UNION DES COMORES

Unité - Solidarité - Développement

Président de l'Union

Moroni, le 18 JAN 2022

DECRET N° 22- 003 /PR

Portant promulgation de la loi N°21-012/AU du 25 juin 2021 relative à la Cyber Sécurité et à la Lutte contre la Cybercriminalité en Union des Comores.

LE PRESIDENT DE L'UNION,

VU la Constitution de l'Union des Comores du 23 décembre 2001, révisée par le référendum du 30 juillet 2018, notamment en son article 64 ;

D E C R E T E :

ARTICLE 1er : Est promulguée la loi N°21-012/AU relative à la Cyber Sécurité et à la Lutte contre la Cybercriminalité en Union des Comores, adoptée le 25 juin 2021, par l'Assemblée de l'Union des Comores et dont la teneur suit :

« TITRE PRELIMINAIRE : DISPOSITIONS GENERALES

CHAPITRE I : OBJET ET CHAMP D'APPLICATION

Article 1er : La présente loi régit, en Union des Comores, le cadre de sécurité des réseaux de communications électroniques et des systèmes d'information ainsi que la lutte contre la cybercriminalité par la définition et la répression des infractions liées à l'utilisation des technologies de l'information et de la communication.

Elle vise, dans sa partie cybercriminalité, à renforcer et à compléter les dispositions du Code pénal en vigueur en Union des Comores.

Article 2 :

Elle a pour objet essentiel de :

- Instaurer la confiance dans les réseaux de communications électroniques et les systèmes d'information ;
- Fixer le régime juridique de la preuve numérique, des activités de sécurité, de cryptographie et de certification électronique ;
- Protéger les droits fondamentaux des personnes physiques, notamment le droit à la dignité humaine, à l'honneur et au respect de la vie privée, ainsi que les intérêts légitimes des personnes morales.
- Protéger les droits et les intérêts de la personne morale telle que définie dans la présente loi.

UNION DES COMORES ★ LE PRESIDENT

Article 3 : Sont exclues du champ de la présente loi, les échanges, les services et les applications spécifiques utilisées en matière de défense et de sécurité nationale.

Article 4 : Lorsque l'infraction peut être localisée sur le territoire national, même partiellement, la loi et les juridictions comoriennes sont compétentes.

Ces dernières sont également compétentes lorsque l'infraction est réputée être commise sur le territoire national.

Lorsque la victime ou l'auteur de l'infraction est de nationalité comorienne, la loi comorienne peut s'appliquer et les juridictions comoriennes peuvent se déclarer compétentes.

CHAPITRE II : TERMINOLOGIE

Article 5 : Accès illégal : Accès sans droit à un système informatique ou tout comportement sans droit susceptible de mettre en péril ou mettant en péril la confidentialité, l'intégrité et la disponibilité de données informatiques.

Altérer : Modifier.

ANADEN : Agence Nationale de Développement du Numérique, Institution de l'État chargée du contrôle et du suivi des activités liées à la sécurité des systèmes d'information et des réseaux de communications électroniques, et à la fourniture des services de confiance.

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

Atteinte à l'intégrité des données : Tout acte intentionnel susceptible de mettre ou mettant en péril la sécurité des données.

Atteinte à l'intégrité d'un système d'information : Tout acte intentionnel entravant l'usage légitime de systèmes informatiques, y compris de systèmes de communications électroniques, en utilisant ou en influençant des données informatiques.

Authentification : Un processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée sous forme électronique ;

Cachet électronique : Des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières ;

Cachet électronique avancé : Un cachet électronique qui satisfait aux exigences énoncées à l'article33 de la présente loi ;

UNION DES COMORES
LE PRESIDENT

Cachet électronique qualifié : Un cachet électronique avancé qui est créé à l'aide d'un dispositif de création de cachet électronique qualifié et qui repose sur un certificat qualifié de cachet électronique ;

Certificat d'authentification de site internet : Une attestation qui permet d'authentifier un site internet et associe celui- ci à la personne physique ou morale à laquelle le certificat est délivré ;

Certificat qualifié d'authentification de site internet : Un certificat d'authentification de site internet, qui est délivré par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées par la présente loi ;

Certificat qualifié de cachet électronique : Un certificat de cachet électronique, qui est délivré par un prestataire de services de confiance qualifié.

Certificat de signature électronique : Une attestation électronique qui associe les données de validation d'une signature électronique à une personne physique et confirme au moins le nom ou le pseudonyme de cette personne ;

Certificat qualifié de signature électronique : Un certificat de signature électronique, qui est délivré par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées par la présente loi ;

CNIL (Commission Nationale Informatique et Liberté) : Autorité nationale administrative indépendante chargée de veiller à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions de la loi relative à la protection des données à caractère personnel.

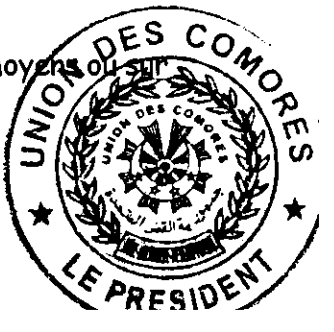
Communication électronique : Toute émission, toute transmission et toute réception de signes, de signaux, d'écrits, d'images, de sons ou d'informations de toute nature par fil, fibre optique, radioélectricité ou autres systèmes électromagnétiques.

Consentement de la personne concernée : Toute manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire ou conventionnel accepte par une déclaration ou par un acte positif clair que les données à caractère personnel le concernant fassent l'objet d'un traitement.

Conservation des données : Conservation des données dans l'état dans lequel elles se trouvent en les protégeant contre tout ce qui pourrait en modifier ou dégrader la qualité ou l'état actuel.

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 : l'ensemble des infractions pénales qui se commettent au moyens ou sur un réseau de communication électronique ou un système d'information ;



Cyberespace : Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques.

Cyber harcèlement : Un acte agressif, intentionnel perpétré par un individu ou un groupe d'individus au moyen de formes de communication électroniques, de façon répétée à l'encontre d'une victime qui ne peut facilement se défendre seule.

Il se pratique via les téléphones portables, messageries instantanées, forums, chats, jeux en ligne, courriers électroniques, réseaux sociaux, sites de partages de photographiés etc.

Il peut prendre plusieurs formes telles que :

. Les intimidations, insultes, moqueries ou menaces en ligne ;
. La propagation des rumeurs ;
. Le piratage de comptes et l'usurpation d'identité digitale ;
. La création d'un sujet de discussion, d'un groupe ou d'une personne sur un réseau social à l'encontre d'un camarade de classe ;
. La publication d'une photo ou d'une vidéo de la victime en mauvaise posture ;
. Le sexting, c'est-à-dire des images produites souvent par les jeunes qui représentent d'autres jeunes et qui pourraient être utilisées dans le cadre de la pornographie infantile ; etc.

Cyber sécurité : Etat de recherche pour un système d'information lui permettant 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 de services connexes que ces systèmes offrent ou qu'ils rendent accessibles .La cyber sécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyber défense.

Cyber sécurité : l'ensemble de mesures , procédures, concepts de sécurité, méthode 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 services connexes que ce système offre ou qu'il rend accessibles. La cyber sécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et la mise en place d'une cyber défense.

Incident de sécurité numérique : Evénement qui porte atteinte à la disponibilité, la confidentialité ou l'intégrité d'une infrastructure comme l'utilisation illégale d'un mot de passe, vol d'équipements informatiques, intrusion dans un fichier ou une application etc.

Diffusion : Action consistant à transmettre des données à autrui.

Dispositif de création de signature électronique : Un dispositif logiciel ou matériel configuré servant à créer une signature électronique;

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

UNION DES COMORES
LE PRESIDENT

Est réputée identifiable, une personne qui peut être identifiée, directement ou indirectement notamment par référence à un identifiant, tel un prénom ou un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique.

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 exécuter une fonction par un système d'information ;

Données relatives aux abonnés : Toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ;

Données relatives au trafic :Toutes données ayant trait à une communication passant par un système d'information, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent ;

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

Entraver: Actions de porter atteinte au bon fonctionnement du système informatique ou de tout autre équipement électronique. Elle résulte de l'introduction, du transfert, de l'endommagement, de l'effacement, de l'altération ou de la suppression de données informatiques. En relation avec un système informatique, l'entrave peut consister, sans s'y limiter, à :

- couper l'alimentation électrique d'un système informatique ;
- provoquer des interférences électromagnétiques dans un système informatique ;
- corrompre un système informatique par quelque moyen que ce soit ;
- introduire, transmettre, endommager, effacer, détériorer, altérer ou supprimer des données informatiques.

