PROJET DE LOI RELATIVE À LA CYBERCRIMINALITÉ

REPUBLIQUE ISLAMIQUE DE MAURITANIE

Honneur-Fraternité-Justice

Le Premier Ministère

Exposé de motif du Projet de loi portant loi relative à la cybercriminalité

La réalisation d'importants projets d'infrastructures des Technologies de l'Information et de la Communication (TIC), tels que la connectivité de notre pays au réseau international à haut débit, via le câble sous-marin ACE, et le projet de connectivité nationale en cours d'exécution WARCIP Mauritanie, stimulera sans doute, le développement de l'usage des TIC dans notre société.

Ce développement contribuera d'une manière considérable, à l'élargissement du champ d'action des opportunités d'échange d'informations et de communication. Une telle situation est susceptible d'engendrer de nouveaux faits et comportements répréhensibles, comme ce fut le cas dans toutes les sociétés avancées en la matière. Ces nouveaux comportements répréhensibles ont besoin d'être pris en compte par le législateur afin d'être incriminés et sanctionnés.

Dans l'environnement juridique mauritanien, la commission d'infractions portant atteintes aux personnes et aux valeurs morales, par le biais de l'usage des TIC, n'a été mentionnée que dans l'ordonnance n°2005-015 portant protection pénale de l'enfant (articles 47 et 48) et dans la loi n°2010-035 du 21 juillet 2010 abrogeant et remplaçant la loi n°2005- 047 du 26 juillet 2005 relative à la lutte contre le terrorisme.

En dehors de ces dispositions, aucune infraction pénale n'est prévue, d'une manière explicite, en la matière par le code pénal et les autres textes en vigueur.

Face à ces lacunes de l'édifice pénal, il est apparu nécessaire de mettre en place un cadre juridique cohérent de prévention, de dissuasion et de répression de la cybercriminalité dans notre pays.

Et c'est ainsi que ce présent projet de loi, met en place le dispositif juridique de lutte contre la cybercriminalité, et apporte des innovations majeures par l'introduction de nouvelles infractions spécifiques aux TIC, en instituant la protection pénale des systèmes et données informatiques et la répression des infractions se rapportant aux contenus.

Ce nouveau dispositif juridique de lutte contre la cybercriminalité, consacre également une amélioration du cadre processuel, par l'admission de la perquisition et de la saisie informatique, et par l'introduction de nouveaux mécanismes de recherche de la preuve numérique.

Enfin, face à l'internationalisation de la cybercriminalité, une obligation générale de coopération à la charge de notre pays a été consacrée, pour les besoins de la répression des actions cybercriminelles.

Il ya lieu de signaler que ce projet de loi a fait l'objet d'un large processus de concertation, et de validation par l'ensemble des parties concernées.

Telle est l'économie du présent projet de loi relatif à la cybercriminalité soumis à votre approbation.

Yahya Ould Hademine

REPUBLIQUE ISLAMIQUE DE MAURITANIE

Honneur-Fraternité-Justice

PRESIDENCE DE LA REPUBLIQUE

VISA : DGLTEJO

Projet de loi n° _____ relative à la cybercriminalité

CHAPITRE I : DES DISPOSITIONS GENERALES

Section 1 : Des définitions

Article premier

Au sens du présent chapitre, on entend par :

1. **Données informatiques :** toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris tout programme de nature à faire en sorte qu'un système informatique exécute une fonction ;
2. **Données relatives aux abonnés :** toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:

- 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 services ;
- toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services ;

3. **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, la taille, l'heure, la date et la durée de la communication ou le type du service sous-jacent ;

