA.

Chapitre III : Responsabilité pénale

Section première : Responsabilité pénale des personnes morales

Article 34 : Conditions de la responsabilité pénale des personnes morales

Toute personne morale, à l'exception de l'Etat, des collectivités locales et des établissements publics, est responsable des infractions prévues par la présente loi, lorsqu'elles sont commises pour son compte par toute personne physique qui, agissant soit individuellement, soit en tant que membre d'un organe de ladite personne morale, exerce un pouvoir de direction en son sein.

Le pouvoir de direction visé à l'alinéa premier du présent article est exercé sur les bases suivantes :

- un pouvoir de représentation de la personne morale ;

- une autorité pour prendre des décisions au nom de la personne morale ;

- une autorité pour exercer un contrôle au sein de la personne morale.

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

Toute personne morale est également tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, a rendu possible la commission des infractions visées par la présente loi pour le compte de ladite personne morale par une personne physique agissant sous son autorité.

Article 35 : Sanctions contre les personnes morales

Les peines encourues par les personnes morales sont :

1) l'amende dont le taux maximum est égal au quintuple de celui prévu pour les personnes physiques par la loi qui réprime l'infraction ;

2) la dissolution, lorsque la personne morale a été créée pour commettre les faits incriminés ;

3) la dissolution, lorsque la personne morale a été détournée de son objet pour commettre les faits incriminés et si l'infraction retenue expose son auteur, personne physique, à une peine d'emprisonnement supérieure à cinq (5) ans ;

4) l'interdiction à titre définitif ou pour une durée de cinq (5) ans au plus d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ;

5) la fermeture définitive ou pour une durée de cinq (5) ans au plus d'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

6) l'exclusion des marchés publics à titre définitif ou pour une durée n'excédant pas cinq (5) ans ;

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

8) l'interdiction pour une durée de cinq (5) ans au plus d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ou d'utiliser des cartes de paiement ;

9) la confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit ;

10) l'affichage de la décision prononcée et la diffusion de celle-ci soit par la presse écrite soit par tout moyen de communication au public par voie électronique.

Section 2 : Autres formes de responsabilité

Article 36 : Complicité

La complicité des infractions prévues par la présente loi est punissable dans les conditions prévues par le code pénal.

Article 37 : Tentative

La tentative de commettre l'une des infractions prévues par la présente loi est punissable comme le délit consommé.

TITRE II : DE LA PROCEDURE PENALE

Chapitre I : Portée des pouvoirs et procédure

Article 38 : Champ d'application

Les procédures prévues dans le présent titre s'appliquent **:**

- aux infractions pénales prévues par la présente loi ;

- à toutes autres infractions pénales commises au moyen d'un système informatique ;

- à la collecte des preuves électroniques de toute infraction pénale.

Chapitre II : Mesures d'investigation

Article 39 : Conservation rapide de données informatiques stockées

Si les nécessités de l'enquête ou de l'information l'exigent, l'officier de police judiciaire ou le juge d'instruction peut ordonner à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

La personne visée à l'alinéa premier du présent article est tenue de conserver et de protéger l'intégrité des données pendant une durée maximale de 90 jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation.

Le gardien des données ou une autre personne chargée de conserver celles-ci est tenu de garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue.

Toute violation du secret est punie des peines applicables au délit de violation du secret professionnel prévu par le code pénal.

Article 40 : Conservation et divulgation rapides de données relatives au trafic

Si les nécessités de l'enquête ou de l'information l'exigent, l'officier de police judiciaire ou le juge d'instruction peut ordonner à une personne de conserver des données relatives au trafic se trouvant en sa possession ou sous son contrôle, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

La mesure prévue par l'alinéa premier du présent article peut être ordonnée lorsqu'un seul ou plusieurs fournisseurs de service ont participé à la transmission de cette communication.

La personne assurant le contrôle des données doit assurer la divulgation rapide à l'autorité compétente, ou à une personne désignée par cette autorité d'une quantité de données relatives au trafic suffisante pour permettre l'identification des fournisseurs de service et de la voie par laquelle la communication a été transmise.

Article 41 : Injonction de produire

Si les nécessités de l'enquête ou de l'information l'exigent, l'officier de police judiciaire ou le juge d'instruction peut ordonner à :

- une personne présente sur son ressort de communiquer les données informatiques spécifiées, en la possession ou sous le contrôle de cette personne, et stockées dans un système informatique ou un support de stockage informatique ;

- un fournisseur de services offrant des prestations sur le territoire national, de communiquer les données en sa possession ou sous son contrôle relatif aux abonnés et concernant de tels services.