Escroquerie : Le fait à travers un système d'information, soit de faire l'usage de faux nom, ou de faux titre, ou de fausse qualité, soit d'employer de manœuvres frauduleuses, des mensonges caractérisés, pour persuader de l'existence de fausses entreprises, d'un pouvoir ou d'un crédit imaginaire, ou pour faire naitre l'esperance ou la crainte d'un succès ou d'un accident ou de tout autre évènement chimérique dans le but de se faire remettre la totalité ou la partie de la fortune d'autrui ou l'obtention de prestation de service.

Fournisseur de services de confiance : Une personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié.

Fournisseur de services de confiance qualifié : Un prestataire de services de confiance qui fournit un ou plusieurs services de confiance qualifiés et a obtenu de l'organe de contrôle le statut qualifié.

UNION DES COMORES
LE PRESIDENT

Horodatage électronique : Des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant.

Information : Tous signes, tous signaux, tous écrits, toutes images, tous sons ou tous enregistrements de toutes natures pouvant être véhiculés par des procédés de communications électroniques.

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

Intégrité : État de sécurité assurant qu'un réseau de communications électroniques, système d'information ou équipement terminal qui est demeuré intact et que les ressources et informations qui y sont 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.

Interception : Acquisition, prise de connaissance, saisie ou copie du contenu ou d'une partie du contenu de toute communication, y compris les données relatives au contenu, les données informatiques, les données relatives au trafic, lors de transmissions non publiques par le biais de moyens techniques. L'interception comprend, sans que cette liste soit limitative, l'écoute, le contrôle ou la surveillance du contenu des communications et l'obtention du contenu des données, soit directement, au moyen de l'accès aux systèmes d'information et de leur utilisation, soit indirectement, au moyen de l'utilisation de dispositifs d'écoute électroniques ou de dispositifs d'écoute par des moyens techniques.

Introduction de données : Manipulations à l'entrée du système de données inexactes, manipulations de programmes ou autres ingérences dans le traitement des données.

Mineur : Toute personne âgée de moins de dix-huit(18) ans, conformément au Code pénal.

Mise à disposition : Action consistant à mettre, entre autres, des dispositifs, matériels, et informations en ligne pour qu'ils soient utilisés par autrui.

Moyen de cryptologie : Tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité.

Opérateur d'infrastructures numériques critiques et vitales : Les personnes publiques et privées gérant des infrastructures numériques critiques et vitales.

UNION DES COMORES
LE PRESIDENT

Opérateur fournissant un accès à internet : Tout opérateur offrant un service permettant un accès à internet à des personnes physiques ou morales, à titre lucratif ou non.

Pornographie/Pédopornographie :

- Toute donnée, quelle qu'en soit la nature ou la forme, représentant de manière visuelle des personnes se livrant à un acte sexuel explicite ou des images réalistes représentant des personnes se livrant à un comportement sexuellement explicite ;
- Tout matériel représentant de manière visuelle un enfant de moins de 18 ans se livrant à un comportement sexuellement explicite, réel ou simulé ;
- Toute représentation des organes sexuels d'un enfant de moins de 18 ans à des fins principalement sexuelles ;
- Tout matériel représentant de manière visuelle une personne qui paraît être un enfant de moins de 18 ans se livrant à un comportement sexuellement explicite, réel ou simulé, ou toute représentation des organes sexuels d'une personne qui paraît être un enfant de moins de 18 ans, à des fins principalement sexuelles ; ou
- Images réalistes d'un enfant de moins de 18 ans se livrant à un comportement sexuellement explicite ou des images réalistes des organes sexuels d'un enfant à des fins principalement sexuelles.

Personne concernée par un traitement de données à caractère personnel : Toute personne physique dont les données à caractère personnel font l'objet d'un traitement ;

Piratage informatique/Hacking : Accès sans autorisation à un système informatique. Il est utilisé pour accéder à des informations confidentielles ou encore pour altérer ou endommager les systèmes et les données qu'elles peuvent comporter. Les attaques pirates peuvent être dirigées vers tous les systèmes informatiques : ordinateurs, comptes de messagerie personnelle, serveurs de grandes compagnies ou infrastructures de sécurité d'un État.

Prestataire de service de confiance : Personne physique ou morale qui fournit un ou plusieurs services de confiance.

Prestation de cryptologie : Toute opération visant à la mise en œuvre, pour le compte d'autrui, des moyens de cryptologie.

Racisme et xénophobie: Tout écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance de l'origine nationale ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou à l'autre de ces éléments ou qui incite à de tels actes.

Sabotage informatique : Manœuvre qui consiste sans autorisation à introduire, modifier ou effacer des données dans un système d'information ou modifier par un moyen technologique l'utilisation normale de données dans un système d'information.

Services de confiance : Services considérés comme essentiels à la création de la confiance en l'économie numérique.

Service d'envoi recommandé électronique : Un service qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée.

Signature électronique : Données électroniques jointes ou liées logiquement à d'autres données électroniques et qui servent à vérifier leur authenticité.

Signature électronique avancée : Une signature électronique qui satisfait aux exigences prévues par l'article 30 de la présente loi.

Signature électronique qualifiée : Une signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifié, et qui repose sur un certificat qualifié de signature électronique.

Surveillance :Toute activité faisant appel à des moyens techniques ou électronique en vue de détecter, d'observer, de copier ou d'enregistrer les mouvements, images, paroles, écrits, ou l'état d'un objet ou d'une personne fixe ou mobile.

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

Technologies de l'Information et de la Communication (TIC) : Toutes techniques utilisées dans le traitement et la transmission des informations, principalement l'informatique, l'internet et les communications électroniques. Elles désignent aussi le secteur d'activité économique des technologies de l'information et de la communication.

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

Traitement automatique ou automatisé de données informatiques : Ensemble des opérations réalisées en totalité ou en partie par des moyens automatisés, relatifs à la collecte, l'enregistrement, l'élaboration, la modification, la conservation, la destruction, l'application d'opérations logiques et/ou arithmétiques l'édition des données et d'une façon générale, leur exploitation sans intervention humaine directe.

Transmission : Tous les transferts de données, par téléphone, télécopie, courriel ou transfert de fichiers.

Violation de données à caractère personnel : Violation de la sécurité entraînant de manière accidentelle ou illicite la destruction, la perte, l'altération, la divulgation ou la consultation non autorisées de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données .

UNION DES COMORES LE PRESIDENT

TITRE I: DE LA CYBERSECURITE

CHAPITRE PREMIER : DES PRESTATIONS DE SERVICES DE CONFIANCE

SECTION I : DE L'AGENCE NATIONALE DE DEVELOPPEMENT DU NUMERIQUE

Article 6 :Il est institué par un décret un établissement public à caractère administratif dénommé ANADEN (L'Agence Nationale de Développement du Numérique), qui assure, à travers son département de cyber-sécurité, le contrôle et le suivi des activités liées à la sécurité des systèmes d'information et des réseaux de communications électroniques, et à la fourniture des services de confiance conformément à la présente loi.

Article 7 : L'ANADEN assure, en matière de cyber-sécurité, les missions suivantes :

- Octroyer l'autorisation d'exercice de l'activité de fournisseur de services de confiance ;
- Contrôler la conformité des signatures électroniques émises et des autres services de confiance ;
- Fixer les standards internationaux à suivre par les fournisseurs de services de confiance en vue d'obtenir le statut de fournisseur agréé ;
- Octroyer et retirer l'agrément aux fournisseurs de services de confiance ;
- Fixer les standards internationaux à suivre par les fournisseurs agréés de services de confiance pour la qualification des services qu'ils fournissent ;
- Octroyer et retirer le statut de service qualifié d'un service de confiance fourni par les fournisseurs agréés des services de confiance ;
- Veiller au contrôle du respect des dispositions de la présente loi et de ses textes d'application par les fournisseurs agréés et non agréés de services de confiance ;
- Analyser les rapports des activités d'audit effectuées par les instances d'évaluation de la conformité auprès des fournisseurs agréés et non agréés des services de confiance ;
- Procéder à des opérations d'audit auprès des fournisseurs agréés et non agréés des services de confiance ou charger les instances d'évaluation de la conformité d'y procéder ;
- Contrôler les activités de sécurité des réseaux de communications électroniques, des systèmes d'information et des services de confiance ;
- Instruire les demandes d'homologation des moyens de cryptographie et de délivrer les certificats d'homologation des équipements de sécurité ;
- Fixer les caractéristiques du dispositif de création et de vérification de la signature électronique ;
- Émettre, délivrer et conserver les certificats électroniques émis par l'Administration publique ;
- Préparer les conventions de reconnaissance mutuelle avec les parties étrangères et de les soumettre à la signature du ministre chargé des communications électroniques ;
- Effectuer un contrôle général des systèmes informatiques et des réseaux relevant des divers organismes publics et privés ;
- S'assurer de la régularité, de l'effectivité des audits de sécurité des systèmes d'information suivant les normes en la matière, des organismes publics et des fournisseurs de services de confiance ;