4. **Fournisseur de services :** toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ou toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs ;
5. **Message de données :** toute information créée, envoyée ou reçue par des procédés ou moyens électroniques ou optiques ou des procédés ou moyens analogues, notamment, l'échange de données informatisées, la messagerie électronique;
6. **Mineur :** toute personne qui n'a pas atteint l'âge de majorité conformément aux lois et règlements en vigueur en République Islamique de Mauritanie ;
7. **Pornographie :** toute donnée qu'elle qu'en soit la nature ou la forme représentant une personne quel que soit son âge et son sexe, se livrant à un agissement sexuellement explicite ou des images réalistes représentant une personne se livrant à un comportement sexuel explicite ;
8. **Matériel raciste et xénophobe :** tout matériel écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage ou incite à 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, ethnique ou de la religion ;
9. **Système informatique :** tout dispositif isolé ou tout ensemble de dispositifs interconnectés ou apparentés qui assurent ou dont un ou plusieurs éléments assurent, en exécution d'un programme en tout ou partie, un traitement automatisé de données;

Section 2 : De l'objet et la portée de la loi

Article 2

La présente loi porte sur les crimes et délits liés à l'usage des Technologies de l'Information et de la Communication.

Elle ne s'applique pas aux services de radiodiffusion sonore ou de radiodiffusion télévisuelle.

Article 3

Les pouvoirs et procédures prévues par la présente loi s'appliquent :

- aux infractions prévues par la présente loi ;
- à toutes les autres infractions pénales commises au moyen d'un système informatique ;
- à la collecte des preuves électroniques de toute autre infraction pénale.

CHAPITRE II – DES INFRACTIONS CONTRE LA CONFIDENTIALITE, L'INTEGRITE ET LA DISPONIBILITE DES DONNEES ET SYSTEMES INFORMATIQUES

Section 1 - Des infractions portant atteinte aux données informatiques.

Article 4

Quiconque aura intercepté ou tenté d'intercepter, intentionnellement et sans droit, par des moyens techniques, des données informatiques lors de transmissions non publiques, en provenance, à destination ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques, sera puni d'un à trois ans d'emprisonnement et d'une amende de 100.000 à 2.000.000 d'ouguiyas ou de l'une de ces deux peines seulement.

Article 5

Quiconque aura, intentionnellement et sans droit, endommagé ou tenté d'endommager, effacé ou tenté d'effacer, détérioré ou tenté de détériorer, altéré ou tenté d'altérer, supprimé ou tenter de supprimer, des données informatiques, sera puni d'un à trois ans d'emprisonnement et d'une amende de 100.000 à 2.000.000 d'ouguiyas, ou de l'une de ces deux peines seulement.

Section 2 : Des infractions portant atteinte aux systèmes informatiques

§.1 : Des infractions relatives à la confidentialité des systèmes informatiques

Article 6

Quiconque aura accédé ou tenté d'accéder, intentionnellement et sans droit, à tout ou partie d'un système informatique, sera puni d'un à trois ans d'emprisonnement et d'une amende de 100.000 à 2.000.000 d'ouguiyas, ou de l'une de ces deux peines seulement.

Article 7

Quiconque se sera maintenu ou aura tenté de se maintenir, intentionnellement et sans droit, à tout ou partie d'un système informatique, sera puni de deux à quatre ans d'emprisonnement et d'une amende de 200. 000 à 3.000.000 d'ouguiyas, ou de l'une de ces deux peines seulement.

§ 2. : Des infractions relatives à l'intégrité et à la disponibilité des systèmes informatiques.

Article 8

Quiconque aura, intentionnellement et sans droit, entravé ou faussé ou aura tenté d'entraver ou de fausser 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 sera puni de deux à quatre ans d'emprisonnement et d'une amende de 200.000 à 3.000.000 d'ouguiyas, ou de l'une de ces deux peines seulement.

Article 9

Quiconque aura introduit ou tenté d'introduire, intentionnellement et sans droit, des données informatiques dans un système informatique, sera puni de deux à quatre ans d'emprisonnement et d'une amende de 200.000 à 3.000.000 d'ouguiyas, ou de l'une de ces deux peines seulement.