<u>Article 42</u> : Perquisition de données informatiques stockées

Lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données informatisées sur le territoire national sont utiles à la manifestation de la vérité, le juge d'instruction ou l'officier de police judiciaire peut perquisitionner ou accéder d'une façon similaire à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées et à un support du stockage informatique permettant de stocker des données informatiques sur son ressort.

Lorsqu'au cours des opérations de perquisition, les autorités visées à l'alinéa premier du présent article ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur le territoire national, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, elles peuvent étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système.

S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par le juge d'instruction ou par l'officier de police judicaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur.

<u>Article 43</u> : Saisie de données informatiques stockées

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

Le juge d'instruction ou l'officier de police judiciaire peut ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures prévues à l'alinéa premier du présent article.

Si les données qui sont liées à l'infraction, soit qu'elles en constituent l'objet, soit qu'elles en sont le produit, sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, le juge d'instruction ou l'officier de

police judiciaire ordonne les mesures conservatoires nécessaires, notamment en désignant toute personne qualifiée avec pour mission d'utiliser tous les moyens techniques appropriés pour rendre ces données inaccessibles.

Lorsque la mesure prévue à l'alinéa premier du présent article n'est pas possible, pour des raisons techniques ou en raison du volume des données, le juge d'instruction utilise les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.

Le juge d'instruction ou l'officier de police judiciaire informe le responsable du système informatique de la recherche effectuée dans le système informatique et lui communique une copie des données qui ont été copiées, rendues inaccessibles ou retirées.

<u>Article 44</u> : Collecte en temps réel des données relatives au trafic

Lorsque les nécessités de l'enquête ou de l'information l'exigent, l'officier de police judiciaire ou le juge d'instruction peut collecter ou enregistrer par l'utilisation de moyens techniques existants ou obliger un fournisseur de services, dans la limite des capacités techniques existantes à :

- collecter ou enregistrer par l'utilisation de moyens techniques existants sur le territoire national ;

- prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur le territoire national au moyen d'un système informatique.

Le fournisseur de services visé à l'alinéa premier du présent article est tenu de garder secret le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.

<u>Article 45</u> : Interception de données relatives au contenu

En matière criminelle ou lorsque la peine encourue est égale ou supérieure à deux (2) ans d'emprisonnement en matière correctionnelle, le juge d'instruction peut, si les nécessités de l'information l'exigent, notamment à la demande d'un officier de police judiciaire, prescrire la collecte, l'interception, l'enregistrement et la transcription de données relatives au contenu de communications spécifiques relevant de son ressort, transmises au moyen d'un système informatique. Ces opérations sont effectuées sous son autorité et son contrôle.

La décision d'interception est écrite. Elle n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours.

La décision d'interception prise en application de l'alinéa premier du présent article comporte tous les éléments d'identification de la liaison à intercepter, l'infraction qui motive le recours à l'interception ainsi que la durée de celle-ci.

Cette décision d'interception est prise pour une durée maximale de trois (3) mois. Elle ne peut être renouvelée qu'une fois dans les mêmes conditions de forme et de durée à condition que la demande de renouvellement soit transmise au plus tard quarante-huit (48) heures avant l'échéance de la première décision d'interception.

Le juge d'instruction ou l'officier de police judiciaire par lui commis peut requérir tout agent qualifié d'un service ou organisme public en charge des communications électroniques ou tout agent qualifié d'un exploitant de réseau ou fournisseur de services, dans le cadre de ses capacités techniques existantes, en vue de procéder à l'installation d'un dispositif d'interception.

Le juge d'instruction ou l'officier de police judiciaire commis par lui dresse procès-verbal de chacune des opérations d'interception et d'enregistrement. Ce procès-verbal mentionne la date et l'heure auxquelles l'opération a commencé et celles auxquelles elle s'est terminée.

Les enregistrements sont placés sous scellés fermés et accessibles par le juge d'instruction, l'officier de police judiciaire ou toute personne habilitée par le juge d'instruction.

Le juge d'instruction ou l'officier de police judiciaire commis par lui transcrit la correspondance utile à la manifestation de la vérité. Il en est dressé procès-verbal. Cette transcription est versée au dossier.

Les correspondances dans une langue autre que la langue officielle sont transcrites en français avec l'assistance d'un interprète requis à cette fin.

A peine de nullité, ne peuvent être transcrites les correspondances entre l'inculpé et son conseil lorsqu'elles relèvent de l'exercice des droits de la défense.

Les enregistrements sont détruits, à la diligence du procureur de la République ou du procureur général, à l'expiration du délai de prescription de l'action publique.