UNION DES COMORES LE PRESIDENT

- Contrôler l'application par les opérateurs des infrastructures numériques vitales et critiques des obligations qui leur incombent en vertu de la présente loi ;
- Établir des critères en vue de classifier les infrastructures numériques vitales et critiques ainsi que les organismes concernés par cette classification ;
- Contrôler le respect des obligations découlant des dispositions légales et réglementaires dans le domaine de la protection des infrastructures vitales et critiques ;
- Participer à l'élaboration de la politique nationale de sécurité des réseaux de communications électroniques et des échanges électroniques ;
- Émettre un avis consultatif sur les textes touchant à son domaine de compétence;
- Suivre l'exécution des plans et des programmes relatifs à la sécurité des réseaux dans le secteur public à l'exception des applications particulières à la défense et à la sécurité nationale et assurer la coordination entre les intervenants dans ce domaine ;
- Veiller à l'exécution des réglementations relatives à l'obligation de l'audit périodique de la sécurité des systèmes informatiques et des réseaux ;
- Assurer la veille technologique et émettre des alertes et recommandations en matière de sécurité des réseaux de communications électroniques et de services de confiance ;
- Contrôler le respect par les fournisseurs des services de confiance des dispositions de la présente loi et de ses textes d'applications ;
- Etablir des normes spécifiques à la sécurité des réseaux et élaborer des guides techniques en l'objet et procéder à leur publication ;
- Participer aux activités de recherche, de formation et d'études afférentes à la sécurité des réseaux de communications électroniques, des systèmes d'information et des services de confiance.

Un décret précise les modalités d'application des dispositions de l'alinéa 1 du présent article.

Article 8 : L'ANADEN est l'Autorité de certification racine. L'ANADEN est le fournisseur des services de certification de l'Administration Publique.

SECTION II : DE L'EXERCICE DES ACTIVITES DE PRESTATION DES SERVICES DE CONFIANCE

Article 9 : Les activités de prestation des services de confiance sont soumises à une autorisation préalable délivrée par l'ANADEN. Elles sont exercées par des fournisseurs de services de confiance.

Article 10 : Les conditions et les modalités d'octroi de l'autorisation visée à l'article 9 de la présente loi sont fixées par décret.

Article 11 : Les fournisseurs de services de confiance sont responsables du préjudice causé aux personnes qui se sont fiées aux certificats présentés par elles comme qualifiés dans chacun des cas suivants :

- les informations contenues dans le certificat, à la date de sa délivrance, étaient inexactes ;
- les données prescrites pour que le certificat puisse être regardé comme qualifié étaient incomplètes ;
- la délivrance du certificat qualifié n'a pas donné lieu à la vérification que le signataire détient la convention privée correspondant à la convention publique de ce certificat ;
- les fournisseurs de services de confiance et les prestataires de certification n'ont pas, le cas échéant, fait procéder à l'enregistrement de la révocation du certificat qualifié et tenu cette information à la disposition des tiers.

Les fournisseurs de services de confiance ne sont pas responsables du préjudice causé par un usage du certificat qualifié dépassant les limites fixées à son utilisation ou à la valeur des transactions pour lesquelles il peut être utilisé, à condition que ces limites figurent dans le certificat qualifié et soient accessibles aux utilisateurs.

Les fournisseurs de services de confiance doivent disposer justifier d'une garantie financière suffisante, dans une des institutions financières présente sur le territoire national spécialement affectée au paiement des sommes qu'elles pourraient devoir aux personnes s'étant fiées raisonnablement aux certificats qualifiés qu'elles délivrent, ou d'une assurance garantissant les conséquences pécuniaires de leur responsabilité civile professionnelle.

Article 12 : Seuls les fournisseurs de services de confiance agréés peuvent émettre les certificats de signatures électroniques qualifiés, les certificats de cachets électroniques qualifiés et les certificats d'authentification des sites Internet qualifiés.

Article 13 : Le fournisseur de services de confiance agréé doit prendre toutes les mesures légales nécessaires afin de fournir les garanties suivantes :

- L'exactitude de l'information approuvée contenue dans le certificat à sa date de délivrance,
- Le lien entre le titulaire du certificat et ses données de vérification,
- Le fait que le titulaire du certificat soit le seul à détenir un dispositif de création de signature électronique fiable et intégré avec les données de vérification de la signature électronique,
- Le fait que le titulaire du certificat soit le seul à détenir un dispositif de création de cachet électronique qualifié et intégré avec les données de vérification du cachet électronique.
- Tout fournisseur de services de confiance agréé est tenu de tenir un registre électronique des certificats ouvert au public pour consultation de manière permanente et gratuite. Le registre doit comporter les certificats émis par le fournisseur, qu'ils soient valides ou expirés, tout en mentionnant la date d'expiration des certificats ou, le cas échéant, la date de leur annulation.
  Ce certificat doit être protégé de toute modification non autorisée au moyen d'une signature électronique qualifiée ou d'un cachet électronique qualifié du fournisseur de services de confiance agréé.

UNION DES COMORES
LE PRESIDENT

Article 14 : Le fournisseur des services de confiance agréé est tenu d'annuler le certificat dans un délai ne dépassant pas vingt-quatre (24) heures dans les cas suivants :

- À la demande du titulaire du certificat,
- Lorsqu'il est notifié du décès de la personne physique ou de la dissolution de la personne morale titulaire du certificat,
- Suite à la suspension du certificat, si des examens approfondis démontrent que les informations sont erronées ou falsifiées ou non conformes à la réalité ou que le dispositif de création de signature a été violé ou le certificat a été utilisé frauduleusement.

La décision d'annulation du certificat par le fournisseur des services est opposable au titulaire du certificat et aux tiers dès la date de sa publication au registre électronique.

Le fournisseur des services de confiance est tenu d'informer immédiatement le titulaire du certificat de l'annulation et de son motif.

Article 15 : Le fournisseur des services de confiance n'est pas responsable des préjudices résultant du non-respect des conditions d'utilisation du certificat ou des conditions de création de la signature ou du cachet électronique par le titulaire du certificat.

Article 16 : Le titulaire du certificat est seul responsable de la confidentialité et de l'intégrité du dispositif de création de signature qu'il utilise, et toute utilisation de ce dispositif est réputée être son fait.

Le titulaire du certificat est tenu de notifier au fournisseur des services de confiance numérique toute modification des informations contenues dans le certificat.

Article 17 : Le titulaire du certificat d'annuler dispose d'un délai de recours de 48h suivant la notification de contester cette décision devant le fournisseur qui dispose d'un délai de 24h pour répondre il peut saisir l'ANADEN dans un délai de 72h.

SECTION III : DES SERVICES DE CONFIANCE

Article 18 : Les services de confiance comportent les services électroniques suivants :

- Le service de création et de vérification des signatures électroniques et des certificats y afférents ;
- Le service de création et de vérification des cachets électroniques et d'horodatages électroniques ;
- Le service de création et de vérification des certificats pour l'authentification de site internet ;
- Le service d'envoi recommandé électronique ;
- Le service d'archivage électronique ;
- Le service de cryptage.

Les conditions de qualification des services électroniques constituant des prestations de services de confiance et énumérés ci-dessus sont fixées par arrêté du ministre en charge des communications électroniques.

Article 19 : Les prestations de services de confiance qualifiés ne peuvent être fournies pour le compte de tiers ou pour son propre compte que par les fournisseurs agréés des services de confiance électronique.

Article 20 : Les conditions de fiabilité des certificats et de fiabilité des dispositifs de création de signatures électroniques, de cachets électroniques et d'horodatage électronique sont fixées par arrêté du ministre en charge des communications électroniques.

SOUS SECTION I: DU DOCUMENT ET DE LA SIGNATURE ELECTRONIQUE

Article 21 : La conservation du document électronique fait foi au même titre que la conservation du document écrit.

L'émetteur s'engage à conserver le document électronique dans la forme de l'émission. Le destinataire s'engage à conserver ce document dans la forme de la réception.

Le document électronique est conservé sur un support électronique permettant :

- La consultation de son contenu tout au long de la durée de sa validité ;
- Sa conservation dans sa forme définitive de manière à assurer l'intégrité de son contenu ;
- La conservation des informations relatives à son origine et sa destination ainsi que la date et le lieu de son émission ou de sa réception.

Article 22 :L'acte électronique bénéficie de la même force de preuve attachée à l'acte manuscrit.

L'acte électronique est considéré acte authentique lorsqu'il est assorti d'une signature électronique fiable apposée par les officiers publics habilités.

L'acte électronique est considéré acte sous seing privé lorsqu'il est assorti d'une signature électronique fiable apposée par le signataire.

Article 23 : Dans tous les cas où les dispositions législatives ou réglementaires nécessitent une signature manuscrite, cette exigence est considérée remplie lorsqu'une signature électronique fiable est utilisée.

