62ème ANNEE N°08 PRIX : 2 500 FCFA DU 01 AU 31 AOÛT 2022

JOURNAL OFFICIEL
DE LA
REPUBLIQUE DU TCHAD

Paraissant du 01 au 30 de chaque mois à N'DJAMENA

ABONNEMENTS	ANNONCES	ABONNEMENTS & INSERTIONS
TCHAD Tous (6 mois)…….…… 15 000 F CFA Voie (1 an)……..…. 30 000 F CFA **AFRIQUE** Voie aérienne (6 mois)…… 30 000 F CFA Exclusivement (1 an)…… 60 000 F CFA **AUTRES PAYS** Voie aérienne (6 mois)…… 60 000 F CFA Exclusivement (1 an)…….……120 000 F CFA	Journal en ligne TIGO CASH *501* 3 // Montant 2 000 F CFA *501// payement partenaires http://www.journal/officieltchad.td	Les abonnements et les insertions seront adressés au : Secrétariat Général du Gouvernement (Direction du Journal Officiel) B.P. 59 Tél. : (235) 22 52 45 19 Fax : (235) 22 52 43 56 Tel : portable (235) 90 44 46 46 99 95 77 77 92 77 48 24 N'DJAMENA (République du Tchad)

SPECIAL

ORDONNANCE

ORDONNANCE N°005/PCMT/2022 Portant Réforme de la Société Nationale des Mines et de la Géologie

LE PRESIDENT DU CONSEIL MILITAIRE DE TRANSITION,
PRESIDENT DE LA REPUBLIQUE,
CHEF DE L'ETAT,
PRESIDENT DU CONSEIL DES MINISTRES,

(/u la Charte de Transition;

(/u la Loi N°018/PCMT/2022 du 04 juillet 2022 portant habilitation du Gouvernement à légiférer par voie d'ordonnances pendant la période allant du 1er Juillet au 31 août 2022 ;

Le Conseil des Ministres consulté à domicile le 26 août 2022 ;

ORDONNE:

Article 1er : Il est substitué à la dénomination : Société Nationale des Mines et de la Géologie, en abrégé « SONAMIG », la dénomination **Société Nationale d'Exploitation Minière et de Contrôle, en abrégé « SONEMIC »**.

Article 2 : La SONEMIC est une société anonyme à capitaux publics.

Elle est dotée de la personnalité juridique et de l'autonomie de gestion. Elle est placée sous la tutelle

du Ministère en charge des Mines et de la Géologie. Son siège est fixé à N'Djamena.

Article 3 : La SONEMIC a pour missions de promouvoir le développement du secteur géologique et minier du Tchad. A ce titre, elle:

- ❖ sert d'instrument de mobilisation de ressources nationales et extérieures au profit des recherches géologiques et minières;
- ❖ concourt au financement des projets se rattachant au développement minier et collabore avec d'autres organismes intervenant dans le domaine des recherches géologiques et minières;
- ❖ conçoit des projets des recherches minières et veille à la mise en œuvre de ses projets;
- ❖ contribue à la réalisation de l'inventaire Minier du Tchad en collaboration avec les structures compétentes du Ministère en charge des Mines et de la Géologie;
- ❖ contribue à l'élaboration des Conventions minières avec les structures compétentes du ministère en charge des mines;
- ❖ détient des titres miniers et autorisation pour la recherche et l'exploitation des substances minérales et assure la mise en œuvre de ces projets;
- ❖ organise l'exploitation artisanale de l'or, d'autres métaux précieux et gemmes en sensibilisant les orpailleurs dans l'utilisation des techniques modernes d'exploitation artisanale et semi-mécanisée ;
- ❖ met en place des comptoirs d'achat et de vente de l'or, d'autres métaux précieux et gemmes, de manière seule et/ou en association avec des tiers;
- ❖ Met en place des unités de traitement et/ou de transformation pour la valorisation de l'or, d'autres métaux précieux et des gemmes, de manière seule et/ou en association avec des tiers;
- ❖ stocke l'or, les autres métaux précieux achetés auprès des artisans miniers;
- ❖ exporte l'or, les autres métaux précieux et gemmes en provenance de l'exploitation artisanale traditionnelle et semi-mécanisée de manière seule et/ou en association avec des tiers;
- ❖ gère les parts de l'Etat dans les sociétés d'exploitation des substances minières ou de carrière sur le territoire national;
- ❖ réalise pour le compte de l'Etat, toute opération minière de manière seule ou en association avec des tiers;
- ❖ suit les conseils d'administration des sociétés minières où elle sera représentée aux côtés des structures techniques;
- ❖ assure la formation et la promotion de son personnel national nécessaire à la maitrise de tous les aspects du secteur des mines et de la géologie;
- ❖ contrôle et supervise à travers une Brigade spéciale dont les modalités d'organisation et de fonctionnement seront fixées par voie règlementaire :

a) les activités minières de toutes les sociétés sur l'ensemble du territoire national;
b) la sécurisation des sites miniers et la répression de la fraude;
c) la canalisation des produits de l'artisanat minier vers les circuits formels;

- ❖ exécute dans le cadre de son objet, toutes missions d'intérêt général que l'Etat pourrait lui confier.

Article 4 : La SONEMIC est administrée conformément à ses Statuts ainsi qu'aux dispositions de l'Acte Uniforme OHADA relatif au Droit des Sociétés Commerciales et du GIE et de celui relatif au Droit Comptable.

Article 5 : Les ressources de la SONEMIC sont constituées de :

- ❖ subventions et autres apports de l'Etat;
- ❖ prélèvement de 10% sur l'ensemble des recettes minières;
- ❖ dons et legs;
- ❖ emprunts;
- ❖ toutes autres ressources provenant de ses activités ou qui viendraient à lui être affectées par la Loi des Finances.

Article 6 : La SONEMIC peut créer des filiales, s'associer aux sociétés nationales ou aux compagnies minières étrangères dans l'exercice de ses activités.

Article 7: Les Statuts de la SONEMIC sont approuvés par Décret pris en Conseil des Ministres.

Article 8 : Toutes les dispositions antérieures contraires sont abrogées notamment l'Ordonnance N°002/PR/2018 du 09 février 2018, portant création d'une Société Nationale des Mines et de la Géologie.

Article 9: La présente Ordonnance sera enregistrée et publiée au Journal Officiel de la République et exécutée comme Loi de l'Etat.

N'Djaména, le 30 Août 2022
Le Général
MAHAMAT IDRISS DEBY ITNO

****

ORDONNANCE N°006/PCMT/2022 Portant création d'un Office du Génie Militaire et de la Production

LE PRESIDENT DU CONSEIL MILITAIRE DE TRANSITION,
PRESIDENTDE LA REPUBLIQUE,
CHEF DE L'ETAT,
PRESIDENT DU CONSEIL DES MINISTRES,

(/u la Charte de Transition;

(/u la Loi N°018/PCMT/2022 du 04 juillet 2022 portant habilitation du Gouvernement à légiférer par voie d'ordonnances pendant la période allant du 1er Juillet au 31 août 2022;

Le Conseil des Ministres consulté à domicile le 31 août 2022 ;

ORDONNE:

Article 1er : Il est créé un Office du Génie Militaire et de la Production en abrégé «**OGEMIP** ».

Article 2: L'OGEMIP est un établissement public à caractère industriel et commercial, doté de la personnalité morale et de l'autonomie de gestion administrative et financière.
Il est placé sous la tutelle du Ministère en charge des Armées.
Son siège est à N'Djamena ; toutefois des antennes peuvent être créées dans les Provinces.
Article 3: L'OGEMIP est régi par un Statut Particulier.
Article 4 : Outre ses missions traditionnelles de participation au combat, aux actions civilo-militaires, d'appui à la mobilité et la contre mobilité opérationnelle, l'OGEMIP a pour missions additionnelles de promouvoir le potentiel du génie militaire en matière de réalisation, de production et d'exploitation dans les domaines des infrastructures, de l'agriculture, de l'élevage, de l'industrie et des mines.
A ce titre, il est notamment chargé de :

- assurer les fonctions de maitre d'œuvre et de conducteur d'opérations de construction d'infrastructures immobilières, routières et aéroportuaires militaires ou civiles;
- assurer l'exploitation industrielle, minière et la production agropastorale;
- créer et gérer des fermes d'élevage intensif;
- suivre et entretenir les bâtiments et infrastructures militaires;
- offrir les prestations intellectuelles relevant de ses domaines de compétence;
- créer et gérer les structures de formation technique des cadres;
- assurer la conservation des archives, l'entretien et la gestion du patrimoine immobilier militaire;
- contribuer à la mobilité opérationnelle des Armées;
- constituer et gérer un dispositif de protection civile;
- créer et gérer des périmètres agropastoraux en collaboration avec les départements techniques concernes, en vue d'appuyer les efforts du Gouvernement pour l'atteinte des objectifs de l'autosuffisance alimentaire.

Article 5 : En tant qu'outil privilégié de contribution des Armées au développement socioéconomique du pays, l'OGEMIP est ouvert à toute coopération ou assistance technique, notamment dans les domaines de la protection civile, des infrastructures, de la production agro-pastorale et de l'exploitation minière.
A ce titre, il est habilité à signer des conventions avec des partenaires publics ou privés, nationaux ou étrangers, des conventions nécessaires au développement de ses activités.
Article 6: L'OGEMIP est structuré comme suit:

- Un Conseil d'Administration;
- Une Direction Générale.

Article 7 : Les ressources de l'OGEMIP proviennent de :

- Subventions et autres apports de l'Etat;
- Produits des prestations; Ressources provenant d'organismes nationaux ou internationaux;
- Dons et legs;
- Toutes autres ressources qui pourraient lui être affectées par la Loi de Finances ou générées par ses activités.

Article 8: Les modalités d'organisation et de fonctionnement de l'OGEMIP sont déterminées par un Décret pris en Conseil des Ministres.
Article 9 : Sont abrogées toutes les dispositions antérieures contraires notamment l'Ordonnance N°006/PR/2019 du 28 août 2019 portant création d'un Office National du Génie Militaire et de la Production.
Article 10 : La présente Ordonnance sera enregistrée au Journal Officiel de la République et exécutée comme Loi de l'Etat.