Il est dressé procès-verbal de l'opération de destruction.

Le fournisseur de services visé au sixième alinéa du présent article est tenu de garder secret le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.

Article 46 : Les correspondances dépendant du bureau ou du domicile d'un parlementaire ne peuvent être interceptées sans que le Bureau de l'Assemblée nationale en soit informé par le juge d'instruction.

Article 47 ; Les correspondances dépendant du cabinet d'un avocat ou de son domicile ne peuvent être interceptées sans que le bâtonnier de l'ordre des avocats en soit informé par le juge d'instruction.

Article 48 : Les correspondances dépendant du cabinet d'un magistrat ou d'un juge ou de leurs domiciles ne peuvent être interceptées sans que le président de la cour d'appel ou le procureur général près la cour dont relève la juridiction à laquelle il appartient en soit informé par le juge d'instruction.

Article 49 : Les correspondances dépendant du cabinet du président d'une cour d'appel, ou du procureur général près une cour d'appel, ou celle d'un magistrat ou d'un juge d'une haute juridiction ou d'un magistrat exerçant dans l'administration, ne peuvent être interceptées sans que le Ministre en charge de la Justice en soit informé par le juge d'instruction.

Article 50 : Les correspondances dépendant du cabinet d'un membre du gouvernement ou de son domicile ne peuvent être interceptées sans que le Premier ministre en soit informé par le juge d'instruction.

Article 51 : Les correspondances dépendant du cabinet du Premier ministre ou de son domicile ne peuvent être interceptées sans que le Président de la République en soit informé par le juge d'instruction.

Article 52 : Les formalités prévues par les articles 45 à 51 ci-dessus sont prescrites à peine de nullité.

Les personnalités avisées sont liées par le secret de l'instruction.

Article 53 : Si les nécessités de l'enquête de flagrance ou de l'enquête préliminaire relative à l'une des infractions prévues par la présente loi l'exigent, le président du tribunal de grande instance ou le juge par lui délégué peut, à la requête du procureur de la République, autoriser l'interception, l'enregistrement et la transcription de correspondances émises par la voie des communications électroniques selon les modalités prévues par le présent article, pour une durée maximale de trois mois, renouvelable qu'une fois dans les mêmes conditions de forme et de durée à condition que la demande de renouvellement soit transmise au plus tard quarante-huit heures (48) avant l'échéance de la première décision d'interception.

La requête du procureur et l'ordonnance du président sont frappées du sceau de la confidentialité.

Article 54 : Enquête sous pseudonyme

Dans le but de constater les infractions mentionnées aux articles 3 à 31 de la présente loi, lorsque celles-ci sont commises par un moyen de communication électronique, d'en rassembler les preuves et d'en rechercher les auteurs, les officiers ou agents de police

judiciaire agissant au cours de l'enquête ou sur commission rogatoire peuvent, s'ils sont affectés dans un service spécialisé et spécialement habilités à cette fin, procéder aux actes suivants sans en être pénalement responsables :

1. participer sous un pseudonyme aux échanges électroniques ;

2. être en contact avec les personnes susceptibles d'être les auteurs de ces infractions ;

3. extraire, acquérir ou conserver par ce moyen les éléments de preuve et les données sur les personnes susceptibles d'être les auteurs de ces infractions ;

4. extraire, transmettre en réponse à une demande expresse, acquérir ou conserver des contenus illicites.

A peine de nullité, ces actes ne peuvent constituer une incitation à commettre ces infractions.

Chapitre III : Preuve électronique

Article 55 : Admissibilité de la preuve électronique

En matière pénale, la preuve électronique est admissible à condition qu'elle soit recueillie et conservée dans des conditions de nature à en garantir l'intégrité.

Chapitre IV : Compétence des juridictions

Article 56 : Champ de compétence

Les juridictions nationales sont compétentes pour juger une des infractions prévues par la présente loi :

- lorsqu'elle est commise, en tout ou en partie, sur le territoire national, à bord d'un navire battant pavillon nigérien, à bord d'un aéronef immatriculé nigérien ;

- lorsqu'elle est commise par un Nigérien, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat ;

- lorsque l'auteur présumé de l'infraction est présent sur le territoire nigérien et ne peut être extradé vers un autre Etat au seul titre de sa nationalité, après une demande d'extradition.

Le présent article n'exclut pas les autres champs de compétence prévus par les dispositions du Code de procédure pénale relatives aux crimes et délits commis à l'étranger.