Article 24 : La signature électronique peut être utilisée comme élément de preuve auprès des tribunaux et ne peut être refusée au seul motif qu'elle est électronique.

Article 25 : Chaque personne désirant apposer sa signature électronique sur un document peut créer cette signature par un dispositif fiable dont les caractéristiques techniques seront fixées par arrêté du ministre en charge des communications électroniques.

Article 26 : Chaque personne utilisant un dispositif de signature électronique doit :

- Prendre des précautions minimales qui seront fixées par arrêté du ministre en charge des communications électroniques, afin d'éviter toute utilisation illégitime des éléments de cryptage ou des équipements personnels relatifs à sa signature.
- Informer le fournisseur de services de confiance de toute utilisation illégitime de sa signature.

UNION DES COMORES
LE PRÉSIDENT

- **Veiller** à la véracité de toutes les données qu'elle a déclarées au fournisseur de services de confiance et à toute personne à qui il a demandé de se fier à sa signature.

Article 27 : En cas de non-respect des engagements prévus par la présente loi, le titulaire de la signature est responsable du préjudice causé à autrui.

Article 28 : La signature électronique avancée a la même valeur juridique que la signature manuscrite et produit les mêmes effets que cette dernière.

Article 29 : Une signature électronique avancée doit remplir les conditions ci-après:

- Les données afférentes à la création de la signature sont liées exclusivement au signataire et sont sous son contrôle exclusif ;
- Toute modification à elle apportée, est facilement décelable ;
- Elle est créée au moyen d'un dispositif sécurisé dont les caractéristiques techniques sont fixées par un arrêté du ministre en charge des communications électroniques ;
- Le certificat utilisé pour la génération de la signature est un certificat qualifié. Un arrêté du ministre en charge des communications électroniques fixe les critères de qualification des certificats.

Article 30 : La signature électronique qualifiée répond aux conditions suivantes :

- Remplir les conditions de signature électronique avancée conformément aux dispositions de l'article 29 de la présente loi ;
- Être créée au moyen d'un dispositif fiable de création de signature électronique ;
- Être rattachée à un certificat de signature électronique qualifiée.

Article 31 : Les certificats électroniques qualifiés ne sont valables que pour les objets pour lesquels ils ont été émis.
Les dispositifs de création et de vérification des certificats qualifiés sont du point de vue technologique neutres, normalisés, homologués et interopérables.

Article 32 : Le fournisseur des services de confiance ayant conféré la validité à un certificat électronique ne peut le renier.

Article 33 : Un certificat électronique émis hors du territoire national produit les mêmes effets juridiques qu'un certificat qualifié émis aux Comores à condition qu'il existe un acte de reconnaissance de l'organisme émetteur signé par le ministre en charge des Communications électroniques.

L'interopérabilité des certificats électroniques qualifiés est règlementée par un arrêté du ministre en charge des communications électroniques.

UNION DES COMORES
LE PRESIDENT

Article 44 : Les documents électroniques qui ont été conservés au moyen d'un service qualifié d'archivage électronique sont considérés sécurisés contre toute modification de leur contenu sauf modifications nécessaires aux fins d'archivage ou de numérisation.

Article 45 : La copie électronique d'un document papier est considérée copie conforme à l'original lorsqu'elle est créée et conservée au moyen d'un service qualifié d'archivage électronique. Dans tel cas, le document papier original peut être détruit tant que la destruction ne déroge pas aux dispositions légales en vigueur.

CHAPITRE II : DE LA SECURITE DES RESEAUXET DES SYSTEMES INFORMATIQUES.

Article 46 : Tout exploitant d'un système informatique ou réseau, qu'il soit organisme public ou privé, doit informer immédiatement ANADEN de toutes attaques, intrusions et autres perturbations susceptibles d'entraver le fonctionnement d'un autre système informatique ou réseau, afin de lui permettre de prendre les mesures nécessaires pour y faire face.

L'exploitant est tenu de se conformer aux mesures arrêtées par l'ANADEN pour mettre fin à ces perturbations.

Article 47 : En vue de protéger les systèmes informatiques et les réseaux, l'ANADEN peut proposer l'isolement du système informatique ou du réseau concerné jusqu'à ce que ces perturbations cessent. L'isolement est prononcé par décision de l'ANADEN.

Article 48 : Les systèmes informatiques et les réseaux relevant des divers organismes publics sont soumis à un régime d'audit obligatoire et périodique de la sécurité, à l'exception des systèmes informatiques et des réseaux appartenant aux ministères de la défense nationale et de l'intérieur.

Sont également soumis à l'audit obligatoire périodique de la sécurité, les systèmes informatiques et les réseaux des organismes qui seront fixés par décret.

Sont fixés par décret, les critères relatifs à la nature de l'audit, à sa périodicité et aux procédures de suivi de l'application des recommandations contenues dans le rapport d'audit.

Article 49 : Dans le cas où les organismes prévus à l'article 48 de la présente loi n'effectuent pas l'audit obligatoire périodique, l'ANADEN avertit l'organisme concerné qui devra effectuer l'audit dans un délai ne dépassant pas un mois à partir de la date de cet avertissement.

À l'expiration de ce délai sans résultat, l'ANADEN est tenue de désigner, aux frais de l'organisme contrevenant, un expert qui sera chargé de l'audit sus indiqué.

Article 50 : Sous réserve des exceptions prévues pat l'article 48 de la présente loi, les organismes publics et privés doivent permettre à l'ANADEN et aux experts qui seront chargés de l'opération d'audit, de consulter tous les documents et dossiers relatifs à la sécurité informatique afin d'accomplir leurs missions.

UNION DES COMORES
LE PRESIDENT

Article 51 : L'opération d'audit est effectuée par des experts, personnes physiques ou morales, préalablement certifiées par l'ANADEN.

Sont fixées par décret, les conditions et les procédures de certification de ces experts.

Article 52 : Il est interdit aux agents de l'ANADEN et aux experts chargés des opérations d'audit de divulguer toutes informations dont ils ont eu connaissance lors de l'exercice de leurs missions.

CHAPITRE III : DE LA SECURITE DES INFRASTRUTURES NUMERIQUE VITALES ET CRITIQUES

Article 53 :L'ANADEN établit la liste des opérateurs d'infrastructures numériques vitales et critiques sur la base des critères suivants :

- Le nombre d'utilisateurs de l'installation ou du service fourni,
- La taille du marché du service fourni,
- La durée et le niveau des impacts et les résultats significatifs qui pourraient en découler,
- Le niveau de connexion avec d'autres systèmes d'information ou réseaux utilisés pour le fonctionnement d'infrastructures vitales et critiques,
- L'importance des systèmes d'information ou des réseaux dans la fourniture du niveau de service requis et les possibilités de leur substitution,
- La portée géographique de l'impact significatif et son ampleur par rapport à des zones particulières du territoire national.

Article 54 :L'ANADEN élabore des rapports trimestriels qu'elle soumet au ministre en charge des communications électroniques sur le niveau de risques auxquels sont confrontés les infrastructures numériques vitales et critiques et l'espace numérique national.

Article 55 :L'ANADEN approuve le plan de sécurité des systèmes d'information et des réseaux pour les opérateurs des infrastructures numériques sensibles et critiques selon des modalités fixées par l'ANADEN en vue de garantir la confidentialité du contenu du document et des informations et données qu'il comporte.

Article 56 : Tout opérateur d'infrastructure numérique vitale et critique s'engage à élaborer et à mettre en œuvre un plan de sécurité de ses systèmes d'information et réseaux les caractéristiques de l'infrastructure vitale et critique qu'il gère.

Le plan de sécurité des systèmes d'information et des réseaux comporte obligatoirement ce qui suit :

- Un plan de continuité du fonctionnement des systèmes d'information et réseaux sensibles et critiques ;
- Un plan de gestion des risques comportant une analyse des risques.

Ce plan est approuvé par l'ANADEN. Il est mis à jour d'une manière périodique définie par l'ANADEN et au moins une fois par an.

UNION DES COMORES
LE PRESIDENT

SOUS-SECTION II : DES AUTRES PRESTATIONS DES SERVICES DE CONFIANCE

Article 34 : Le cachet électronique peut être utilisé comme élément de preuve auprès des tribunaux et ne peut être refusé au seul motif qu'il est électronique.

Article 35 : Le cachet électronique avancé répond aux conditions suivantes :

- Être exclusivement rattaché au titulaire du cachet.
- Permettre d'identifier le titulaire du cachet,
- Être créé au moyen de données de création du cachet électronique soumises au contrôle exclusif de son titulaire,
- Être rattaché aux données sur lesquelles a été apposé le cachet de manière à laisser apparaitre toute modification ultérieure apportée.