N'Djaména, le 30 Août 2022
Le Général
MAHAMAT IDRISS DEBY ITNO

****

ORDONNANCE N°007/PCMT/2022 Portant sur la Cybercriminalité et Cyberdéfense en République du Tchad

LE PRESIDENT DU CONSEIL MILITAIRE DE TRANSITION,
PRESIDENT DE LA REPUBLIQUE,
CHEF DE L'ETAT,
PRESIDENT DU CONSEIL DES MINISTRES,

(/u la Charte de Transition;
(/u la Loi N°018/PCMT/2022 du 04 juillet 2022 portant habilitation du Gouvernement à légiférer par voie d'ordonnances pendant la période allant du 1er Juillet au 31 août 2022 ;
Le Conseil des Ministres consulté à domicile le 31 août 2022 ;

ORDONNE:

CHAPITRE PREMIER : DES DISPOSITIONS GENERALES
Section première: De l'objet et du champ d'application
Article 1er : La présente loi fixe:

- Les infractions de cybercriminalité ;
- les règles de procédure et les dispositions pénales dans la lutte contre la cybercriminalité ;
- les règles et les dispositions de sécurité applicables aux infrastructures d'importance vitale.

Section II: Définitions
Article 2: Au sens de la présente loi, on entend par:

- « **Cyberdéfense** » : Ensemble de moyens physiques et virtuels permettant à un État de protéger ses systèmes d'information vitaux dans le cyberespace.
- « **Cyberterrorisme** » Ensemble des attaques graves (virus, piratage, etc.) et à grande échelle des ordinateurs, des réseaux et des systèmes informatiques d'une entreprise, d'une institution ou d'un État, commises dans

le but d'entraîner une désorganisation générale susceptible de créer la panique.

- « **Cybersécurité**» l'ensemble de mesures, procédures, concepts de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques, et technologies permettant à un système d'information de résister à des évènements issus du cyberespace, susceptibles de compromettre .la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ce système offre ou qu'il rend accessibles;
- «**Cybercriminalité** » : l'ensemble des actes contrevenant à la législation nationale ou aux traités internationaux ratifiés par la République du Tchad, ayant pour cible les réseaux ou les systèmes d'information ou les utilisant comme moyens de la commission d'un délit ou d'un crime;
- « **Cybermenace** » : toute action qui vise à compromettre la sécurité d'un système d'information en altérant la disponibilité, l'intégrité ou la confidentialité d'un système ou de l'information qu'il contient;
- « **Cyberéthique**»: l'ensemble des normes et règles pour un comportement responsable dans le cyberespace ;
- « **Infrastructures d'importance vitale**» : les installations, les ouvrages et les systèmes qui sont indispensables au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social, et dont le dommage ou l'indisponibilité ou la destruction aurait un impact induisant la défaillance de ces fonctions;
- «**Secteur d'activités d'importance vitale**» : l'ensemble des activités exercées par les infrastructures d'importance vitale et concourant à un même objectif. Ces activités ont trait soit à la production et la distribution de biens ou de services indispensables à la satisfaction des besoins essentiels pour la vie des populations, ou à l'exercice des prérogatives de l'Etat ou au maintien de ses capacités de sécurité ou au fonctionnement de l'économie, dès lors que ces activités sont difficilement substituables ou remplaçables, ou qui peuvent présenter un danger grave pour la population;
- «**Système d'information**» : un ensemble organisé de ressources telles que les personnels, matériels, logiciels, données et procédures qui permettent de collecter, de classifier, de traiter et de diffuser l'information sur un environnement donné;
- « **Système d'information sensible** » système d'information traitant des informations ou des données sensibles sur lesquelles une atteinte à la confidentialité, à l'intégrité ou à la disponibilité porterait préjudice à une entité ou à une infrastructure d'importance vitale;
- « **Service de cybersécurité** »: tout service de sécurité fourni par des prestataires de services de cybersécurité à une entité ou à une infrastructure d'importance vitale et portant sur la détection et le diagnostic des incidents de cybersécurité et le renforcement de la sécurité de leurs systèmes d'information;
- « **Prestataire de services numériques** » : toute personne physique ou morale qui fournit à distance, par voie électronique et à la demande d'un destinataire, l'un des services ci-après:
    - un service numérique qui permet à des consommateurs ou à des professionnels de conclure des contrats de vente ou de service en ligne;
    - un service numérique qui permet aux utilisateurs d'effectuer des recherches sur les sites Internet;
    - un service numérique qui permet l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées, y compris les hébergeurs de données et/ou systèmes d'information (Datacenter) et les prestataires des services d'informatique en nuage (Cloud) ;
- « **Hébergement**» : toute prestation de stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournie, à titre onéreux ou gratuit, par des prestataires de services numériques;
- « **Externalisation d'un système d'information**» : toute opération qui consiste à confier, en partie ou en totalité, le système d'information d'une entité à un prestataire dans le cadre d'un contrat fixant de façon précise notamment le niveau de services et la durée de l'externalisation ;
- « **Homologation des systèmes d'information**» : document par lequel le responsable d'une infrastructure d'importance vitale atteste de sa connaissance du système d'information et des mesures de sécurité techniques, organisationnelles ou juridiques mises en œuvre et accepte les risques résiduels;

- « **Incident de cybersécurité**» : un ou plusieurs événements indésirables ou inattendus liés à la sécurité des systèmes d'information et présentant une forte probabilité de compromettre les activités d'une entité, d'une infrastructure d'importance vitale ou d'un opérateur ou de menacer la sécurité de leurs systèmes d'information;
- « **Crise cybernétique**» : l'état résultant de l'occurrence d'un ou plusieurs événements de cybersécurité pouvant avoir un impact grave sur la vie des populations, l'exercice de l'autorité de l'Etat, le fonctionnement de l'économie, ou sur le maintien des capacités de sécurité et de défense du pays;
- « **Gestion des incidents de cybersécurité** » le processus de détection, de signalement et d'évaluation des incidents de cybersécurité, ainsi que les mesures d'intervention et de traitement y afférentes.

CHAPITRE II : DE LA CYBERCRIMINALITE
SECTION I : DES DISPOSITIONS PROCEDURALES

Article 3 : En cas d'infraction relevant de la cybercriminalité, les officiers de police judiciaire et les agents habilités de l'ANSE procèdent aux enquêtes conformément aux dispositions du Code de Procédure Pénale en vigueur.

Article 4: Lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données sur le territoire national, sont utiles à la manifestation de la vérité, les officiers de police judiciaire et les agents habilités de l'ANSE peuvent perquisitionner, accéder ou ordonner de perquisitionner ou d'accéder au système informatique ou à une partie de celui-ci ou au support de stockage.

Article 5: Lorsque les officiers de police judiciaire et les agents habilités de l'ANSE perquisitionnent, accèdent ou ordonnent la perquisition ou l'accès d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément à l'article précédent et 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, ceux-ci peuvent étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système.

Article 6 : Lorsque les officiers de police judiciaire et les agents habilités de l'ANSE découvrent dans un système informatique des données qui sont utiles à la manifestation de la vérité, mais que la saisie du support ne paraît pas souhaitable, ils peuvent saisir, ordonner la saisie ou l'obtenir d'une façon similaire des données informatiques pour lesquelles l'accès a été réalisé en application de l'article précédent. Cette mesure inclut les prérogatives suivantes:

a) saisie ou obtention d'une façon similaire d'un système informatique ou d'une partie de celui-ci, ou un support de stockage informatique;
b) réalisation et conservation d'une copie de ces données;
c) préservation de l'intégrité des données informatiques stockées jugées pertinentes;
d) action en vue de rendre inaccessibles ou en vue d'enlever ces données informatiques du système informatique consulté.

Article 7 : Les officiers de police judiciaire et les agents habilités de l'ANSE peuvent 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 par le présent article, et par l'article précédent.

Article 8 : En cas de condamnation, le tribunal peut prononcer la confiscation des matériels, équipements, instruments, programmes informatiques ou données ainsi que des sommes aux produits résultant de l'infraction et appartenant au condamné.

Article 9 : L'écrit électronique en matière pénale est admis comme mode de preuve au même titre que l'écrit sur support papier pour établir les infractions à la loi pénale sous réserves des conditions suivantes:

a) d'une part, qu'elle soit apportée au cours des débats contradictoires et discutée devant le juge;
b) d'autre part, que puisse être dûment identifiée la personne dont elle émane et qu'elle soit établie et conservée dans des conditions de nature à garantir son intégrité.

Article 10 : Les officiers de police judiciaire et les agents habilités de l'ANSE ont accès, lors des investigations, aux moyens de transport, à tout local à usage professionnel, à l'exclusion des domiciles privés, en vue de rechercher, de constater les infractions, de demander la communication de tous les documents professionnels et d'en prendre copie, de recueillir, sur convocation ou sur place, les renseignements et justifications nécessaires à l'accomplissement de leur mission.

Article 11 : Les perquisitions en matière de cybercriminalité sont susceptibles de porter sur des données stockées sur des supports physiques ou des copies réalisées en présence des personnes qui assistent à la perquisition.

Lorsqu'une copie des données saisies a été faite, celle-ci peut être détruite sur instruction du Procureur de la République pour des raisons de sécurité.

Sur accord du Procureur de la République, seuls seront gardés sous scellé par l'officier de Police Judiciaire, les objets, documents et données utilisées à la manifestation de la vérité.

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

Article 12 : Les perquisitions et les saisies sont effectuées dans les conditions prévues par le Code de Procédure Pénale.

Article 13 : Lorsqu'il apparaît que les données saisies ou obtenues au cours de l'enquête ou de l'instruction

ont fait l'objet d'opérations de transformation empêchant d'accéder en clair ou sont de nature à compromettre les informations qu'elles contiennent, le Procureur de la République, le Juge d'instruction ou la juridiction de jugement peuvent réquisitionner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair desdites données.

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

Article 14: La réquisition prévue à l'article 19 ci-dessus peut être faite à tout expert. Dans ce cas, son exécution est faite conformément aux dispositions du Code de Procédure Pénale relative à la commission d'expert.

Article 15 : Les autorités judiciaires tchadiennes peuvent donner commission rogatoire tant nationale qu'internationale, à toute personne physique ou morale pour rechercher les éléments constitutifs des infractions de cybercriminalité, dont au moins l'un des éléments constitutifs a été commis sur le territoire de la République du Tchad ou dont l'un des auteurs ou complices se trouve dans ledit territoire.

Sous réserve des règles de réciprocité entre le Tchad et les pays tiers liés par un accord de coopération judiciaire, les commissions rogatoires sont exécutées conformément aux dispositions du Code de Procédure Pénale.

Article 16 : Les personnes physiques ou morales qui fournissent des prestations de cryptographie visant à assurer une fonction de confidentialité, sont tenues de remettre aux officiers de police judiciaire ou aux agents habilités de l'ANSE sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies.

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

Article 17 : Lorsque les nécessités de l'enquête ou de l'instruction le justifient, l'audition ou l'interrogatoire d'une personne et/ou la confrontation entre plusieurs personnes, peuvent être effectuées en plusieurs points du territoire national se trouvant reliés par des moyens de communications électroniques garantissant la confidentialité de la transmission. Il est dressé, dans chacun des lieux, un procès-verbal des opérations qui y ont été effectuées. Ces opérations peuvent faire l'objet d'enregistrement audiovisuel et/au sonore.