Article 10

Quiconque aura, intentionnellement et sans droit, produit, vendu, importé, diffusé, utilisé, offert, cédé, aidé ou mis à disposition d'une quelconque façon :un dispositif, y compris un programme informatique principalement conçu et adapté pour commettre l'une des infractions visées par la présente loi ; un mot de passe, un code d'accès, des données informatiques similaires ou tout autre procédé technique, permettant d'accéder à tout ou partie d'un système informatique, dans l'intention qu'ils soient utilisés aux fins de commettre l'une ou l'autre des infractions susvisés, sera puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Aucune responsabilité pénale n'est encourue au titre du présent article, lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées ci-dessus, n'a pas eu pour but de commettre une infraction visée par les articles de la présente loi, notamment, en cas d'essais autorisés ou de protection d'un système informatique.

Article 11

Quiconque aura, intentionnellement et sans droit, aidé à perpétrer une ou plusieurs des infractions prévues par la présente section ou s'en est rendu complice avec l'intention que ces infractions soient commises, sera puni d'un mois à un an d'emprisonnement et d'une amende de 100.000 à 2.000.000 d'ouguiyas, ou de l'une de ces deux peines seulement.

Section 3 : Des infractions informatiques

Article 12

Quiconque aura introduit, altéré, effacé ou supprimé, 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, sera puni de deux à cinq ans d'emprisonnement et d'une amende de 500.000 à 2.000.000 d'ouguiyas, ou de l'une de ces deux peines seulement.

Article 13

Quiconque aura, intentionnellement et sans droit, causé un préjudice patrimonial à autrui par :

- l'introduction, l'altération, l'effacement ou la suppression de données informatiques ;
- 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, sera puni de deux à cinq ans emprisonnement et d'une amende de 500.000 à 3.000.000 d'ouguiyas, ou de l'une de ces deux peines seulement.

CHAPITRE III : DES INFRACTIONS SE RAPPORTANT AUX CONTENUS

Section 1 : Des infractions portant atteinte à la propriété intellectuelle et aux droits connexes

Article 14

Les atteintes à la propriété intellectuelle et aux droits connexes, définis par la législation nationale, conformément aux obligations internationales de la Mauritanie, à l'exception de tout droit moral conféré par ces engagements internationaux, commises délibérément à une échelle commerciale, et au moyen d'un système informatique, sont punies d'un à trois ans d'emprisonnement et d'une amende de 100 000 à 2.000.000 d'ouguiyas, ou de l'une de ces deux peines seulement.

Section 2: Des infractions se rapportant à la pornographie

§ 1: Des infractions se rapportant à la pornographie en général

Article 15

Quiconque aura intentionnellement, produit, enregistré, offert, mis à disposition, diffusé une image ou toute forme de représentation visuelle présentant un caractère pornographique par le biais d'un système informatique, sera puni de deux à quatre ans d'emprisonnement et d'une amende de 200.000 à 3.000.000 d'ouguiyas, ou de l'une de ces deux peines seulement.

Article 16

Sera puni de la même peine, quiconque se sera intentionnellement, procuré ou aura procuré à autrui, importé ou fait importer, exporté ou fait exporter une image ou toute forme de représentation visuelle d'un contenu à caractère pornographique par le biais d'un système informatique.

§ 2: Des infractions se rapportant à la pornographie enfantine

Article 17

Quiconque aura intentionnellement, enregistré, offert, mis à disposition, diffusé, transmis de la pornographie enfantine par le biais d'un système informatique, sera puni de trois à sept ans d'emprisonnement et de 500.000 à 4.000.000 d'ouguiyas, ou de l'une de ces deux peines seulement.

Article 18

Sera puni des mêmes peines prévues à l'article précédent, quiconque se sera intentionnellement, procuré ou aura procuré à autrui, importé ou fait importer, exporté ou fait exporter de la pornographie enfantine par le biais d'un système informatique.

Article 19

Sera puni des mêmes peines prévues à l'article 17 ci-dessus, quiconque aura intentionnellement, possédé de la pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques.