Article 36 : Le cachet électronique qualifié répond aux conditions suivantes :

- Remplir les conditions de cachet électronique avancé conformément aux dispositions de l'article 33 de la présente loi.
- Être créé au moyen d'un dispositif fiable de création de cachet électronique,
- Être rattaché à un certificat de cachet électronique avancé.

Article 37 : L'horodatage électronique peut être utilisé comme élément de preuve auprès des tribunaux et ne peut être refusé au seul motif qu'il est électronique. Lorsque l'horodatage électronique est fiable, la date et l'heure auxquelles il renvoie ainsi que l'intégrité des données rattachées sont considérées comme certaines.

Article 38 : Dans tous les cas où les dispositions législatives ou réglementaires nécessitent l'établissement de la date, cette exigence est considérée remplie lorsqu'un horodatage électronique fiable est utilisé.

Article 39 : Les données envoyées et reçues au moyen d'un service de messagerie électronique recommandée font foi devant les tribunaux comme éléments de preuve et ne peuvent être refusées au seul motif qu'elles sont électroniques.

Article 40 : Dans tous les cas où les dispositions légales et réglementaires exigent des écrits recommandés, cette obligation est considérée remplie lorsqu'est utilisé un service qualifié de messagerie électronique recommandée.

Article 41 : Les données envoyées et reçues au moyen d'un service qualifié de messagerie électronique recommandée jouissent de la garantie de reconnaissance de :

- L'exactitude et l'intégrité de leur contenu ;
- Leur envoi de la part de l'expéditeur défini ;
- Leur réception par le destinataire défini ;
- Le caractère certain de la date et de l'heure d'envoi et de réception.

Article 42 : Les archives électroniques font foi devant les tribunaux comme éléments de preuve et ne peuvent être refusés en raison de leur forme électronique.

Article 43 : Dans tous les cas où les dispositions légales et réglementaires exigent la conservation de documents sous format papier ou électronique, cette obligation est considérée remplie lorsqu'est utilisé un service qualifié d'archivage électronique.

Article 57 : Tout opérateur d'infrastructure numérique vitale et critique est tenu de veiller à la conformité de ses systèmes d'information sensibles et critiques aux règles légales et à la réglementation relatives à la sécurité informatique ainsi qu'aux normes fixées à cet effet par l'ANADEN.

Article 58 : Tout opérateur d'infrastructure vitale et critique est tenu d'élaborer un manuel et des règlements afférents aux systèmes d'informations vitales et critiques et de le soumettre à l'ANADEN pour approbation dans un délai n'excédant pas un mois à compter de la date de son élaboration.

Les manuels et les règlements des systèmes d'information des infrastructures numériques vitales et critiques sont confidentiels.

Article 59: Tout opérateur d'infrastructure vitale et critique est tenu de fournir les moyens nécessaires pour contrôler les attaques et les incidents numériques et y faire face, de mettre à la disposition de l'ANADEN les données obtenues par le biais de ces moyens afin de lui permettre d'analyser le risque et de développer les moyens pour y faire face,

Article 60 : En cas de survenance d'un incident numérique, l'opérateur concerné est tenu de transmettre à l'ANADEN les données et rapports afférents aux attaques, intrusions et incidents qu'il a subis et ce dans un délai de quarante-huit (48) heures à compter de leur survenance. Il est également tenu de fournir à l'ANADEN les informations supplémentaires qu'elle demande concernant l'incident. L'ANADEN peut intervenir sur le terrain le cas échéant.

Article 61 : En cas de survenance d'un incident numérique grave, l'ANADEN est tenue de présenter au ministre en charge des communications électronique et aux ministres en charge de la défense nationale et de la sécurité nationales un rapport détaillé comportant toutes les informations obtenues, les recommandations découlant de ces informations et les mesures à prendre par l'organisme concerné.

Article 62 : Les opérateurs des infrastructures numériques vitales et critiques sont tenus de soumettre leurs systèmes à un programme d'audit fixé par l'ANADEN et mis en œuvre par l'ANADEN directement ou par l'intermédiaire de prestataires privés qu'elle approuve. Les opérateurs concernés sont tenus de mettre en œuvre les conclusions et les recommandations l'application des opérations d'audit sous le contrôle de l'ANADEN.

Article 63 :L'ANADEN établit en cas d'urgence numérique un Plan d'intervention en vue d'éviter les incidents numériques et d'y faire face ou d'atténuer leurs effets et d'assurer la reprise des services d'importance vitale et de garantir leur continuité.

Un décret fixe les conditions et les procédures d'élaboration du plan d'urgence numérique ainsi que les modalités de sa mise en œuvre et de son suivi.

UNION DES COMORES
LE PRESIDENT

CHAPITRE IV : DES MOYENS ET DES PRESTATIONS DE CRYPTOLOGIE

Article 64 :L'utilisation des moyens de cryptologie est libre.
La fourniture, le transfert depuis ou vers un autre État, l'importation et l'exportation des moyens de cryptologie assurant exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont libres

La fourniture, le transfert depuis un autre État ou l'importation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont soumis à une déclaration préalable auprès du Ministre en charge des communications électroniques, sauf dans les cas prévus du présent article.

Le fournisseur ou la personne procédant au transfert ou à l'importation tient à la disposition du Ministre en charge des communications électroniques une description des caractéristiques techniques de ce moyen de cryptologie, ainsi que le code source des logiciels utilisés. Un décret fixe :

- Les conditions dans lesquelles sont souscrites ces déclarations, les conditions et les délais dans lesquels le ministre en charge des communications électroniques peut demander communication des caractéristiques du moyen, ainsi que la nature de ces caractéristiques ;
- Les catégories de moyens dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'État, leur fourniture, leur transfert depuis un autre État ou leur importation peuvent être dispensés de toute formalité préalable.

Le transfert vers un autre État et l'exportation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont soumis à autorisation du ministre en charge des communications électroniques, sauf dans les cas prévus par le présent article. Un décret fixe :

- Les conditions dans lesquelles sont souscrites les demandes d'autorisation ainsi que les délais dans lesquels le Ministre en charge des communications électroniques statue sur ces demandes ;
- Les catégories de moyens dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'État de l'Union des Comores, leur transfert vers un autre État ou leur exportation peuvent être soit soumis au régime déclaratif et aux obligations d'information prévus au paragraphe III du présent article, soit dispensés de toute formalité préalable.

Article 65 : La fourniture de prestations de cryptologie doit être déclarée auprès du ministre en charge des communications électroniques. Un décret définit les conditions dans lesquelles est effectuée cette déclaration et peut prévoir des exceptions à cette obligation pour les prestations dont les caractéristiques techniques ou les conditions de fourniture sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'État, cette fourniture peut être dispensée de toute formalité préalable.

Les personnes exerçant cette activité sont assujetties au secret professionnel.

Sauf à démontrer qu'elles n'ont commis aucune faute intentionnelle ou négligence, les personnes fournissant des prestations de cryptologie à des fins de confidentialité sont responsables au titre de ces prestations, nonobstant toute stipulation contractuelle contraire, du préjudice causé aux personnes leur confiant la gestion de leurs conventions secrètes en cas d'atteinte à l'intégrité, à la confidentialité ou à la disponibilité des données transformées à l'aide de ces conventions.

Sauf à démontrer qu'ils n'ont commis aucune faute intentionnelle ou négligence, les prestataires de services de certification électronique sont responsables du préjudice causé aux personnes qui se sont fiées raisonnablement aux certificats présentés par eux comme qualifiés dans chacun des cas suivants :

- Les informations contenues dans le certificat, à la date de sa délivrance, étaient inexactes ;
- Les données prescrites pour que le certificat puisse être regardé comme qualifié étaient incomplètes ;
- La délivrance du certificat n'a pas donné lieu à la vérification que le signataire détient la convention privée correspondant à la convention publique de ce certificat ;
- Les prestataires n'ont pas, le cas échéant, fait procéder à l'enregistrement de la révocation du certificat et tenu cette information à la disposition des tiers.

Les prestataires ne sont pas responsables du préjudice causé par un usage du certificat dépassant les limites fixées à son utilisation ou à la valeur des transactions pour lesquelles il peut être utilisé, à condition que ces limites figurent dans le certificat et soient accessibles aux utilisateurs.

Ils doivent justifier d'une garantie financière suffisante, spécialement affectée au paiement des sommes qu'ils pourraient devoir aux personnes s'étant fiées raisonnablement aux certificats qualifiés qu'ils délivrent, ou d'une assurance garantissant les conséquences pécuniaires de leur responsabilité civile professionnelle.

Article 66 : Lorsqu'un fournisseur de moyens de cryptologie, même à titre gratuit, ne respecte pas les obligations auxquelles il est assujetti en application de l'article 65 de la présente loi, le ministre en charge des communications électroniques peut, après avoir mis l'intéressé à même de présenter ses observations, prononcer l'interdiction de mise en circulation du moyen de cryptologie concerné.