Lorsque les circonstances l'exigent, l'interprétation peut être faite au cours d'une audition, d'un interrogatoire ou d'une confrontation par des moyens de communications électroniques.

Les dispositions du présent article sont également applicables pour l'exécution simultanée, sur un point du territoire national et sur un point situé à l'extérieur, des demandes d'entraide émanant des autorités judiciaires étrangères ou des actes d'entraide réalisés à l'étranger sur demande des autorités judiciaires tchadiennes.

Article 18 : Si les nécessités de l'information l'exigent, notamment lorsqu'il y a des raisons de penser que des données informatiques stockées dans un système informatique sont particulièrement susceptibles de perte ou de modification, les officiers de police judiciaire et les agents habilités de l'ANSE peuvent 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 deux (2) ans maximum, pour la bonne marche des investigations judiciaires.

Article 19 : La personne en charge de la garde des données est tenue de garder le secret sur la mise en œuvre desdites procédures.

Article 20 : Les officiers de police judiciaire et les agents habilités de l'ANSE peuvent ordonner:

a) 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;
b) 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 21 : Pour la constatation des infractions définies par la présente loi, les officiers de police judiciaire et les agents habilités de l'ANSE peuvent utiliser les moyens techniques appropriés pour collecter ou enregistrer en temps réel, les données relatives au contenu de communications spécifiques sur le territoire national, transmises au moyen d'un système informatique. Ils peuvent dans les mêmes circonstances, obliger un fournisseur de services, en considération de ses capacités techniques, à prêter aux autorités compétentes, son concours et son assistance pour la collecte ou enregistrement de ces données.

Article 22 : Le fournisseur de services a l'obligation de garder le secret sur les informations reçues.

Article 23 : Les officiers de police judiciaire et les agents habilités de l'ANSE peuvent collecter, enregistrer ou ordonner la collecte ou l'enregistrement par l'utilisation de moyens techniques existant sur le territoire national ou obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes :

a) à collecter ou à enregistrer les informations requises par l'utilisation de moyens techniques existant sur son territoire;
b) à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives aux trafics associés à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

Article 24 : Le fournisseur de services est tenu de garder le secret sur le fait que l'un quelconque des pouvoirs prévus dans le présent article ait été exécuté ainsi que toute information à ce sujet.

Article 25 : Si les officiers de police judiciaire et les agents habilités de l'ANSE sont convaincus que dans le cadre d'une enquête concernant une infraction prévue par la présente loi, il y a des motifs

raisonnables de croire que des preuves essentielles ne peuvent pas être collectées par l'application d'autres instruments énumérés au chapitre I, du titre III de la présente loi, ils peuvent utiliser un logiciel à distance et l'installer dans le système informatique de la personne mise en cause afin de recueillir les éléments de preuve pertinents recherchés. Afin d'éviter tout abus, la démarche doit nécessairement mentionner par écrit les informations suivantes:

a) la personne mise en cause, si possible avec nom et adresse;
b) la description du système informatique ciblée;
c) la description de la mesure envisagée, l'étendue et la durée de l'utilisation
d) les raisons de la nécessité de l'utilisation du logiciel.

Article 26 : Lorsqu'il y a des raisons de penser que des données archivées dans un système informatique sont particulièrement susceptibles de perte ou de modification, le juge d'instruction peut faire injonction à toute personne de conserver et de protéger l'intégrité des données en sa possession ou sous son contrôle pendant une durée de dix (10) ans maximums, pour la bonne marche des investigations judiciaires.

La personne en charge de la garde des données ou toute autre personne chargée de conserver celles-ci sont tenues d'en garder le secret.

Toute violation du secret est punie des peines applicables au délit de violation du secret professionnel.

Article 27 : Si les nécessités de l'information l'exigent et lorsqu'il y a des raisons de craindre la disparition des données archivées valant preuve, le juge d'instruction peut faire injonction à toute personne de conserver et de protéger dans le secret l'intégrité des données en sa possession ou sous son contrôle, pendant une durée de dix (10) ans maximums, pour la bonne marche des investigations judiciaires.

Article 28 : lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données sur le territoire national, sont utiles à la manifestation de la vérité, le juge peut opérer une perquisition ou accéder à un système informatique ou à une partie de celui-ci ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponible pour le système initial.

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

Article 29 : Lorsque le juge découvre dans un système informatique des données stockées qui sont utiles à 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 désigne toute personne qualifiée pour utiliser les moyens techniques appropriées afin d'empêcher l'accès aux données visées à l'alinéa ci-dessus 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.

Si les données qui sont liées à l'infraction, soit qu'elles en constituent l'objet, soit qu'elles en ont été 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 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 2 du présent article n'est pas possible, pour des raisons techniques ou en raison du volume des données, le juge utilise les moyens techniques appropriées 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 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.

Article 30 : Lorsqu'il apparaît que les données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait l'objet d'opérations de transformation empêchant d'accéder en clair ou sont de nature à compromettre les informations qu'elles contiennent, le Procureur de la République, le Juge d'instruction ou la juridiction de jugement peuvent réquisitionner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair desdites données.

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

Article 31 : Si les nécessités de l'information l'exigent. le juge d'instruction peut, sur réquisition du Procureur de la République, utiliser les moyens techniques appropriés pour collecter ou enregistrer en temps réel, les données relatives au contenu des communications spécifiques, transmises au moyen d'un système informatique ou obliger un fournisseur de services, dans le cadre de ses capacités techniques à collecter ou à enregistrer, avec les moyens techniques existants, ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer lesdites données informatiques.

Le fournisseur d'accès est tenu de garder le secret. Toute violation du secret est punie des peines applicables au délit de violation de secret professionnel.

Article 32 : En cas de condamnation pour une infraction commise par le biais d'un support de communication numérique, la juridiction saisie peut prononcer à titre de peines complémentaires l'interdiction d'émettre des messages de

communication numérique, l'interdiction à titre provisoire au définitif de l'accès au site ayant servi à commettre l'infraction, en couper l'accès par tous moyens techniques disponibles ou même en interdire l'hébergement.

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, d'hébergement ou la coupure de l'accès au site incriminé.

Article 33 : En cas de condamnation pour une infraction commise par le biais d'un support numérique, le juge ordonne à titre complémentaire la diffusion au frais du condamné, par extrait, de la décision sur ce même support.

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

La personne condamnée qui ne fera pas diffuser ou qui ne diffusera pas l'extrait prévu à l'alinéa précédent sera puni des peines prévues par le Code pénal.

Si dans le délai de quinze (15) jours après que la condamnation soit devenue définitive, la personne condamnée n'a pas diffusé ou fait diffuser cet extrait, les peines prévues au présent article sont portées au double.

SECTION II: DISPOSITIONS PROPRES AUX INFRASTRUCTURES D'IMPORTANCE VITALE DISPOSANT DE SYSTEMES D'INFORMATION SENSIBLES

Article 34: Les dispositions de la section première du présent chapitre s'appliquent aux infrastructures d'importance vitale.

Article 35: La liste des secteurs d'activités d'importance vitale et des autorités gouvernementales, établissements publics ou autres personnes morales de droit public, assurant la coordination de ces secteurs est fixée par voie réglementaire.

Article 36 : Les infrastructures d'importance vitale sont désignées pour chaque secteur d'activité d'importance vitale par l'autorité gouvernementale, l'établissement public ou la personne morale de droit public dont relève la coordination de ce secteur, et ce après avis de l'ANSE.

La liste de ces infrastructures doit être tenue secrète et doit être actualisée à intervalles réguliers et au moins tous les deux ans.

Article 37 : Le responsable de l'infrastructure d'importance vitale établit, sur la base des résultats d'une analyse des risques, la liste des systèmes d'information sensibles et la transmet avec les mises à jour de celle-ci à l'ANSE.

Article 38: L'ANSE peut faire des observations au responsable de l'infrastructure d'importance vitale sur la liste des systèmes d'information sensibles qui lui a été transmise.

Dans ce cas, le responsable de l'infrastructure d'importance vitale est tenu de modifier sa liste conformément à ces observations et transmet la liste modifiée à l'ANS dans un délai de deux mois à compter de la date de réception des observations.

La liste des systèmes d'information sensibles doit être tenue secrète.

Article 39: Tout système d'information sensible doit faire l'objet d'une homologation de sa sécurité par l'ANSE avant sa mise en exploitation.

Le guide d'homologation des systèmes d'information sensibles est fixé par l'ANSE.

Article 40: A la demande de l'ANSE, les responsables des infrastructures d'importance vitale soumettent les systèmes d'information sensibles desdites infrastructures à un audit effectué par l'ANSE ou par des prestataires d'audit qualifiés par l'ANSE.

Les critères de qualification des prestataires d'audit et les modalités de déroulement de l'audit sont fixés par voie réglementaire.

Article 41: Les responsables des infrastructures d'importance vitale sont tenus de communiquer à l'ANSE ou au prestataire d'audit qualifié les informations et éléments nécessaires pour réaliser l'audit, y compris les documents relatifs à leur politique de sécurité et, le cas échéant, les résultats d'audit de sécurité précédents, et leur permettre d'accéder aux réseaux et systèmes d'information faisant l'objet du contrôle afin d'effectuer des analyses et des relevés d'informations techniques.

Les prestataires d'audit qualifiés et leurs employés sont astreints, sous peine des sanctions prévues par le code pénal, au respect du secret professionnel pendant toute la durée de la mission d'audit et après son achèvement, sur les renseignements et documents recueillis ou portés à leur connaissance à l'occasion de cette mission.

Article 42: Lorsque l'audit est effectué par un prestataire d'audit qualifié, le rapport d'audit est transmis par le responsable de l'infrastructure d'importance vitale à l'ANSE.

Le prestataire d'audit qualifié doit veiller à la confidentialité du rapport d'audit.

Article 43: Lorsque les opérations d'audit sont effectuées par les prestataires d'audit qualifiés, les coûts sont supportés par le responsable de l'infrastructure d'importance vitale concernée par ces opérations.

Article 44 : Chaque responsable d'infrastructure d'importance vitale auditée doit mettre en place un plan d'actions pour mettre en œuvre les recommandations figurant dans les rapports d'audit et le transmet à l'ANSE pour le suivi de sa mise en œuvre.

Article 45 : Les responsables des infrastructures d'importance vitale doivent recourir à des services, produits ou solutions qui permettent le renforcement des fonctions de sécurité, définis par l'ANSE.

En cas d'externalisation des services de cybersécurité, les responsables des infrastructures d'importance vitale doivent recourir à des prestataires qualifiés par l'ANSE.

Les critères de qualification des prestataires de services de cybersécurité sont fixés par voie réglementaire.