Article 20

Sera puni des mêmes peines prévues à l'article 17 ci-dessus, quiconque aura intentionnellement, accédé ou facilité l'accès à de la pornographie enfantine par le biais d'un système informatique.

Section 3: Des infractions portant atteinte aux valeurs morales et aux bonnes mœurs

Article 21

Sans préjudice des peines prévues par l'article 306 du code pénal, sera puni d'un à quatre ans d'emprisonnement et d'une amende de 200.000 à 3.000.000 d'ouguiyas, ou de l'une de ces deux peines seulement, quiconque aura intentionnellement, créé,

enregistré, mis à disposition, transmis ou diffusé par le biais d'un système informatique, un message texte, une image, un son ou toute autre forme de représentation audio ou visuelle qui porte atteinte aux valeurs de l'Islam.

Section 4 – Des infractions liées aux actes racistes et xénophobes

Article 22

Quiconque aura intentionnellement, par le biais d'un système informatique, insulté une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion ou un groupe de personne qui se distingue par une de ces caractéristiques, sera puni d'un mois à un an d'emprisonnement et d'une amende de 300.000 à 2.000.000 d'ouguiyas, ou de l'une de ces deux peines seulement, sans préjudice des dommages-intérêts à allouer à la victime.

Article 23

Quiconque aura intentionnellement, par le biais d'un système informatique, produit, enregistré, offert, mis à disposition, diffusé un message texte, une image, un son ou toute autre forme de représentation d'idées ou de théorie, faisant l'apologie des crimes contre l'humanité ou incitant à la violence et/ou à la haine raciale, sera puni d'un mois à un an d'emprisonnement et d'une amende de 200.000 à 2.000.000 d'ouguiyas, ou de l'une de ces deux peines seulement, sans préjudice des dommages-intérêts à allouer à la victime.

Section 5 – Des infractions portant atteinte aux personnes

Article 24

Hormis les cas où la loi en dispose autrement, est constitutif d'acte d'atteinte volontaire à la vie privée et passible d'un mois à un an d'emprisonnement et de 100.000 à 1.000.000 d'ouguiyas, d'amende, ou de l'une de ces deux peines seulement, le fait d'enregistrer sciemment à l'insu de toutes personnes visées, par quelque moyen que ce soit, sur tout support que ce soit, des images, sons ou textes, dans l'objectif de porter préjudice à ces personnes.

Le fait de diffuser intentionnellement, par le biais d'un système informatique, l'enregistrement de telles images, sons ou textes, mentionnés à l'alinéa précédent, est puni en outre de deux mois à un an d'emprisonnement et de 200.000 à 2.000.000 d'ouguiyas, d'amende, ou de l'une de ces deux peines seulement.

Article 25

Sans préjudice des dommages-intérêts à allouer aux victimes, sera puni d'un mois à un an d'emprisonnement et d'une amende de 100.000 à 600.000 ouguiyas, ou de l'une de ces deux peines seulement, quiconque aura, intentionnellement , usurpé sur tout système informatique ou tout autre procédé technique, l'identité d'une personne physique, morale ou d'une autorité publique, dans l'objectif de tirer un profit ou de bénéficier d'une faveur quelconque, pour soi-même ou pour autrui. La même peine s'applique lorsque l'acte est commis dans l'intention de porter préjudice à la personne dont l'identité est usurpée, ou en vue de commettre ou de faciliter la commission d'une ou plusieurs des infractions prévues par la présente loi.

Article 26

Quiconque aura intentionnellement, aidé à perpétrer une ou plusieurs des infractions prévues par la présente section ou s'en est rendu complice avec l'intention que ces infractions soient commises, sera puni d'un mois à un an d'emprisonnement et d'une amende de 100.000 à 2.000.000 d'ouguiyas, ou de l'une de ces deux peines seulement.

Article 27

Tout doute quant à l'application des dispositions de la présente loi, doit être interprété en faveur de la liberté d'expression, sauf les cas où la loi en dispose autrement, notamment, quand les faits se rapportent aux principes sacrés de l'Islam.