L'interdiction de mise en circulation est applicable sur l'ensemble du territoire national. Elle emporte en outre pour le fournisseur l'obligation de procéder au retrait :

- Auprès des diffuseurs commerciaux, des moyens de cryptologie dont la mise en circulation a été interdite ;
- Des matériels constituant des moyens de cryptologie dont la mise en circulation a été interdite et qui ont été acquis à titre onéreux, directement ou par l'intermédiaire de ces diffuseurs commerciaux.

UNION DES COMORES
UNION DES COMORES
LE PRESIDENT

Le moyen de cryptologie concerné pourra être remis en circulation dès que les obligations antérieurement non respectées auront été satisfaites, dans les conditions prévues à l'article 65 de la présente loi.

Article 67 : Outre les officiers et agents de police judiciaire, agissant conformément aux dispositions qui régissent leurs activités, et, dans leur domaine de compétence, les agents des douanes ainsi que les agents habilités à cet effet par le Ministre en charge des communications électroniques peuvent rechercher et constater par procès-verbal les infractions aux dispositions des articles 65 et 66 de la présente loi et des textes pris pour leur application.

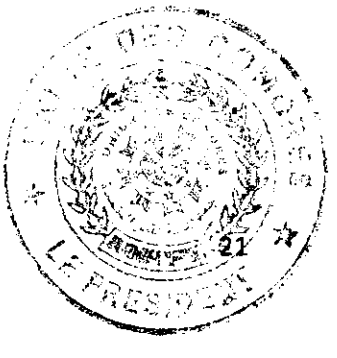
Les agents habilités par le ministre en charge des communications électroniques mentionnés à l'alinéa précédent peuvent accéder aux moyens de transport, terrains ou locaux à usage professionnel, à l'exclusion des parties de ceux-ci affectées au domicile privé, en vue de rechercher et de constater les infractions, demander la communication de tous les documents professionnels et en prendre copie, recueillir, sur convocation ou sur place, les renseignements et justifications. Les agents ne peuvent accéder à ces locaux que pendant leurs heures d'ouverture lorsqu'ils sont ouverts au public et, dans les autres cas, qu'entre huit (8) heures et vingt (20) heures.

Le procureur de la République est préalablement informé des opérations envisagées en vue de la recherche des infractions. Il peut s'opposer à ces opérations. Les procès-verbaux lui sont transmis dans les cinq jours suivant leur établissement. Une copie en est également remise à l'intéressé.

Les agents habilités peuvent, dans les mêmes lieux et les mêmes conditions de temps, procéder à la saisie des moyens de cryptologie sur autorisation judiciaire. La demande doit comporter tous les éléments d'information de nature à justifier la saisie. Celle-ci s'effectue sous l'autorité et le contrôle du juge qui l'a autorisée.

Les matériels et logiciels saisis sont immédiatement inventoriés. L'inventaire est annexé au procès-verbal dressé sur les lieux. Les originaux du procès-verbal et de l'inventaire sont transmis, dans les cinq jours suivant leur établissement, au juge qui a ordonné la saisie. Ils sont versés au dossier de la procédure.

Le président du tribunal ou le magistrat délégué par lui peut à tout moment, d'office ou sur la demande de l'intéressé, ordonner la mainlevée de la saisie.
Est puni de six mois d'emprisonnement et d'une amende maximale de 10 000 000 FC le fait de faire obstacle au déroulement des enquêtes prévues au présent article ou de refuser de fournir les informations ou documents y afférant.



TITRE II : DE LA LUTTE CONTRE LA CYBERCRIMINALITE

CHAPITRE PREMIER : INFRACTIONS SPECIFIQUES AUX TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION (TIC)

Article 68 : Constitue une atteinte aux systèmes d'information le fait d'infecter un système d'information et de communication, tout comme l'intrusion par l'accès et le maintien frauduleux ou irrégulier dans tout ou partie d'un système d'information, ainsi que l'introduction frauduleuse de données dans tout ou partie d'un système d'information,

Est puni d'un à deux ans d'emprisonnement et de 500.000 à 5.000.000 de francs comoriens d'amende, quiconque accède ou tente d'accéder frauduleusement à tout ou partie d'un système d'information.

Est puni de cinq à dix ans d'emprisonnement et de 4.000.000 à 6.000.000 de francs comoriens d'amende, quiconque produit ou fabrique un ensemble de données par l'introduction, engendrant des données contrefaites, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient originales.

Est puni d'un à cinq ans d'emprisonnement et de 3.000.000 à 5.000.000 de francs comoriens d'amende, quiconque obtient frauduleusement, pour soi-même ou pour autrui, un avantage quelconque, par l'introduction de données informatiques ou par toute forme d'atteinte au système d'information.

Article 69 : Constitue une atteinte à l'intégrité des systèmes d'information toute action faite de manière intentionnelle et sans droit, directement ou indirectement par tout moyen technologique, qui provoque une interruption du fonctionnement normal d'un système informatique.

Est puni d'un emprisonnement de deux ans à cinq ans et d'une amende de 10.000.000 à 20.000.000 de francs comoriens ou de l'une de ces peines seulement quiconque porte atteinte à l'intégrité d'un système d'information.

Est puni d'un emprisonnement de cinq ans à dix ans et d'une amende de 10.000.000 à 20.000.000 de francs comoriens ou de l'une de ces peines seulement, quiconque, suite à la commission des faits visés à l'alinéa premier, cause un dommage à des données dans le système d'information concerné ou dans tout autre système d'information,

Est condamné à la réclusion criminelle à temps de dix ans à vingt ans et à une amende de 20.000.000 à 50.000.000 de francs comoriens ou de l'une de ces peines seulement, quiconque, suite à la commission des faits visés à l'alinéa premier, provoque une perturbation grave ou empêche, totalement ou partiellement, le fonctionnement normal du système d'information concerné ou de tout autre système d'information,

La personne responsable des faits visés à l'alinéa premier, est condamnée à la réclusion criminelle à temps de dix ans à vingt ans et à une amende de 30.000.000 à 50.000.000 de francs comoriens ou de l'une de ces peines seulement, lorsque la commission des faits visés à l'alinéa premier touche une ou plusieurs infrastructures sensibles et critiques, au sens de la présente loi.

La peine d'emprisonnement et l'amende sont applicables même si les conséquences sur le ou les systèmes d'information visés aux alinéas précédents sont temporaires ou permanentes.

UNION DES COMORES
UNION DES COMORES
LE PRESIDENT

Article 70 : Constitue une atteinte à l'intégrité des données, toute action réalisée de manière intentionnelle et sans droit, directement ou indirectement, qui altère ou tente d'altérer, modifie ou tente de modifier, supprime ou tente de supprimer, qui endommage ou tente d'endommager, qui efface ou tente d'effacer frauduleusement des données informatiques.

Est puni de cinq à dix ans d'emprisonnement et de 4.000.000 à 6.000.000 de francs comoriens d'amende, quiconque porte atteinte à l'intégrité des données.

Si l'infraction visée à l'alinéa premier est commise avec une intention frauduleuse ou dans le but de nuire, la peine d'emprisonnement est de dix à vingt ans et l'amende de 10.000.000 à 20.000.000 ou l'une de ces deux peines seulement.

Est puni de un à cinq ans d'emprisonnement et de 3.000.000 à 5.000.000 de francs comoriens d'amende, quiconque obtient frauduleusement, pour soi-même ou pour autrui, un avantage quelconque, par l'utilisation, la modification, l'altération ou la suppression de données informatiques ou par toute forme d'atteinte à l'intégrité des données.

La peine d'emprisonnement et l'amende sont applicables même si les conséquences sur les données visées aux alinéas précédents sont temporaires ou permanentes.

Article 71 : Constitue une atteinte aux données informatiques, le fait d'intercepter ou de tenter d'intercepter, divulguer, utiliser, altérer ou détourner intentionnellement et sans droit par des moyens techniques, des données informatiques lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques.

Est puni de cinq à dix ans d'emprisonnement et de 4.000.000 à 6.000.000 de francs comoriens d'amende, quiconque porte atteinte aux données informatiques.

Est puni d'un emprisonnement de cinq ans à dix ans et d'une amende de cinq millions 10.000.000 à 20 000 000) de francs comoriens, quiconque transfère sans autorisation des données d'un système d'information ou d'un moyen de stockage de données informatiques.

Si l'infraction visée à l'alinéa précédent est commise avec une intention frauduleuse, ou en rapport avec un système d'information connecté à un autre système information, ou en contournant les mesures de protection mises en place pour empêcher l'accès au contenu de la transmission non publique, les peines prévues à l'alinéa précédent sont doublées.