SECTION III : De la défense des infrastructures vitales.

Article 46: Pour répondre à une attaque informatique qui vise les systèmes d'information affectant le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation, les services de l'ANSE, peuvent procéder aux opérations techniques nécessaires à la caractérisation de l'attaque et à la

neutralisation de ses effets en accédant aux systèmes d'information qui sont. à l'origine de l'attaque.

Pour être en mesure de répondre aux attaques mentionnées au premier alinéa, l'ANSE peut détenir des équipements, des instruments, des programmes informatiques et tous outils numériques susceptibles de combattre efficacement ces actes de malveillance.

Article 47 : Lorsqu'elle a connaissance d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information vitales, l'ANSE peut mettre en œuvre, sur le réseau d'un opérateur de communications électroniques ou sur le système d'information d'un particulier des dispositifs mettant en œuvre des marqueurs techniques aux seules fins de détecter des événements susceptibles d'affecter la sécurité des systèmes d'information vitales. Ces dispositifs sont mis en œuvre pour la durée et dans la mesure strictement nécessaire à la caractérisation de la menace.

Les agents de l'ANSE individuellement désignés et spécialement habilités sont autorisés, aux seules fins de prévenir et de caractériser la menace affectant les systèmes d'information vitales, à procéder au recueil et à l'analyse des seules données techniques pertinentes, à l'exclusion de toute autre exploitation.

Les données techniques recueillies directement par l'ANSE ne peuvent être conservées plus de dix ans. Les données recueillies autres que celles directement utiles à la prévention et à la caractérisation des menaces sont immédiatement détruites.

CHAPITRE III DES INFRACTIONS DE CYBERCRIMINALITE

SECTION I : DES ATTEINTES AUX SYSTEMES INFORMATIQUES

Sous-Section 1 : Des atteintes à la confidentialité et à l'intégrité des systèmes informatiques

Article 48 : Est punie d'un emprisonnement d'un (1) an à cinq ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement toute personne qui accède ou tente d'accéder frauduleusement à tout ou partie d'un système informatique.

Est puni des mêmes peines, celui qui se procure ou tente de se procurer frauduleusement, pour soi-même au pour autrui, un avantage quelconque en s'introduisant dans un système informatique.

Article 49 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement toute personne qui se maintient ou tente de se maintenir frauduleusement dans tout ou partie d'un système informatique.

Article 50 : Est punie d'un emprisonnement d'un (1)an a cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui entrave, fausse ou tente d'entraver ou de fausser le fonctionnement d'un système informatique.

Sous-Section 2 : De l'introduction frauduleuse de données dans un système

Article 51 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement toute personne qui introduit ou tente d'introduire frauduleusement des données dans un système informatique.

SECTION II : DES ATTEINTES AUX DONNEES INFORMATIQUES

Sous-Section 1 : De la falsification et de l'usage des données falsifiées.

Article 52 : Est punie d'un emprisonnement de cinq (5) ans à dix (10) ans et d'une amende de cinq (5) millions à cinquante (50) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui introduit ou tente d'introduire, altère ou tente d'altérer, efface ou tente d'effacer, supprime ou tente de supprimer Frauduleusement 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 au non directement lisibles et intelligibles.

Article 53 : Est punie d'un emprisonnement de cinq (5) ans à dix (10) ans et d'une amende de trois (3) millions à trente (30) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui en connaissance de cause, fait usage des données obtenues dans les conditions énoncées par l'article 88 ci-dessus.

Article 54 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne, qui intercepte ou tente d'intercepter frauduleusement par des moyens techniques des données informatisées lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système informatique.

Article 55 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui endommage ou tente d'endommager, efface ou tente d'effacer, détériore ou tente de détériorer, altère ou tente d'altérer, modifie ou tente de modifier frauduleusement des données informatiques.

Article 56 : Est punie d'un emprisonnement d'un (1) an a cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui produit ou fabrique un ensemble de données numérisées par l'introduction, l'effacement ou la suppression frauduleuse de données informatisées stockées, traitées ou transmises par un système informatique, engendrant des données contrefaites, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient originales.

Article 57 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui obtient frauduleusement, pour lui-même ou pour autrui, un avantage quelconque, par l'introduction, l'altération, l'effacement ou la suppression de données informatisées ou par toute forme d'atteinte au fonctionnement d'un système informatique.

Article 58 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui, même par négligence,

procède ou fait procéder à des traitements de données à caractère personnel sans avoir respecté les formalités préalables à leur mise en œuvre prévues par la loi sur les données personnelles prévue à cet effet.

Sous-Section 2 : Des abus de dispositifs

Article 59 : Est punie d'un emprisonnement d'un (1) an à trois (3) ans et d'une amende d'un (1) million a dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui produit vend, importe, détient, diffuse, offre, cède ou met à disposition :

a) un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions visées par les articles 51, 52, 53, 54 et 55 ci-dessus;
b) 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 des infractions visées par les articles 51,52, 53, 54 et 55 ci-dessus.

Les auteurs de l'une des infractions prévues à l'article 81 ci-dessus encourent également les peines complémentaires suivantes:

a) la confiscation, selon les modalités prévues par les textes en vigueur, de tout objet destiné ou ayant servi à commettre l'infraction considéré, à l'exception des objets susceptibles de restitution;
b) l'interdiction dans les conditions prévues par les textes en vigueur pour une durée de cinq (5) ans au moins, d'exercer une fonction publique ou une activité socioprofessionnelle, lorsque les faits ont été commis dans l'exercice ou à l'occasion de l'exercice des fonctions de la personne incriminée;
c) la fermeture, dans les conditions prévues par les textes en vigueur, pour une durée de cinq (5) ans au moins, des établissements ou de l'un ou plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés;
d) d) l'exclusion, pour une durés de cinq (5) ans au moins, des marchés publics.

Sous-Section 3 : De l'usurpation d'identité numérique, de l'association de malfaiteurs informatiques et de ta complicité.

Article 60 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement. Toute personne qui usurpe l'identité numérique d'un tiers ou une ou plusieurs données permettant d'identifier, en vue de troubler sa tranquillité ou celle d'autrui ou de porter atteinte à son honneur, à sa considération ou à ses intérêts.

Article 61 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement toute personne qui participe à une association formée ou à une entente établie en vue de préparer ou de commettre une ou plusieurs des infractions prévues dans la présente loi.

Article 62 Une personne qui intentionnellement commet un acte de complicité en vue de la perpétration d'une des infractions prévues par la présente loi, dans l'intention qu'une telle infraction soit perpétrée, commet une infraction punissable des mêmes peines que celles prévues pour l'infraction principale.

SECTION III : DES INFRACTIONS RELATIVES AU CONTENU

Sous-Section 1: De la pornographie enfantine.

Article 63 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui produit en vue de sa diffusion, tente de produire en vue de la vente, offre, met à disposition, diffuse ou tente de diffuser de la pornographie enfantine par le biais d'un système informatique.

Article 64 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement toute personne qui se procura ou procure à autrui, importe au fait importer, exporter ou fait exporter de la pornographie enfantine par le biais d'un système informatique.

Article 65 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui possède Intentionnellement de la pornographie enfantine dans un système informatique ou dans un moyen quelconque de stockage de données informatiques.

Article 66 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) million de francs, ou de l'une de ces deux peines seulement toute personne qui facilite l'accès des mineurs à des images, des documents, du son ou une représentation présentant un caractère de pornographie.

Article 67 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) million de francs, ou de l'une de ces deux peines seulement, toute personne qui propose intentionnellement, par le biais des technologies de l'information et de la communication, une rencontre à un enfant mineur, dans le but de commettre à son encontre une des infractions prévues par les articles 62,63,64 et 65 ci-dessus.

Lorsque la proposition sexuelle a été suivie d'actes matériels conduisant à ladite rencontre, l'auteur commet une infraction aggravé punissable d'un emprisonnement de cinq (5) ans à dix (10) ans et d'une amende de deux (2) millions à vingt (20) millions de francs, au de l'une de ces deux peines seulement.

Sous-Section 2 : Des actes racistes et xénophobes par le biais d'un système informatique

Article 68 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui crée, télécharge, diffuse ou met à disposition sous quelle que forme que ce soit des écrits, messages, photos, dessins ou toute autre représentation d'idées ou de théories, de nature

raciste ou xénophobe, par le biais d'un système informatique.

Article 69 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) à dix (10) millions de francs, ou de l'une de ces deux peines seulement.

Toute personne auteur de menace commise par le biais d'un système informatique envers une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance, l'affiliation ou l'origine nationale ou ethnique, ou la religion dans la mesure où cette appartenance sert de prétexte à l'un ou l'autre de ces éléments, ou un groupe de personnes qui se distingue par une de ces caractéristiques.

Article 70 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement toute personne auteur d'une insulte commise par le biais d'un système informatique envers 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, la religion, l'affiliation au l'opinion politique dans la mesure où cette appartenance sert de prétexte à l'un ou l'autre de ces éléments, ou un groupe de personnes qui se distingue par une de ces caractéristiques.

Article 71 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement toute personne qui, intentionnellement, nie, approuve ou justifie des actes constitutifs de génocide ou de crimes contre l'humanité par le biais d'un système informatique.

SECTION IV : DE LA NON EXECUTION DES INJONCTIONS ET DE LA DIVULGATION DES INFORMATIONS D'ENQUETE

Article 72 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement toute personne, autre que le mis en cause, qui omet intentionnellement sans excuse légitime ou justification de se conformer à une injonction des officiers de police judiciaire et des agents habilités de l'ANSICE.

Article 73 : Est puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, tout fournisseur de service qui reçoit une injonction, dans le cadre d'une enquête criminelle, qui stipule explicitement que la confidentialité doit être maintenue ou qu'elle résulte de la loi et qui, intentionnellement et sans excuse ou justification légitime divulgue les informations relatives à l'enquête.

Article 74 : Est puni (e) d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, le responsable légal du site ayant servi à commettre l'infraction ou toute personne qualifiée pour 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 et qui ne respecte pas les injonctions émises par le juge à cet effet.

SECTION V : DES INFRACTIONS EN MATIERE DE CRYPTOLOGIE

Article 75 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement toute personne qui n'aura pas satisfait à l'obligation de communiquer à l'Autorité publique en charge de la cryptologie une description des caractéristiques techniques des moyens de cryptologie conformément aux textes s'y rapportant

Article 76 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement toute personne qui aura importé un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité, sans satisfaire à l'obligation de déclaration préalable auprès de l'Autorité publique en charge de la cryptologie.

Article 77 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui aura fourni des prestations de cryptologie sans en avoir obtenu préalablement l'agrément de l'Autorité publique en charge de la cryptologie.