CHAPITRE IV : DES INFRACTIONS PORTANT ATTEINTE AUX BIENS

Article 28

Quiconque aura, intentionnellement et sans droit, copié des données informatiques au préjudice d'autrui, sera puni d'un à trois ans d'emprisonnement et d'une amende de 100.000 à 2.000.000 d'ouguiyas, ou de l'une de ces deux peines seulement.

Article 29

Quiconque aura reçu, intentionnellement et sans droit, des données informatiques personnelles, confidentielles ou celles qui sont protégées par le secret professionnel, en usant de manœuvres frauduleuses quelconques, soit en faisant usage de faux noms ou de fausses qualités, sera puni d'un à trois ans d'emprisonnement et d'une amende de 100.000 à 2.000.000 d'ouguiyas, ou de l'une de ces deux peines seulement.

Article 30

Quiconque aura, intentionnellement et sans droit, recelé des données informatiques enlevées, détenues ou obtenues à l'aide d'un crime ou d'un délit, seront punis d'un à trois ans d'emprisonnement et d'une amende de 100.000 à 2.000.000 d'ouguiyas, ou de l'une de ces deux peines seulement.

Article 31

Les infractions prévues par la présente loi, lorsqu'elles sont commises en bande organisée, seront punies de cinq à dix ans d'emprisonnement et d'une amende de 2.000.000 à 9.000.000 d'ouguiyas, ou de l'une de ces deux peines seulement.

CHAPITRE V : DES INFRACTIONS PORTANT ATTEINTE A LA DEFENSE ET A LA SECURITE NATIONALE

Article 32

Sera coupable d'atteinte à la défense nationale et puni de la réclusion à perpétuité et la confiscation de tout ou partie du patrimoine, sans préjudice de peines plus lourdes prévues par des lois spéciales, quiconque intentionnellement, par le biais d'un système informatique :

1. livre ou aide une puissance étrangère ou ses agents, à obtenir des informations sous quelque forme que ce soit, qui doivent être tenues secrètes dans l'intérêt de la défense nationale ;
2. s'assure, par quelque moyen que ce soit, de la possession de telles informations, en vue de les livrer à un Etat ou à une institution publique ou privée étrangère ou à ses agents ;
3. détruit ou laisse détruire de telles informations, en vue de favoriser un Etat ou une institution publique ou privée étrangère ;
4. rassemble des informations dont la réunion et l'exploitation sont de nature à nuire à la défense nationale ;
5. contribue directement ou indirectement à la réalisation ou à la tentative de réalisation d'une ou de plusieurs des infractions visées au présent chapitre.

Article 33

Les systèmes des Technologies de l'Information et de la Communication fonctionnant dans des secteurs, considérés comme sensibles pour la sécurité nationale et l'ordre public économique de la République Islamique de Mauritanie, et désignés ainsi par décret, constituent des infrastructures critiques. A cet égard, les infractions prévues par la présente loi, commises sur ces infrastructures, sont punies conformément à l'article 32 ci-dessus, en tant qu'atteinte à la défense nationale.

CHAPITRE VI : DE LA RESPONSABILITE DES PERSONNES MORALES

Article 34

Les personnes morales autres que l'Etat, les collectivités locales et les établissements publics, sont pénalement responsables des infractions prévues par la présente loi, commises pour leur compte, par 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, fondé sur :

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

La personne morale peut être tenue responsable, lorsque l'absence de surveillance ou de contrôle, de la part d'une personne physique, mentionnée au paragraphe précédent, a rendu possible la commission de l'infraction.