Une personne ne commet pas une infraction au sens du présent article, si :

- l'interception est réalisée conformément à un mandat de justice ;
- la communication est envoyée par ou est destinée à une personne qui a consenti à l'interception ;
- un fonctionnaire habilité estime qu'une interception est nécessaire en cas d'urgence, dans le but de prévenir un décès, une blessure ou un dommage à la santé physique ou mentale d'une personne, ou d'atténuer une blessure ou un dommage à la santé physique ou mentale d'une personne ;
- une personne morale ou physique légalement autorisée pour les besoins de la sécurité publique ou de la défense nationale ; ou
- une personne morale ou physique légalement autorisée en vertu des dispositions du code de procédure pénale.

UNION DES COMORES
LE PRESIDENT

Article 72 : Constitue un sabotage informatique le fait de transmettre ou de modifier des données sans autorisation, de falsifier ou de dissimuler de données enregistrées sur n'importe quel système d'information, tout comme le fait d'effacer ou détruire des données et de logiciels, de même que le fait d'entraver l'accès à un système d'information. Est puni de un à cinq ans d'emprisonnement et de 1.000.000 à 4.000.000 de francs comoriens d'amende, quiconque entrave, fausse ou tente d'entraver ou de fausser frauduleusement le fonctionnement d'un système d'information.

Est puni de cinq à dix ans d'emprisonnement et de 4.000.000 à 6.000.000 de francs comoriens d'amende, quiconque altère ou tente d'altérer, modifie ou tente de modifier, supprime ou tente de supprimer frauduleusement des données informatiques.

Est puni de cinq à dix ans d'emprisonnement et de 4.000.000 à 6.000.000 de francs comoriens d'amende, quiconque produit ou fabrique un ensemble de données par la modification, l'altération ou la suppression frauduleuse de données informatiques, engendrant des données contrefaites, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient originales.

Est puni de un à cinq ans d'emprisonnement et de 3.000.000 à 5.000.000 de francs comoriens d'amende, quiconque obtient frauduleusement, pour soi-même ou pour autrui, un avantage quelconque par la modification, l'altération ou la suppression de données informatiques ou par toute forme de sabotage informatique.

Article 73 : Constitue un acte de piratage informatique ou de hacking tout comportement qui consiste à manipuler un système d'information et de communication, sans qu'il soit tenu compte ou non du but poursuivi par l'auteur, ou tout comportement qui consiste à saboter un système d'information et de communication par le fait de casser le système de sécurité mis en place par le propriétaire, afin d'accéder aux informations confidentielles stockées dans le système ou de fausser le système.

Est puni d'un emprisonnement de deux à cinq ans et d'une amande de 2.000.000 à 5.000.000 de francs comoriens quiconque se rend coupable de piratage.

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

Article 74 : Constitue une usurpation d'identité le fait de s'emparer de l'identité d'un tiers ou de faire usage d'une ou de plusieurs données d'identification de toute nature y compris son adresse IP, son pseudonyme sur un réseau social permettant de l'identifier en vue ou non pour l'auteur de l'acte, de troubler sa tranquillité ou celle d'autrui ou de porter atteinte à son honneur ou à sa considération.

Est puni de un à cinq ans de prison et d'une amande 1.000.000 à 4.000.000 de francs comoriens quiconque se rend coupable d'usurpation d'identité.

UNION DES COMORES
LE PRESIDENT

Article 75 : Constitue un acte de cyber harcèlement tout fait qui consiste à utiliser un réseau ou un service de communications électroniques ou un autre moyen électronique par l'initiation d'une communication électronique qui contraint, intimide, harcèle ou provoque une détresse émotionnelle chez une personne, dans le but d'encourager un comportement grave, répété et hostile ayant pour objet ou pour effet une dégradation de ses conditions de vie se traduisant par une altération de sa santé physique ou mentale.

Est puni d'un emprisonnement d'un an à cinq ans et d'une amande de 3.000.000 à 5.000.000 de francs comoriens quiconque se rend coupable de cyber harcèlement.

Est puni d'une peine d'emprisonnement d'un mois à deux ans et d'une amende de 5.00.000 à 5.000.000 de francs comoriens, ou de l'une de ces deux peines seulement quiconque aura harcelé, par le biais d'une communication électronique, une personne alors qu'il savait ou aurait dû savoir qu'il affecterait gravement par ce comportement la tranquillité de la personne visée.

Est puni d'une peine d'emprisonnement d'un mois à six mois et d'une amende de 500.000 à 3.000.000 de francs comoriens, ou de l'une de ces peines seulement quiconque initie ou relaie une fausse information contre une personne par le biais des réseaux sociaux ou toute forme de support électronique.

Si les faits visés aux alinéas 3 et 4 sont commis au préjudice d'une personne dont la situation de vulnérabilité en raison de l'âge, d'un état de grossesse, d'une maladie, d'une infirmité ou d'une déficience physique ou mentale était apparente ou connue de l'auteur des faits, les peines minimales prévues aux alinéas précédents seront doublées.

Nonobstant les sanctions prévues pour l'infraction, la victime du cyber harcèlement peut demander le retrait des publications à leur auteur ou au responsable du support informatique.

Article 76 : Constitue une diffusion illégale des contenus personnels la révélation, la fourniture à un tiers ou le fait de porter à la connaissance du public, sans l'autorisation de la personne concernée, une ou des images ou des enregistrements audiovisuels, qui ont été obtenues auprès d'elle ou dans un autre endroit ou contexte hors de portée des tiers et qui porte gravement atteinte au droit à la vie privée de la personne.
Est puni de un à cinq ans d'emprisonnement et de 5.000.000 à 10.000.000 de francs comoriens d'amande quiconque se rendra coupable de diffusion illégale.

Article 77 : Constitue une violation du secret des correspondances électroniques toute violation par l'ouverture, la suppression, le retardement, l'écoute, l'interception, le stockage de communications et des données relatives au trafic y afférentes, ou la soumission à tout autre moyen d'interception ou de surveillance, ou le détournement de correspondances électroniques arrivées ou non à destination, exclusivement destinées à un tiers ou à plusieurs personnes physiques ou morales, déterminées ou individualisées, par le fait de tout autre personne autre que les utilisateurs y compris les fournisseurs de messagerie électronique ou les fournisseurs d'accès à internet, sans le consentement des utilisateurs.

Est puni d'un à cinq ans d'emprisonnement et de 10.000.000 à 20.000.000 de francs comoriens d'amande quiconque se rend responsable d'une violation du secret des correspondances électroniques.

S'agissant des personnes dépositaires de l'autorité publique, des personnes chargées d'une mission de service public et des personnes agissant dans l'exercice ou à l'occasion de l'exercice de leur fonction ou mission, si ces dernières violent les dispositions de l'alinéa premier hors les cas prévu par la loi, la violation du secret des correspondances est punie de trois à dix ans d'emprisonnement et de 10.000.000 à 20.000.000 de francs comoriens d'amande.

Article 78 : Constitue un vol d'information tout fait qui consiste à prendre frauduleusement connaissance d'une information à l'intérieur d'un système d'information électronique, ou copier frauduleusement une information à partir d'un tel système, ou encore soustraire frauduleusement le support physique sur lequel se trouve une information.

Est puni d'un emprisonnement de cinq à dix ans et de 3.000.000 à 5.000.000 de francs d'amende quiconque commet un vol d'information.

La tentative est punissable.

La peine est d'un emprisonnement de dix à vingt ans et d'une amende **de 5.000.000** à 10.000.000 de francs comoriens si le vol d'information ou la tentative de vol d'information a été commis accompagné d'une au moins des circonstances ci-après :

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

Article 79 : Le vol d'information ou la tentative de vol d'information est puni de vingt ans d'emprisonnement et de 10.000.000 **à 20.000.000** de francs comoriens d'amende, s'il a été commis dans l'une des deux circonstances ci-après :

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

Est puni de **cinq à dix ans** d'emprisonnement et de **5.000.000 à 10.000.000** de francs comoriens d'amende, quiconque fait usage, en connaissance de cause, de données informatiques frauduleusement obtenues.

UNION DES COMO
UNION DES COMORES
LE PRESIDENT

Article 80 : La pédopornographie est tout fait qui consiste sans droit avec l'usage d'un système d'information ou tout autre moyen de stockage pour exposer, produire pour lui-même ou pour autrui, vendre, offrir, louer, distribuer, transmettre, diffuser, publier ou mettre à la disposition des emblèmes, objets, films, photos, diapositives ou autres supports visuels qui représentent des positions ou des actes sexuels à caractère pornographique, impliquant ou présentant des mineurs ou les aura, en vue du commerce ou de la distribution, la diffusion, fabriqués, détenus, importés ou fait importer, remis à un agent de transport ou de distribution.

Est puni de cinq à dix ans d'emprisonnement et de 7.000.000 à 10.000.000 de francs comoriens d'amende, quiconque produit, enregistre, offre, met à disposition, diffuse, transmet une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système d'information ou d'un moyen de stockage de données informatiques.