TITRE III : DE LA COOPERATION INTERNATIONALE EN MATIERE PENALE

Article 57 : Principes généraux relatifs à la coopération internationale

L'autorité compétente coopère avec les autres Etats, conformément aux dispositions du présent titre, en application des instruments internationaux en vigueur sur la coopération

internationale en matière pénale auxquels le Niger est partie, dans la mesure la plus large possible, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et données informatiques ou pour recueillir les preuves, sous forme électronique, d'une infraction pénale.

Article 58 : Extradition

Le présent article s'applique à l'extradition pour les infractions pénales définies aux articles de la présente loi, à condition qu'elles soient punissables dans la législation interne et dans la législation de l'Etat requérant d'une peine privative de liberté pour une période maximale d'au moins un an, ou par une peine plus sévère.

Lorsqu'il est exigé une peine minimale différente, sur la base d'un instrument international applicable entre le Niger et l'Etat requérant, la peine minimale prévue par cet instrument s'applique.

L'extradition est soumise aux conditions prévues par le droit interne ou par les traités d'extradition en vigueur, y compris les motifs pour lesquels l'autorité compétente peut refuser l'extradition.

Si l'extradition pour une infraction pénale mentionnée au premier paragraphe du présent article est refusée uniquement sur la base de la nationalité de la personne recherchée ou parce que l'autorité habilitée s'estime compétente pour cette infraction, elle soumet l'affaire à la demande de l'Etat requérant, à ses autorités compétentes aux fins de poursuite, et rend compte, en temps utile, de l'issue de l'affaire à l'Etat requérant. Les autorités en question prennent leur décision et mènent l'enquête et la procédure de la même manière que pour toute autre infraction de nature comparable, conformément à la législation du Niger.

Article 59 : Principes généraux relatifs á l'entraide

L'autorité compétente accorde l'entraide la plus large possible aux autres Etats aux fins d'investigation ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale.

L'autorité compétente peut, en cas d'urgence, formuler une demande d'entraide ou des communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification, y compris, si nécessaire, le cryptage, avec confirmation officielle ultérieure si l'Etat requis l'exige. Si le Niger fait l'objet d'une telle demande, l'autorité compétente accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.

Lorsque le Niger reçoit une demande d'entraide, celle-ci est soumise, sauf disposition contraire expressément prévue dans les articles du présent chapitre, aux conditions

fixées par le droit national ou par les traités d'entraide applicables, y compris les motifs sur la base desquels l'Etat requis peut refuser la coopération. L'Etat requis ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 3 à 31 au seul motif que la demande porte sur une infraction qu'il considère comme de nature fiscale.

La condition de double incrimination, à laquelle est subordonnée toute demande d'entraide, est considérée comme satisfaite dès lors que le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale dans le droit nigérien, que cette dernière classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de l'Etat requérant.

Article 60 : Information spontanée

L'autorité compétente peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à un autre Etat des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider l'Etat destinataire à engager ou mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente loi, ou lorsque ces informations pourraient aboutir à une demande de coopération.

Avant de communiquer de telles informations, le Niger peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions.

Article 61 : Conservation rapide de données informatiques stockées

L'autorité compétente peut se voir ordonnée ou imposée d'une autre façon par un autre Etat partie la conservation rapide de données stockées au moyen d'un système informatique se trouvant sur le territoire du Niger, et au sujet desquelles l'Etat requérant a l'intention de soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation desdites données.

Une demande de conservation faite en application du paragraphe précédent doit préciser :

- l'autorité qui demande la conservation ;
- l'infraction faisant l'objet de l'enquête ou de procédures pénales et un bref exposé des faits qui s'y rattachent ;
- les données informatiques stockées à conserver et la nature de leur lien avec l'infraction ;
- toutes les informations disponibles permettant d'identifier le gardien des données informatiques stockées ou l'emplacement du système informatique ;

- la nécessité de la mesure de la conservation ;
- le fait que l'Etat requérant entend soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données informatiques stockées.

Après avoir reçu la demande d'un autre Etat, l'autorité compétente doit prendre toutes les mesures appropriées afin de procéder sans délai à la conservation des données spécifiées, conformément au droit interne. Pour pouvoir répondre à une telle demande, la double incrimination n'est pas requise comme condition préalable à la conservation.

Une demande de conservation peut être refusée uniquement :

- si l'autorité compétente a des raisons de penser que, au moment de la divulgation, la condition de double incrimination ne pourra pas être remplie ;
- si la demande porte sur une infraction que l'Etat requis considère comme étant de nature politique ou liée à une infraction de nature politique ;
- si l'Etat requis estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à d'autres intérêts essentiels.