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

Article 35

Les peines encourues par les personnes morales sont :

1. l'amende dont le quantum maximum est égal au quintuple de celui prévu pour les personnes physiques;
2. la dissolution lorsqu'il s'agit d'une personne morale, ou d'une peine d'emprisonnement supérieure à cinq ans lorsqu'il s'agit d'un crime ou d'un délit commis par une personne physique ;
3. l'interdiction à titre définitif ou pour une durée de cinq ans au plus d'exercer, directement ou indirectement, une ou plusieurs activités professionnelles ou sociales en rapport avec les faits;
4. la fermeture définitive, ou pour une durée de cinq ans au plus, d'un ou de plusieurs des établissements de l'entreprise, ayant participé à commettre les faits incriminés ;
5. l'exclusion de participation aux marchés publics à titre définitif, ou pour une durée de cinq ans au plus,
6. la saisie et la confiscation de la chose qui a servi ou était destinée, à commettre l'infraction, ou de la chose qui en est le produit ;
7. l'affichage de la décision de justice prononcée, ou la diffusion de celle-ci, soit par la presse écrite, soit par tout moyen de communication au public, notamment par voie électronique.

CHAPITRE VII: DES PEINES COMPLEMENTAIRES

Article 36

En cas de condamnation pour une infraction commise par le biais d'un support de communication électronique, le juge peut faire injonction à toute personne responsable légalement du site physique ou électronique ayant servi à commettre l'infraction, et à toute personne qualifiée, de mettre en œuvre les moyens techniques nécessaires en vue de garantir, l'interdiction d'accès, d'hébergement ou la coupure de l'accès au site incriminé.

La violation des injonctions prononcées par le juge, sera punie d'un emprisonnement d'un mois à un an et d'une amende de 200.000 à 1.000.000 d'ouguiyas, ou de l'une de ces deux peines seulement.

Le juge peut en outre, prononcer une astreinte de 100 à 2.000 ouguiyas, par jour de retard, dans la mise en œuvre des mesures prévues au paragraphe précédent, à compter de la date où la violation de l'injonction a été constatée.

Article 37

En cas de condamnation pour une infraction commise par le biais d'un support de communication électronique, le juge peut ordonner, à titre complémentaire, la diffusion au frais du condamné, par extrait en première page et de manière très lisible, de la décision sur ce même support.

La publication prévue à l'alinéa précédent doit être exécutée dans les quinze jours suivant le jour où la condamnation est devenue définitive.

Article 38

Les matériels, équipements, instruments, programmes informatiques ou tous dispositifs ou données en relation avec les infractions prévues par la présente loi, seront saisis.

En cas de condamnation, et sous réserve des droits des tiers de bonne foi, le tribunal prononcera la confiscation des matériels, équipements et instruments ayant servi l'infraction et ordonne la destruction des programmes et données en rapport avec l'infraction.

CHAPITRE VIII : DES REGLES DE PROCEDURE

Article 39

Lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données informatiques sur le territoire national, sont utiles à la manifestation de la vérité, l'autorité judiciaire peut, opérer une perquisition ou accéder de façon similaire, à un système informatique ou à une partie de celui-ci,

ainsi qu'aux données qui y sont stockées, et à un support de stockage informatique permettant de stocker des données informatiques sur son territoire.

Lorsque l'autorité judiciaire a des raisons de penser, que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial, l'autorité judiciaire peut, dans les mêmes conditions, 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 disponible pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par l'autorité judiciaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur.

Article 40

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

Article 41

L'autorité judiciaire désigne toute personne qualifiée pour utiliser les moyens techniques appropriés, afin d'empêcher l'accès aux données visées à l'article précédent dans le système informatique, ou aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique et de garantir leur intégrité, et si besoin leur confidentialité.

Article 42

L'autorité 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 de perquisition et de saisie informatiques.

Article 43

Si les nécessités de l'information l'exigent, notamment lorsqu'il y a des raisons de penser que des données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, sont particulièrement susceptibles de perte ou de modification, l'autorité judiciaire peut faire injonction à toute personne, de conserver et de protéger l'intégrité des données en sa possession ou sous son contrôle, pendant une durée de quatre-vingt-dix jours au maximum, afin de permettre aux autorités judiciaires et aux services d'investigation, d'obtenir leur divulgation. Une telle injonction peut être renouvelée par la suite, pour la bonne marche des investigations judiciaires.