Article 78 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement toute personne qui aura exporté un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sans en avoir obtenu préalablement l'autorisation de l'Autorité publique en charge de la cryptologie.

Article 79: Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amande d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui aura mis à la disposition d'autrui un moyen de cryptologie ayant fait l'objet d'une interdiction d'utilisation et de mise en circulation.

Article 80 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui utilise un moyen de cryptologie pour préparer ou commettre un crime ou un délit ou pour en faciliter la préparation ou la commission.

SECTION VI : DU SPAMMING

Article 81 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui, de manière intentionnelle et sans excuse ou justification légitime:

a) déclenche intentionnellement la transmission de courriers électroniques multiples à partir ou par l'intermédiaire d'un système informatique;
b) utilise un système informatique protégé pour relayer ou retransmettre des courriers électroniques multiples dans l'intention de tromper ou d'induire en erreur, quant à l'origine de ces messages les destinataires ou

tout prestataire de services de courriers électroniques ou de services internet;

c) falsifie matériellement les informations se trouvant dans les en-têtes de messages électroniques multiples et déclenche intentionnellement la transmission desdits messages.

CHAPITRE IV : DE L'ADAPTATION DES INFRACTIONS CLASSIQUES AUX TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

SECTION I : DES INFRACTIONS CONTRE LES BIENS

Article 82 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui copie ou tente de copier frauduleusement des données Informatiques au préjudice d'un tiers.

Article 83 : Est punie d'un emprisonnement d'un (1)an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui, sait en faisant usage de faux noms ou de fausses qualités, sait en employant des manœuvres frauduleuses quelconques, aura obtenu la remise ou aura tenté d'obtenir la remise de données informatiques et aura par un de ces moyens, escroqué ou aura tenté d'escroquer en partie ou en totalité la fortune d'autrui.

Article 84 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, ou de l'une de ces deux peines seulement, toute personne qui, ayant reçu des propriétaires, possesseurs, ou détenteurs des données informatiques à titre de louage, de dépôt, de mandat de nantissement, de prêt à usage ou pour un travail salarié ou non salarié, n'aura pas, après simple mise en demeure, exécuté son engagement de les rendre ou de les représenter, ou d'en faire un usage ou un emploi déterminé.

Article 85 : Est punie d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende d'un (1) million à dix (10) millions de francs, au de l'une de ces deux peines seulement, toute personne qui, sciemment, aura recelé, en tout ou en partie, des données informatiques enlevées, détournées ou obtenues à l'aide d'un crime ou d'un délit.

Article 86 : Est considérée comme infraction aggravée et punie d'un emprisonnement de cinq (5) ans à dix (10) ans et d'une amende de (10) millions à cinquante (50) millions de francs, ou de l'une de ces deux peines seulement, le fait pour toute personne qui, soit en faisant usage de faux noms au de fausses qualités, soit en employant des manœuvres frauduleuses quelconques, se sera fait remettre ou délivrer, ou aura tenté de se faire remettre ou délivrer des fonds, des meubles ou des obligations, billets, promesses, quittances ou décharges par le biais d'un système informatique ou d'un réseau de communication électronique et aura par un de ces moyens, escroqué ou tenté d'escroquer en partie ou en totalité la fortune d'autrui.

SECTION II : DES ATTEINTES A LA DEFENSE NATIONALE

Article 87 : Est puni d'un emprisonnement de cinq (5) ans à dix (10) ans, tout citoyen tchadien qui:

a) livre à une puissance étrangère ou à ses agents, sous quelle que forme au par quelque moyen que ce soit, un renseignement, objet, document, procédé, donnée numérisée ou fichier informatisé qui doit être tenu secret dans l'intérêt de la défense nationale;

b) s'assure, par quelque moyen que ce soit, la possession d'un tel renseignement, objet, document procédé, donnée informatisée ou fichier informatisé en vue de le livrer à une puissance étrangère ou à ses agents;

c) détruit ou laisse détruire un renseignement, objet document, procédé, une donnée informatisée ou un fichier informatisé en vue de le (la) livrer à une puissance étrangère.

SECTION III: DES INFRACTIONS DE PRESSE

Article 88 : Une personne qui commet une infraction de presse, notamment une diffamation, une injure publique, une apologie de crime, par le biais d'un moyen de communication électronique public, commet une infraction punissable, sur déclaration de culpabilité, des mêmes peines que celles prévues pour les infractions de presse commises par d'autres moyens.

SECTION IV : DE LA RESPONSABILITE DES PERSONNES MORALES

Article 89 : Les personnes morales autres que l'État, les collectivités territoriales décentralisées et les établissements publics sont responsables des infractions prévues par la présente loi, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein et qui est 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.

Article 90 : Outre les cas déjà prévus à l'article 87 ci-dessus, une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée audit article a rendu possible la commission des infractions prévues par la présente loi pour le compte de ladite personne morale par une personne physique agissant sous son autorité.

Article 91 : La responsabilité des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits.

Article 92 : Les peines encourues par les personnes morales sont:

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

b) la dissolution, lorsque la personne morale a été créée ou lorsqu'il s'agit d'un crime ou d'un délit puni en ce qui concerne les personnes physiques d'une peine d'emprisonnement supérieure à cinq (5) ans, détournée de son objet pour commettre les faits incriminés;

c) 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;
d) 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;
e) l'exclusion des marchés publics à titre définitif ou pour une durée de cinq (5) ans au plus;
f) l'interdiction à titre définitif au pour une durée de cinq (5) ans au plus de faire appel public à l'épargne;
g) 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;
h) la confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit;
i) l'affichage de la décision prononcée ou la diffusion de celle-ci soit par la presse écrite sait par tout moyen de communication au public par voie électronique aux frais de la personne morale incriminée,

Chapitre V : Des techniques spéciales de renseignement

Article 93: L'ANSE est chargée de la mise en œuvre des moyens spécifiques destinés à entraver les menaces contre la sécurité et les intérêts fondamentaux de la Nation ou à prévenir ou déjouer des activités d'ingérence dirigés contre les intérêts nationaux dans le cyberespooe.

Article 94: En matière de cyberterrorisme, défense des infrastructures vitales du pays ou de trafics internationaux, l'ANSE peut procéder à des enquêtes judiciaires, ouvertes au moment le plus opportun, lorsqu'il résulte des renseignements et indices dont ils disposent une présomption de crime ou de délit.

Article 95 : Les enquêtes visées à l'article 93 sont diligentées par des officiers et agents de police judiciaire regroupés au sein d'un service spécialisé de l'ANSE. Elles sont conduites conformément aux règles prévues par le Code de procédure pénale, sous réserve des dispositions spéciales prévues par la présente loi et éventuellement par d'autres textes législatifs.

Article 96: Le service spécialisé de l'ANSE peut être saisi par le procureur de la République, les services nationaux ou étrangers de recherche de renseignement ou par toute administration ou personne physique ou morale mettant à leur disposition des informations crédibles relatives à la préparation ou à la commission d'une infraction portant sur l'une des matières visées à l'article 93.

Article 97: L'ANSE peut, avec l'autorisation et sous le contrôle du procureur de la République compétent, recourir aux moyens d'investigation prévus à l'article 97.

Les preuves régulièrement recueillies par ces moyens sont recevables en justice et sont laissées à l'appréciation des juridictions pénales compétentes.

Article 98: Les services spéciaux de renseignement peuvent, lorsqu'ils disposent d'indices relatifs à l'une des menaces prévues à l'article 92 et en l'absence de tout autre moyen, recourir à des procédés techniques, intrusifs, de surveillance ou de localisation pour recueillir les renseignements utiles à la neutralisation de la menace.

Article 99: Les activités de renseignement régulièrement menées par l'ANSE ne doivent faire l'objet d'aucune entrave volontaire sur l'étendue du territoire national.

Requis en cas de besoin, les agents de la force publique, les autres services de l'Etat notamment l'ANSICE ainsi que les organismes privés compétents fournissent sans délai aux services de renseignement le concours nécessaire et observent le secret sur les opérations et investigations en cours.

CHAPITRE V : DES DISPOSITIONS PARTICULIERES

Article 100 : Constitue une circonstance aggravante au sens de la présente loi l'utilisation des technologies de l'information et de la communication (TIC) en vue de commettre des infractions de droit commun, comme le vol, l'escroquerie, le recel, l'abus de confiance, l'extorsion de fonds, le terrorisme, le blanchiment de capitaux ou la commission d'infractions en bande organisée.

Article 101 : Commet une infraction au sens de la présente loi toute personne qui porte atteinte aux biens d'autrui par l'utilisation des TIC, notamment aux données informatiques, par vol, escroquerie, recel, abus de confiance, extorsion de fonds, terrorisme, blanchiment d'argent chantage.

Article 102 : Ne constitue pas une infraction au sens de la présente loi, l'utilisation des nouveaux supports immatériels à savoir les « données numérisées » ou les « fichiers informatisés» qui sont tenus secrets par les États dans l'intérêt de la sécurité et/ou de la défense nationale.

CHAPITRE VI : DE LA COOPERATION ET DE L'ENTRAIDE JUDICIAIRES INTERNATIONALES

SECTION 1: DE LA COOPERATION JUDICIAIRE INTERNATIONALE

Article 103 Les autorités judiciaires nationales peuvent donner commission rogatoire tant nationale qu'internationale, à toute personne morale ou physique pour rechercher les éléments constitutifs des infractions de cybercriminalité, dont au moins l'un des éléments constitutifs a été commis sur le territoire tchadien ou dont l'un des auteurs ou complices se trouve sur ledit territoire. Sous réserve des règles de réciprocité entre le Tchad et les pays étrangers liés par un accord de coopération judiciaire, les commissions rogatoires sont exécutées conformément aux dispositions du Code de Procédure Pénale.

Article 104 : A la demande d'un autre État membre de la CEMAC ou de la CEEAC, les autorités nationales compétentes pourront instruire les instances en charge de lutte contre la cybercriminalité afin de coopérer à la recherche et à la constatation de toutes les infractions pénales relatives aux systèmes informatiques, ainsi

qu'à la collecte de preuves sous forme électronique se rapportant à une infraction pénale.
Cette coopération est mise en œuvre dans le respect des instruments internationaux pertinents sur la coopération internationale en matière pénale.