Lorsque l'autorité compétente estime que la conservation simple ne suffira pas à garantir la disponibilité future des données, ou compromettra la confidentialité de l'enquête de l'Etat requérant, ou nuira d'une autre façon à celle-ci, elle en informe rapidement cet Etat.

Toute conservation effectuée en réponse à une demande visée au présent article est valable pour une durée de soixante (60) jours afin de permettre à l'Etat requérant de soumettre une demande en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données. Après la réception d'une telle demande, les données doivent continuer à être conservées en attendant l'adoption d'une décision concernant la demande.

<u>Article 62</u> : Divulgation rapide de données conservées

Lorsque, en exécutant une demande de conservation de données relatives au trafic concernant une communication spécifique formulée en application de l'article précédent, l'autorité compétente découvre qu'un fournisseur de services dans un autre Etat a participé à la transmission de cette communication, l'autorité compétente divulgue rapidement à cet Etat une quantité suffisante de données concernant le trafic, aux fins d'identifier ce fournisseur de services et la voie par laquelle la communication a été transmise.

La divulgation de données relatives au trafic en application du paragraphe précédent peut être refusée seulement :

- si la demande porte sur une infraction que l'autorité compétente considère comme étant de nature politique ou liée à une infraction de nature politique ;
- si elle considère que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

<u>Article 63</u> : Entraide concernant l'accès aux données stockées

L'autorité compétente peut se voir requise par un autre Etat de perquisitionner ou d'accéder de façon similaire, de divulguer des données stockées au moyen d'un système informatique se trouvant sur son territoire, y compris les données conservées conformément aux articles 39 et 40 de la présente loi.

L'autorité compétente satisfait à la demande en appliquant les instruments internationaux en vigueur et en se conformant aux dispositions pertinentes du présent titre.

La demande doit être satisfaite aussi rapidement que possible dans les cas où :

- il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification ;
- les instruments internationaux en vigueur prévoient une coopération rapide.

<u>Article 64</u> : Accès transfrontalier à des données stockées

L'autorité compétente peut accéder à des données informatiques stockées accessibles au public, quelle que soit la localisation géographique de ces données et sans l'autorisation de l'Etat sur le territoire duquel se trouvent ces données.

L'autorité compétente peut recevoir ou accéder, au moyen d'un système informatique situé sur son territoire, à des données informatiques situées sur le territoire d'un autre Etat dès lors qu'elle obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

<u>Article 65</u> : Entraide dans la collecte en temps réel de données relatives au trafic

L'autorité compétente accorde aux autres Etats l'entraide dans la collecte en temps réel de données relatives au trafic, associées à des communications spécifiées sur son territoire, transmises au moyen d'un système informatique. Sous réserve des dispositions du paragraphe suivant, cette entraide est régie par les conditions et les procédures prévues en droit interne.

L'autorité compétente accorde cette entraide au moins à l'égard des infractions pénales pour lesquelles la collecte en temps réel de données concernant le trafic serait disponible dans une affaire analogue au niveau interne.

<u>Article 66</u> : Entraide en matière d'interception de données relatives au contenu

Dans la mesure permise par les traités et son droit interne applicables, l'autorité compétente accorde aux autres Etats l'entraide pour la collecte ou l'enregistrement en temps réel de données relatives au contenu de communications spécifiques transmises au moyen d'un système informatique.

Article 67 : Point de contact 24/7

Pour les infractions relevant de la présente loi, la Direction de la police judiciaire constitue, en attendant la mise en place d'une structure spécialement dédiée, le point de contact central joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale.

Cette assistance doit englober la facilitation, si le droit le permet, et l'application directe des mesures suivantes :

- Apport de conseils techniques ;
- Conservation des données, conformément aux articles 60 et 61 ;
- Recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.

Le point de contact, dit 24/7, doit être doté des moyens de correspondre avec le point de contact d'un autre Etat selon une procédure accélérée.

Article 68 : Autorité compétente.

L'autorité compétente désignée aux fins de l'application de la présente loi est le Ministre chargé de la Justice.

A ce titre, il a l'obligation de faire en sorte que le point de contact dispose d'un personnel suffisamment formé et équipé en vue de faciliter le fonctionnement du point de contact 24/7 établi par la Convention du Conseil de l'Europe sur la cybercriminalité et les autres conventions pertinentes.

Article 69 : La présente loi qui abroge toutes dispositions antérieures contraires est publiée au Journal Officiel de la République du Niger et exécutée comme loi de l'Etat.

Le Secrétaire Parlementaire **Le Président de l'Assemblée Nationale**

ILLIASOU DILLE **OUSSEINI TINNI**