Le gardien des données ou toute autre personne, chargée de conserver celles-ci, est tenu au secret professionnel.

La violation des dispositions de l'alinéa précédent est punie conformément aux dispositions législatives et réglementaires en vigueur.

Article 44

Lorsque les nécessités de l'information l'exigent, le juge d'instruction peut ordonner, à une personne présente sur le territoire national, de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique, et à un fournisseur de services, offrant des prestations sur le territoire national, de communiquer les données en sa possession ou sous son contrôle, relatives aux abonnés et concernant de tels services.

Article 45

Lorsque les nécessités de l'information l'exigent, le juge d'instruction peut collecter ou enregistrer, par l'application de moyens techniques existant sur son territoire, et obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou à 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 son territoire au moyen d'un système informatique.

Article 46

Lorsque les nécessités de l'information l'exigent, s'agissant des infractions dont le maximum de la peine d'emprisonnement n'est pas inférieur à quatre ans, le juge d'instruction peut faire intercepter ou enregistrer par l'application de moyens techniques existant sur son territoire, et obliger un fournisseur de services, dans le cadre de ses capacités techniques, à collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, ou à prêter aux autorités compétentes, son concours et son assistance, pour intercepter ou enregistrer, en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique.

Le fournisseur de services est tenu au secret professionnel.

La violation des dispositions de l'alinéa précédent est punie conformément aux dispositions législatives et réglementaires en vigueur.

Article 47

Les officiers de police judiciaire peuvent, pour les nécessités de l'enquête ou de l'exécution d'une délégation judiciaire, procéder aux opérations prévues par les articles 39 à 45 de la présente loi, dans les conditions de droit.

Ils ne peuvent procéder à la mesure prévue à l'article 46 de la présente loi, dans les conditions prévues par ce texte, que sur autorisation du procureur de la République au cours de l'enquête ou par délégation judiciaire.

CHAPITRE IX : DE LA COMPETENCE DES JURIDICTIONS

Article 48

Les juridictions mauritaniennes sont compétentes pour connaître des infractions prévues par la présente loi :

1. lorsque l'infraction est commise :

- sur le territoire national ;
- à bord d'un navire battant pavillon mauritanien ou d'un aéronef immatriculé selon les lois de la République Islamique de Mauritanie;

2. lorsque l'infraction commise, porte atteinte aux intérêts de l'Etat, ou a pour victime une personne de droit mauritanien ;
3. lorsque l'auteur présumé de l'infraction, se trouve sur le territoire mauritanien et n'est pas extradé vers un autre Etat, au seul titre de sa nationalité, après une demande d'extradition.

Ces règles n'excluent pas l'application d'autres critères de compétence prévus par le code de procédure pénale.

Article 49

La mise en œuvre et l'application des pouvoirs et procédures prévus dans le présent chapitre, qui doivent intégrer le principe de la proportionnalité, sont soumises aux conditions et sauvegardes prévus par les règles applicables en République Islamique de Mauritanie, pour assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application du Pacte International relatif aux droits civils et politiques ou d'autres instruments internationaux applicables, concernant les droits de l'homme.

Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir, ou de la procédure en question.

Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, la République Islamique de Mauritanie, examinera l'effet des pouvoirs et procédures prévus au présent chapitre sur les droits, responsabilités et intérêts légitimes des tiers.

CHAPITRE X : DE LA COOPERATION INTERNATIONALE

Article 50

La République islamique de Mauritanie s'engage à coopérer avec tout Etat tiers, en application des instruments internationaux de coopération pertinents en matière pénale, des arrangements reposant sur des législations uniformes ou réciproques, 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, conformément aux dispositions de la présente loi.

CHAPITRE XI : DES DISPOSITIONS FINALES

Article 51

Les dispositions de la présente loi seront complétées, au besoin, par décrets et arrêtés.