SECTION II : DE L'ENTRAIDE JUDICIAIRE INTERNATIONALE

Article 105 : A moins qu'une convention internationale à laquelle le Tchad est partie n'en dispose autrement, les demandes d'entraide émanant des autorités judiciaires tchadiennes et destinées aux autorités judiciaires étrangères sont transmises par l'intermédiaire du Ministère en charge des Affaires Étrangères.
Les pièces d'exécution sont renvoyées aux autorités de l'État requérant par la même voie.
Les demandes d'entraide judiciaire émanant des autorités judiciaires étrangères et destinées aux autorités judiciaires tchadiennes doivent être présentées par la voie diplomatique par le Gouvernement étranger intéressé.
Les pièces d'exécution sont renvoyées aux autorités de l'État requérant par la même voie.
En cas d'urgence, les demandes d'entraide judiciaires émises par les autorités tchadiennes ou étrangères peuvent être transmises directement aux autorités de l'État requis pour leur exécution. Le renvoi des pièces d'exécution aux autorités compétentes de l'État requérant est effectué selon les mêmes modalités.
Sous réserve des conventions internationales, les demandes d'entraide émanant des autorités judiciaires étrangères et destinées aux autorités judiciaires tchadiennes doivent faire l'objet d'un avis de la part du gouvernement étranger intéressé. Cet avis est transmis aux autorités judiciaires tchadiennes compétentes par voie diplomatique.
En cas d'urgence, les demandes d'entraide émanant des autorités judiciaires étrangères sont transmises au Procureur de la République ou au Juge d'instruction territorialement compétent.
Si le Procureur de la République reçoit directement d'une autorité étrangère, une demande d'entraide qui ne peut être exécutée que par le Juge d'instruction, il la transmet pour exécution à ce dernier ou saisit le Procureur Général dans le cas prévu à l'article 107ci-dessus.
Avant de procéder à l'exécution d'une demande d'entraide judiciaire dont il a été directement saisi, le Juge d'instruction la communique immédiatement pour avis au Procureur de la République.

Article 106 : les demandes d'entraide émanant des autorités judiciaires étrangères sont exécutées par le Procureur de la République ou par les officiers ou agents de Police Judiciaire requis à cette fin par ce magistrat. Elles sont exécutées par le Juge d'instruction ou par des officiers de Police Judiciaire agissant sur commission rogatoire de ce magistrat lorsqu'elles nécessitent certains actes de procédure qui ne peuvent être ordonnés ou exécutés qu'au cours d'une instruction préparatoire.

Article 107 : Les demandes d'entraide émanant des autorités judiciaires étrangères sont exécutées selon les règles de procédure prévues par le Code de Procédure Pénale.
Toutefois, si la demande d'entraide le précise, elle est exécutée selon les règles de procédure expressément indiquées par les autorités compétentes de l'État requérant, sans que ces règles ne réduisent les droits des parties ou les garanties procédurales prévues par le Code de Procédure Pénale.
Lorsque la demande d'entraide ne peut être exécutée conformément aux exigences de l'État requérant, les autorités compétentes tchadiennes en informent sans délai les autorités de l'État requérant et indiquent dans quelles conditions la demande pourrait être exécutée.
Les autorités tchadiennes compétentes et celles de l'État requérant peuvent ultérieurement s'accorder sur la suite à réserver à la demande, le cas échéant, en la subordonnant au respect desdites conditions.
L'irrégularité de la transmission de la demande d'entraide ne peut constituer une cause de nullité des actes accomplis en exécution de cette demande.

Article 108 : Si l'exécution d'une demande d'entraide émanant d'une autorité judiciaire étrangère est de nature à porter atteinte à l'ordre public ou aux intérêts essentiels de la Nation, le Procureur de la République saisi ou avisé de cette demande, la transmet au Procureur Général qui en saisit le Ministre chargé de la Justice et donne, le cas échéant, avis de cette transmission au Procureur de la République.
S'il est saisi, le Ministre chargé de la Justice informe l'autorité requérante, le cas échéant, de ce qu'il ne peut être donné suite, totalement ou partiellement à sa demande. Cette information est notifiée à l'autorité judiciaire concernée et fait obstacle à l'exécution de la demande d'entraide ou au retour des pièces d'exécution.

CHAPITRE VII : DES DISPOSITIONS FINALES

Article 109 : En tant que de besoin, les conditions d'application de la présente loi seront précisées par voie réglementaire.

Article 110 : Sont abrogées toutes les dispositions antérieures contraires.

Article 111 ; La présente ordonnance sera enregistrée et publiée au Journal Officiel de la République et exécutée comme loi de l'État.

N'Djamena, le 31 Août 2022
Le Général
MAHAMAT IDRISS DEBY ITNO
****

ORDONNANCE N°008/PCMT/2022 Portant sur la Cybersécurité en République du Tchad

LE PRESIDENT DU CONSEIL MILITAIRE DE TRANSITION,
PRESIDENT DE LA REPUBLIQUE,
CHEF DE L'ETAT,
PRESIDENT DU CONSEIL DESMINISTRES

Vu la Charte de Transition;
Vu la Loi N°18/PCMT/2022 du 04 juillet 2022 portant Habilitation du Gouvernement à légiférer par voie d'Ordonnance pendant la période allant du 1er juillet au 31 aout 2022
Le Conseil des Ministres consulté à domicile en date du 31 Août 2022
ORDONNE:

TITRE I: DES DISPOSITIONS GENERALES

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

Article 1er : Objet de la Loi
La présente loi fixe les règles et les dispositions de sécurité applicables aux systèmes d'information des administrations de l'État, des collectivités territoriales,

des établissements et entreprises publics et toute autre personne morale de droit public, les organisations du secteur privé, désignés dans la présente loi par « entité» ;

Article 2 : Champ d'application.

Sont soumis à la présente loi:

- La politique et stratégie de sécurité des informations numériques du pays
- Toute activité d'audit des systèmes d'information de l'État et des organismes privés.
- Les activités de formation et de sensibilisation des membres des administrations de l'État, des collectivités territoriales, des établissements et entreprises publics et toute autre personne morale de droit public ou privé, souhaitant bénéficier de l'expertise de l'ANSICE

Article 3 : Sont exclues du champ d'application de la présente Loi:

- les applications spécifiques en matière de défense et de sécurité nationales ;
- les moyens de cryptologie utilisés par les missions diplomatiques et consulaires visées par la Convention de Vienne sur les relations diplomatiques ;
- la protection numérique des infrastructures vitales du pays

CHAPITRE II : DES DEFINITIONS

Article 4 : Au sens de la présente loi, les termes et expressions suivants, s'entendent:

ANSICE: Agence Nationale de Sécurité Informatique et de Certification Électronique. Autorité nationale administrative indépendante chargée de veiller au respect, sur le territoire national, des dispositions de la présente loi.

Chiffrement: procédé grâce auquel on transforme à l'aide d'une convention secrète appelée clé, des informations claires en informations inintelligibles par des tiers n'ayant pas la connaissance de la clé.

Clé : dans un système de chiffrement, elle correspond à une valeur mathématique, un mot, une phrase, qui permet, grâce à l'algorithme de chiffrement, de chiffrer ou de déchiffrer un message.

Communication électronique : toute transmission au public ou à une catégorie du public, par un procédé de communication électronique ou magnétique, de signes, de signaux, d'écrits, d'images, de sons ou de message de toute nature.

Confidentialité : état de sécurité permettant de garantir le secret des informations et ressources stockées dans les réseaux et systèmes de communication électroniques, systèmes d'information ou des équipements terminaux, afin de prévenir la divulgation non autorisée d'informations à des tiers, par la lecture, l'écoute, la copie illicite d'origine intentionnelle ou accidentelle durant leur stockage, traitement au transfert.

Cryptographie : ensemble des techniques qui, au moyen d'un cade secret appelé clé, visent à rendre un message indéchiffrable pour toute autre personne que son émetteur ou son destinataire.

Cryptologie : 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 activités criminelles pénalement répréhensibles qui se commettent au moyen ou sur un réseau de communications électroniques ou sur un système d'information par d'autres moyens que ceux habituellement mis en œuvre et de manière complémentaire à le criminalité classique.

Cyberespace : ensemble de données numérisées constituant un univers d'information et un milieu de communication, lié à l'interconnexion mondiale des ordinateurs.

Cybersécurité : désigne un ensemble des mesures de prévention, de protection et de dissuasion d'ordre technique, organisationnel, juridique, financier, humain, procédural et autres actions permettant d'atteindre les objectifs de sécurisation des réseaux de communications électroniques, des systèmes d'information et pour la protection de la vie privée des personnes.

Déchiffrement : Opération faisant écho au chiffrement, ayant pour but l'obtention de la version originale d'un message précédemment chiffré.

Disponibilité: désigne l'état de sécurité permettant de garantir que les informations et ressources des réseaux de communications électroniques, des systèmes d'information ou des équipements terminaux soient accessibles et utilisables selon les besoins.

Données: représentation de faits, d'informations ou de notions sous une forme susceptible d'être traitée par un équipement terminal, y compris un programme permettant à ce dernier d'exécuter une fonction.

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 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 de service sous-jacent.

Fournisseur de services : toute personne physique ou morale fournissant pour son propre compte ou pour le compte d'autrui des services de communications électroniques ou de services d'information électroniques, y compris la fourniture de l'accès à l'utilisation de ces services.

Intégrité: désigne l'état de sécurité assurant qu'un réseau de communications électroniques, système d'information ou équipement terminal demeuré intact et que les ressources et informations qui y stockées n'ont pas été altérées, modifiées ou détruites, d'une façon intentionnelle ou accidentelle, de manière à assurer leur exactitude, leur fiabilité et leur pérennité.

Mineur: toute personne âgée de moins de dix-huit (18) ans au sens de la loi nationale.

Prestataire de service de sécurité: toute personne physique ou morale qui exerce des activités liées à la sécurité électronique notamment la délivrance et la gestion des certificats électroniques ou la fourniture d'autres services liés aux signatures électroniques, la création des logiciels de sécurité, la surveillance des réseaux, la détection d'intrusions, l'audit des réseaux et systèmes de sécurité.

Preuve numérique : toute information probante stockée ou transmise sous forme numérique.

Pornographie enfantine: toute donnée quels qu'en soient la nature, la forme ou le support 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.

Réseau de communications électroniques : systèmes de transmission, actif ou passif et, le cas échéant, les équipements de commutation et de routage et les autres ressources qui permettent l'acheminement des signaux par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques comprenant les réseaux satellitaires, les réseaux terrestres fixes (avec commutation de circuits ou de paquets, y compris l'internet) et mobile, les systèmes utilisant le réseau électrique, pour autant qu'ils servent à la transmission des signaux, les réseaux utilisés pour la radiodiffusion sonore et télévisuelle et les réseaux câblés de télévision, quel que soit le type d'information transmise.

Sécurité : situation dans la quelle quelqu'un ou quelque chose n'est exposé à aucun danger. Mécanisme destiné à prévenir un événement dommageable ou à en limiter les effets. Service de communications électroniques prestation consistante entièrement ou principalement en la fourniture de communications électroniques à l'exclusion des contenus des services de communication audiovisuelle.

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

Système d'information: désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, assurant par lui-même ou par un ou plusieurs de ses éléments, conformément à un programme, un traitement automatisé de données.

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

Article 5 : Pour les termes et expressions qui ne sont pas définis dans la présente loi, il convient en tant que de besoin, de se référer aux définitions données par les conventions, décisions et documents de l'Union Internationale des Télécommunications (UIT) ou à ceux de l'Union Africaine (UA), de la Communauté Économique des États de l'Afrique Centrale (CEEAC), ou à ceux de la Communauté Économique et Monétaire de l'Afrique Centrale (CEMAC).

TITRE II : DU DISPOSITIF DE SECURITE DES SYSTEMES D'INFORMATION

CHAPITRE I: DE LA PROTECTION DES SYSTEMES INFORMATIQUES

Section première : De la mission de l'État

Article 6: En collaboration avec les parties prenantes comprenant, l'industrie et les organisations professionnelles, la société civile et les citoyens, l'État, à travers le Ministère en charge des communications électroniques, élabore et met en œuvre une politique nationale de sécurité des systèmes d'information en tenant compte de l'évolution technologique et des priorités du gouvernement dans ce domaine.

A ce titre, l'Etat, à travers l'ANSICE:

a) assure la promotion de la sécurité des réseaux de communications électroniques et des systèmes d'information ainsi que le suivi de l'évolution des questions liées aux activités de sécurité informatique;
b) coordonne sur le plan national les activités concourant à la sécurisation et à la protection des réseaux de communications électroniques et des systèmes d'information;
c) veille à la mise en place d'un cadre légal et règlementaire adéquat pour la sécurité des communications électroniques;
d) assure la représentation de l'État aux instances internationales chargées des activités liées à la sécurisation et à la protection des réseaux de communications électroniques et des systèmes d'information.

Article 7: La politique nationale de cybersécurité devra intégrer dans ses grandes lignes, la protection de l'information dans les réseaux, la sécurité des transactions électroniques, la protection de la vie privée et des mineurs dans le cyberespace, ainsi que la lutte contre la fracture numérique.

Section II : Dispositions propres aux entités

Article 8: Chaque entité doit veiller à ce que ses systèmes d'information soient conformes aux directives, règles, règlements, référentiels ou recommandations, édictés par l'ANSICE.

Article 9: Chaque entité doit élaborer et mettre en œuvre une politique de sécurité de ses systèmes d'information qui soit conforme aux directives de l'ANSICE.

Chaque entité est tenue d'identifier les risques qui menacent la sécurité de ses systèmes d'information et de prendre des mesures techniques et organisationnelles nécessaires pour gérer ces risques, éviter les incidents de nature à porter atteinte aux systèmes d'information ainsi que pour en réduire au minimum l'impact.

Tout système d'information d'une entité offrant des services numériques à des tiers doit, avant sa mise en exploitation, faire l'objet d'un audit de sa sécurité par l'ANSICE.

Chaque entité doit, régulièrement, auditer ses systèmes d'information.

Article 10: Chaque entité doit classifier ses actifs informationnels et systèmes d'information selon leur niveau de sensibilité en termes de confidentialité, d'intégrité et de disponibilité. Les mesures de protection des actifs Informationnels et systèmes d'information doivent être proportionnés au niveau de classification attribué.

Chaque entité doit arrêter des procédures d'habilitation des personnes pouvant accéder aux informations classifiées et des conditions d'échange, de conservation ou de transport de ces informations.

Le référentiel de classification des actifs informationnels et des systèmes d'information est fixé par l'ANSICE.

Article 11: Chaque entité doit désigner un responsable de la sécurité des systèmes d'information qui veille à l'application de la politique de sécurité des systèmes d'information.

Le responsable de la sécurité des systèmes d'information est l'interlocuteur de l'ANSICE et doit jouir de l'indépendance requise dans l'exercice de sa mission.

Article 12: Chaque entité met en place des moyens appropriés de supervision et de détection des évènements susceptibles d'affecter la sécurité de ses systèmes d'information et d'avoir un impact significatif sur la continuité des services qu'elle assure.

Les données techniques générées par les moyens précités ne peuvent être exploitées par l'ANSICE qu'aux seules fins de caractériser et traiter la menace affectant la sécurité des systèmes d'information de l'entité concernée.

Article 13: Chaque entité doit, dès qu'elle prend connaissance d'un incident affectant la sécurité ou le fonctionnement de ses systèmes d'information, le déclarer à l'ANSICE.

A la demande de l'ANSICE, chaque entité lui communique, sans délai, les informations complémentaires relatives aux incidents affectant la sécurité ou le fonctionnement de ses systèmes d'information.

L'ANSICE précise les données techniques et les informations relatives aux incidents qui doivent être communiquées ainsi que les modalités de leur transmission. Elle adresse à l'entité concernée une synthèse des mesures et recommandations relatives au traitement de l'incident.

Article 14: Chaque entité prépare un plan de continuité ou de reprise d'activités intégrant l'ensemble des solutions de secours pour neutraliser les interruptions des activités, protéger les processus métier cruciaux des effets causés par les principales défaillances des systèmes d'information ou par des sinistres et garantir une reprise de ces processus dans les meilleurs délais.

Le plan de continuité ou de reprise d'activités doit être testé régulièrement afin de le mettre à jour en fonction des évolutions propres de l'entité et de l'évolution des menaces.

Article 15 : L'ANSICE fixe les règles et le référentiel technique régissant la sécurité relative à l'externalisation des systèmes d'information.

Section III : De l'obligation d'audit

Article 16 : Les réseaux de communications électroniques et les systèmes d'information des opérateurs, des Autorités de certification et des fournisseurs de services de communications électroniques sont soumis à l'audit de sécurité obligatoire et périodique par l'Agence Nationale de Sécurité Informatique et de Certification Électronique (ANSICE) ou par un prestataire d'audit qualifié par L'ANSICE.

L'audit de sécurité et les mesures d'impact de gravité sont effectués chaque année ou lorsque les circonstances l'exigent.

Les rapports d'audit sont confidentiels et adressés au Directeur Général de l'ANSICE.

Les conditions d'évaluation des menaces, des vulnérabilités des systèmes d'information et l'impact de potentielles attaques sur ces systèmes d'information, ainsi que les conditions et les modalités de l'audit de sécurité seront fixées par voie règlementaire par l'ANSICE.

Article 17 : Le personnel de l'ANSICE et les experts commis en vue d'accomplir des opérations d'audit sont astreints au secret professionnel.

Section IV : De la cryptologie

Article 18: L'utilisation des moyens et prestations de cryptologie est libre.

Toutefois, lorsque les moyens ou des prestations de cryptologie permettent d'assurer des fonctions de confidentialité, le principe de libre utilisation ne s'applique que conformément à la présente loi.

La fourniture, l'importation et l'exportation des moyens de cryptologie assurant exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont également libres.

Article 19: Nonobstant les dispositions de la présente loi, les modalités d'utilisation de la taille de certaines clés sont fixées par décret.

Article 20: La fourniture ou l'importation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité est soumise à une déclaration préalable auprès de l'ANSICE.

Le prestataire ou la personne procédant à la fourniture ou à l'importation d'un service de cryptologie tient à la disposition de l'ANSICE une description des caractéristiques techniques de ce moyen de cryptologie. Les prestataires de services de cryptologie sont assujettis au secret professionnel.

Un décret définit les conditions dans lesquelles est effectuée la déclaration visée à l'alinéa premier du présent article.

Article 21: Sauf dispositions contraires, l'exportation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité est soumise à autorisation de l'ANSICE.

Article 22: Les conditions de délivrance de l'agrément aux organismes exerçant des prestations de cryptologie ainsi que leurs obligations sont définies par décret.

Article 23 : Les organismes exerçant des prestations de cryptologie doivent être agréés par l'ANSICE.

Article 24: Les conditions de délivrance de l'agrément aux organismes exerçant des prestations de

cryptologie ainsi que leurs obligations sont définies par décret.

CHAPITRE II : DES DROITS, OBLIGATIONS ET MESURES DE SECURITE ELECTRONIQUE

Section I : Des droits et obligations relatives à la vie privée

Article 25 : Les opérateurs et exploitants des réseaux de communications électroniques et des systèmes d'information sont tenus d'assurer la confidentialité des communications acheminées à travers les réseaux de communications électroniques et les systèmes d'information, y compris les données relatives au trafic.

Article 26: Le fournisseur de contenus est responsable des contenus véhiculés par son système d'information, notamment lorsque ces contenus portent atteinte à la dignité humaine, à l'honneur et à la vie privée.

Article 27 : Il est interdit à toute personne physique ou morale d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférent, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés, sauf lorsque cette personne y est légalement autorisée.

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

Article 28 : L'enregistrement des communications et des données de trafic y afférentes, effectué dans le cadre professionnel en vue de fournir la preuve numérique d'une communication électronique est autorisé.

Article 29: les fournisseurs de contenus des réseaux de communications électroniques et systèmes d'information, sont tenus de conserver les contenus ainsi que les données stockées dans leurs installations pendant une durée de dix (10) ans maximum.

Les fournisseurs de contenus des réseaux de communications électroniques et systèmes d'information, ont l'obligation de mettre en place des dispositifs nécessaires pour faire face aux atteintes préjudiciables aux données personnelles et à la vie privée des utilisateurs.

Article 30: l'utilisation des réseaux de communications électroniques et des systèmes d'information aux fins de stocker les informations ou d'accéder à des informations stockées dans un équipement terminal d'une personne physique ou morale, ne peut se faire qu'avec son consentement préalable ou à la demande des autorités judiciaires.

Article 31 : L'émission des messages électroniques à des fins de prospection en dissimulant l'identité de l'émetteur au nom duquel la communication est faite, ou sans indiquer une adresse valide à laquelle le destinataire peut transmettre une demande visant à obtenir l'arrêt de ces informations est interdite.

Article 32: L'émission des messages électroniques en usurpant l'identité d'autrui est interdite.

Article 33 : les personnes dont l'activité est d'offrir un accès à des services de communications électroniques, sont tenus d'informer leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposer au moins un de ces moyens.

Article 34: La responsabilité des personnes qui assurent, même à titre gratuit le stockage des signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis aux destinataires de ces services, peut être engagée. Toutefois, la responsabilité prévue à l'alinéa 1 ci-dessus n'est point engagée dans les cas suivants:

a) si les personnes n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaitre ce caractère;
b) si, dès le moment où elles ont eu connaissance des faits, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible.

Article 35 : Les personnes mentionnées aux articles 33 et 34 ci-dessus, sont tenues de conserver, pendant une durée de dix (10) ans, les données permettant l'identification de toute personne ayant contribué à la création du contenu des services dont elles sont prestataires.

L'autorité judiciaire peut requérir communication des données prévues à l'alinéa 1 ci-dessus auprès des prestataires mentionnés aux articles 33 et 34.

Article 36: la juridiction compétente saisie doit statuer dans un délai maximum de trois (3) mois sur toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication électronique.

Article 37: Toute personne victime d'une diffamation au moyen d'un service de communications électroniques, dispose d'un droit de réponse et peut en exiger la rectification suivant les conditions prévues par les textes en vigueur.

En cas de refus ou de non publication de son droit de réponse, la personne victime d'une diffamation peut user des voies de droit prévues par les textes en vigueur pour obtenir réparation du préjudice subi.

Article 38: Toute personne assurant une activité de transmission de contenus sur un réseau de communications électroniques ou de fourniture d'accès à un réseau de communications électroniques ne peut voir sa responsabilité engagée que lorsqu'elle:

a) est à l'origine de la demande de transmission litigieuse;
b) sélectionne ou modifie les contenus faisant l'objet de la transmission.

Article 39 : Toute personne assurant dans le seul but de rendre plus efficace leur transmission ultérieure, une activité de stockage automatique, intermédiaire et temporaire des contenus qu'un prestataire transmet ne peut voir sa responsabilité civile ou pénale engagée en raison de ces contenus que dans le cas où elle:

a) a modifié ces contenus;
b) ne s'est pas conformée à leurs conditions d'accès et aux règles usuelles concernant leur mise à jour; ou
c) a entravé l'utilisation licite et usuelle de la technologie utilisée pour obtenir les données.

Section II : De l'obligation de protection des réseaux de communications électroniques

Article 40: Les opérateurs des réseaux de communications électroniques et les fournisseurs de services de communications électroniques sont tenus de prendre toutes les mesures techniques et administratives nécessaires pour garantir la sécurité des services offerts.
A cet effet, ils sont tenus d'informer les usagers:

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

Article 41: Les opérateurs de réseaux et les fournisseurs de services de communications électroniques ont l'obligation de conserver les données de connexion et de trafic pendant une période de dix (10) ans.
Les opérateurs de réseaux et les fournisseurs de services de communications électroniques sont tenus d'installer des mécanismes de surveillance de trafic des données de leurs réseaux. Ces données peuvent être accessibles lors des investigations judiciaires.
La responsabilité des opérateurs de réseaux et celles des fournisseurs de services de communications électroniques est engagée si l'utilisation des données prévue à l'alinéa 2 ci-dessus porte atteinte aux libertés individuelles des usagers.

Section III : De l'obligation de protection des systèmes d'information

Article 42 : Les exploitants des systèmes d'information sont tenus de prendre toutes les mesures techniques et administratives afin de garantir la sécurité des services offerts. A cet effet, ils doivent se doter de systèmes normalisés leur permettant d'identifier, d'évaluer, de traiter et de gérer de manière continue les risques liés à la sécurité des systèmes d'information dans le cadre des services offerts directement ou indirectement.
Les exploitants des systèmes d'information doivent mettre en place des mécanismes techniques pour faire face aux atteintes préjudiciables à la disponibilité permanente des systèmes, à leur intégrité, à leur authentification, à leur non répudiation par des utilisateurs tiers, à la confidentialité des données et à la sécurité physique.
Les mécanismes prévus à l'alinéa 2 ci-dessus, doivent faire l'objet d'approbation par l'ANSICE.
Les plates-formes des systèmes d'information doivent faire l'objet de protection contre d'éventuels rayonnements et des intrusions qui pourraient compromettre l'intégrité des données transmises et contre toute autre attaque externe notamment par un système de détection d'intrusions.
Article 43 : les personnes morales dont l'activité est d'offrir un accès à des systèmes d'information sont tenues d'informer les usagers:

a) du danger encouru dans l'utilisation des systèmes d'information non sécurisés notamment pour les particuliers;
b) de la nécessité d'installer des dispositifs de contrôle parental;
c) des risques particuliers de violation de sécurité, notamment la famille générique des virus;
d) de l'existence de moyens techniques permettant de restreindre l'accès à certains services et de leur proposer au moins l'un de ces moyens, notamment l'utilisation des systèmes d'exploitation les plus récents, les outils antivirus et contre les logiciels espions et trompeurs, l'activation des pare-feu personnels, de systèmes de détection d'intrusions et l'activation des mises à jour automatiques.

Article 44 : Les exploitants des systèmes d'information sont tenus d'informer les utilisateurs de l'interdiction faite d'utiliser le réseau de communications électroniques pour diffuser des contenus illicites ou tout autre acte qui peut entamer la sécurité des réseaux ou des systèmes d'information, ou attenter à la vie privée des individus.
L'interdiction porte également sur la conception de logiciel trompeur, de logiciel espion, de logiciel potentiellement indésirable ou de tout autre outil conduisant à un comportement frauduleux.
Article 45 : Les exploitants des systèmes d'information ont l'obligation de conserver les données de connexion et de trafic de leurs systèmes d'information pendant une période de dix (10) ans.
Les exploitants des systèmes d'information sont tenus d'installer des mécanismes de surveillance et de contrôle d'accès aux données de leurs systèmes d'information, les données conservées doivent être accessibles lors des investigations judiciaires.
Les installations des exploitants des systèmes d'information peuvent faire l'objet de perquisition ou de saisie sur ordre d'une autorité judiciaire dans les conditions prévues par les lois et règlements en vigueur.
Article 46 : les exploitants des systèmes d'information doivent évaluer et réviser périodiquement leurs systèmes de sécurité et introduire en cas de nécessité les modifications appropriées dans leurs pratiques, mesures et techniques de sécurité en fonction de l'évolution des technologies.
Les exploitants des systèmes d'information et leurs utilisateurs peuvent coopérer entre eux pour l'élaboration et la mise en œuvre des pratiques, mesures et techniques de sécurité de leurs systèmes.
Article 47 : Les fournisseurs de contenus des réseaux de communications électroniques et systèmes d'information sont tenus d'assurer la disponibilité des contenus, ainsi que celle des données stockées dans leurs installations.
Ils ont l'obligation de mettre en place des filtres pour faire face aux atteintes préjudiciables aux données personnelles et à la vie privée des utilisateurs.

CHAPITRE II : DE LA REGULATION ET DU SUIVI DES ACTIVITES DE SECURITE DES SYSTEMES INFORMATIQUES ET DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Article 48: La régulation des activités de sécurité des systèmes d'information, la sécurité des transactions électronique, la protection des données à caractère personnel, la protection de la vie privée dans le cyberespace, la protection des mineurs en ligne, les audits de sécurité, les agréments des prestataires de service d'audit de sécurité et de cryptologie, l'homologation des équipements de cryptographie sur l'ensemble du territoire national et la mise en œuvre des dispositions de la présente loi, de la loi portant protection des données à caractère personnel et de celle portant sur les transactions électroniques de la République du Tchad sont assurées par l'Agence Nationale de Sécurité informatique et de Certification Électronique (ANSICE).

CHAPITRE III : DE LA FORMATION, DE LA SENSIBILIBATION ET DE LA COOPERATION

Article 49 : L'ANSICE organise, en collaboration avec les acteurs et professionnels de la sécurité des systèmes d'information, des cycles de formation et des exercices au profit du personnel et renforcer les capacités nationales en la matière.

Article 50: l'ANSICE définit et met en œuvre des programmes de sensibilisation sur la cyberéthique et sur les enjeux liés aux menaces et risques de cybersécurité au profit du personnel de l'Etat et du secteur privé et des particuliers.

Des conseils et recommandations d'hygiène en sécurité informatique au profit du personnel des de l'Etat et du secteur privé et des particuliers sont régulièrement publiés sur le site web de l'ANSICE.

Article 51: l'ANSICE contribue aux programmes initiés par les organes compétents de l'Etat pour le renforcement de la confiance numérique, le développement de la digitalisation des services et la protection des données à caractère personnel.

Article 52: l'ANSICE développe et coordonne, en concertation avec les administrations concernées, les relations de coopération avec les organismes nationaux et étrangers dans le domaine de la sécurité des systèmes d'information.

CHAPITRE IV DES DISPOSITIONS TRANSITOIRES ET FINALES

Article 53: En tant que de besoin, les conditions d'application de la présente loi seront précisées par voie réglementaire.

Article 54: la présente Ordonnance abroge toutes dispositions antérieures contraires, sera enregistrée et publiée au Journal Officiel de la République et exécutée comme loi de l'Etat.

N'Djamena, le 31 Août 2022
Le Général
MAHAMAT IDRISS DEBY ITNO

****

ORDONNANCE N°0011/PCMT/2022 Portant modification de l'article 17 de l'Ordonnance N°016/PR/2018 du 31 mai 2018 portant attributions, organisation et fonctionnement de la Haute Autorité des Media et de l'Audiovisuel

LE PRESIDENT DU CONSEIL MILITAIRE DE TRANSITION,
PRESIDENT DE LA REPUBLIQUE,
CHEF DEL'ETAT,
PRESIDENT DU CONSEIL DES MINISTRES,

(/u la Charte de Transition;

(/u la Loi N°018/PCMT/2022 du 04 juillet 2022 portant habilitation du Gouvernement à légiférer par vole d'ordonnances pendant la période allant du 1er Juillet au 31 août 2022;

Le Conseil des Ministres consulté à domicile le 25 août 2022 ;

ORDONNE:

Article 1er : Les dispositions de l'article 17 de l'Ordonnance N°016/PR/2018 du 31 mai 2018 suscité, sont modifiées comme suit:

Au lieu de:

Article 17 (ancien): Tout membre de la HAMA doit, avant d'entrer en fonction, prêter serment **selon la formule confessionnelle consacrée par la loi**. Le serment est reçu par la Cour Suprême lors d'une cérémonie solennelle en présence du Président de la République et du Président de l'Assemblée Nationale.

Lire:

Article 17 (nouveau): Tout membre de la HAMA doit, avant d'entrer en fonction, prêter serment dans les termes suivants: « ***je jure solennellement et fidèlement de remplir ma mission dans une totale impartialité, de garder le secret des délibérations et de me conduire en tout comme un digne et loyal serviteur de l'intérêt national*** »,

Il ne peut en aucun cas, être relevé de ce serment.

Le serment est reçu lors d'une cérémonie solennelle par la Cour Suprême. Les agents des Commissions, des services et les chargés de mission de la HAMA prêtent le même serment devant la Cour d'Appel.

(Le reste sans changement)

Article 2 : La présente Ordonnance qui abroge toutes dispositions antérieures contraires, sera enregistrée et publiée au Journal Officiel de la République et exécutée comme Loi de l'Etat.

N'Djamena, le 31 Août 2022
Le Général
MAHAMAT IDRISS DEBY ITNO