Est puni de cinq à dix ans d'emprisonnement et de 5.000.000 à 10.000.000 de francs comoriens d'amende, quiconque se procure ou procure à autrui, importe ou fait importer, exporte ou fait exporter une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système d'information ou d'un moyen de stockage de données informatiques.

Est puni de trois à cinq ans d'emprisonnement et de 2.000.000 à 4.000.000 de francs comoriens d'amende, quiconque possède intentionnellement une image ou une représentation présentant un caractère de pornographie infantile dans un système d'information ou dans un moyen de stockage de données informatiques.

Est puni de trois à cinq ans d'emprisonnement et de 2.000.000 à 4.000.000 de francs comoriens d'amende, quiconque facilite l'accès à des images, des documents, du son ou une représentation présentant un caractère de pornographie à un mineur.

Article 81 : La falsification informatique tout fait qui consiste à commettre un faux, en introduisant, intentionnellement et sans droit, dans un système informatique, en modifiant, altérant ou effaçant des données, qui sont stockées, traitées ou transmises par un système d'information, ou en modifiant par tout moyen technologique l'utilisation possible des données dans un système d'information, et ce dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si les données falsifiées étaient authentiques.

Est puni d'un emprisonnement de cinq ans à dix ans et d'une amende de 10.000.000 à 20.000.000 de francs comoriens ou de l'une de ces peines seulement quiconque se rend coupable de falsification informatique.

Est puni d'un emprisonnement de cinq ans à dix ans et d'une amende de 5.000.000 à 10.000.000 de francs comoriens ou de l'une de ces peines seulement quiconque cherchant à se procurer, pour lui-même ou pour autrui, avec une intention frauduleuse, un avantage économique illégal en introduisant dans un système d'information, en modifiant ou effaçant des données qui sont stockées, traitées ou transmises par un système d'information, ou en modifiant par tout moyen technologique l'utilisation normale des données dans un système d'information,

UNION DES COMORES
LE PRESIDENT

Est puni d'un emprisonnement de cinq ans à dix ans et d'une amende de 10.000.00 à 20.000.000 de francs comoriens ou de l'une de ces peines seulement, comme s'il était l'auteur de la falsification informatique quiconque en connaissance de cause, décide de faire usage de données falsifiées, au sens du présent article, sans en être l'auteur,

La peine d'emprisonnement et l'amende sont applicables même si les conséquences de la falsification visées aux alinéas précédents sont temporaires ou permanentes.

Article 82 : La tromperie est tout fait qui consiste à produire ou fabriquer un ensemble de données par la modification, l'altération ou la suppression frauduleuse de données informatiques, engendrant des données contrefaites, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient originales.

Est puni de cinq à dix ans d'emprisonnement et de 4.000.000 à 6.000.000 de francs comoriens d'amende, quiconque se rend coupable de tromperie.

Article 83 :L'escroquerie est tout fait qui consiste à utiliser frauduleusement un ou des éléments d'identification d'une personne physique ou morale par le biais d'un système d'information.

Est puni de deux à cinq ans d'emprisonnement et de 5.00.000 à 1.000.000 de francs comoriens d'amende, quiconque se rend coupable d'escroquerie.

Est puni de deux à cinq ans d'emprisonnement et de 5.00.000 à 1.000.000 de francs comoriens d'amende, quiconque utilise, possède, offre, vend, met à disposition, transmet en toute connaissance de cause de fausses données d'identification

Est puni de deux à cinq ans d'emprisonnement et de 5.00.000 à 1.000.000 de francs comoriens d'amende quiconque réalise ou tente de réaliser de fausses données d'identification.

Article 84 : Est puni d'une peine d'emprisonnement d'un à cinq ans et d'une amende de 1.000.000 à 10 000 000 de francs comoriens, quiconque ne respecte pas l'interdiction d'exercer la profession de prestataire de cryptologie ou l'obligation de retrait des moyens de cryptologie conformément à la présente loi.

Article 85 : Le fait de ne pas satisfaire à l'obligation de déclaration prévue à l'article 63 de la présente loi en cas de fourniture, de transfert, d'importation ou d'exportation d'un moyen de cryptologie ou à l'obligation de communication au ministre en charge des communications électroniques prévue par ce même article est puni d'un an d'emprisonnement et d'une amende maximale de 10 000 000 de francs comoriens.

Le fait d'exporter un moyen de cryptologie ou de procéder à son transfert vers un autre Etat sans avoir préalablement obtenu l'autorisation mentionnée à l'article 63 de la présente loi ou en dehors des conditions de cette autorisation, lorsqu'une telle autorisation est exigée, est puni de deux ans d'emprisonnement et d'une amende maximale de 10 000 000 de francs comoriens.

UNION DES COMORES
UNION DES COMORES
LE PRESIDENT

Le fait de vendre ou de louer un moyen de cryptologie ayant fait l'objet d'une interdiction administrative de mise en circulation, en application de l'article 65 de la présente loi, est puni de deux ans d'emprisonnement et d'une amende maximale de 10 000 000 de francs comoriens.

Le fait de fournir des prestations de cryptologie visant à assurer des fonctions de confidentialité sans avoir satisfait à l'obligation de déclaration prévue à l'article 64 de la présente loi est puni de deux ans d'emprisonnement et d'une amende maximale de 10 000 000 de francs comoriens.

Article 86 : Est puni d'un an à deux ans d'emprisonnement et de 1.000.000 à 5.000.000 de francs comoriens d'amende, quiconque, dans l'intention de commettre l'une des infractions prévues par la présente loi, produit, vend, importe, détient, diffuse, offre, cède ou met à disposition, en connaissance de cause :

- Un équipement, un dispositif ou un programme informatique ;
- Un mot de passe, un code d'accès ou des données informatiques similaires.

Article 87 : Est puni de dix à vingt ans d'emprisonnement et de 7.000.000 à 10.000.000 de francs comoriens d'amende, quiconque participe à une association formée ou à une entente établie en vue de préparer ou de commettre une ou plusieurs des infractions prévues dans la présente loi.

Article 88 : Lorsqu'elle est faite intentionnellement et sans droit, la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission d'un vol d'information, ou l'usage d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système d'information, dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions prévues par la présente loi, est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée d'entre elles.

La possession d'un dispositif ou tout autre outil ou programme informatique, dans les mêmes conditions et buts que ceux prévus à l'alinéa précédent, permettant d'accéder à tout ou à une partie d'un système d'information, dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions prévues par la présente loi, est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée d'entre elles.

Article 89 : Les personnes condamnées pour les délits prévus au présent chapitre peuvent encourir également les peines complémentaires suivantes :

- L'interdiction, pour une durée de cinq ans, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;
- La confiscation du moyen qui a servi à commettre l'infraction ou qui était destiné à la commission de l'infraction ou du bien qui en est le produit ;
- La fermeture, pour une durée de cinq ans s'il y a lieu, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

UNION DES COMORES
LE PRESIDENT

- L'exclusion, pour une durée de cinq ans, des marchés publics ;
- L'interdiction, pour une durée de cinq ans, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;
- L'affichage ou la diffusion de la décision prononcée, aux frais du condamné.

CHAPITRE II : DES INFRACTIONS LIEES A L'UTILISATION DES DONNEES A CARACTERE PERSONNEL

Article 90 : Tout fait qui consiste à envoyer un message électronique non sollicité sur la base de la collecte de données à caractère personnel constitue un envoi de message non sollicité.

Tout message électronique non sollicité envoyé sur la base de la collecte de données à caractère personnel doit contenir un lien pouvant permettre au bénéficiaire de se désabonner.

Le non-respect de cette disposition expose le contrevenant à une amende de cinq cent mille 500 000 FC à deux millions 2 000 000 de FC.

Article 91 : Tout fait qui consiste à utiliser les éléments d'identification d'une personne physique ou morale dans le but de tromper les destinataires d'un message électronique ou les usagers d'un site internet en vue de les amener à communiquer des données à caractère personnel ou des informations confidentielles est constitutif d'un détournement des donnés .

Quiconque utilise les éléments d'identification d'une personne physique ou morale dans le but de tromper les destinataires d'un message électronique ou les usagers d'un site internet en vue de les amener à communiquer des données à caractère personnel ou des informations confidentielles est puni d'un emprisonnement de cinq (5) ans et d'une amende de dix millions (10 000 000) de FC.

Article 92: Tout fait qui consiste à utiliser des données à caractère personnel ou des informations confidentielles communiquées dans le but de détourner des fonds publics ou privés est constitutif de détournement de fonds.

Est puni d'un emprisonnement de dix (10) ans et d'une amende de vingt millions 20 000 000) de francs comoriens quiconque utilise des données à caractère personnel ou des informations confidentielles communiquées dans le but de détourner des fonds publics ou privés

Article 93 : Tout fait qui porte sur un traitement de données à caractère personnel soit sans avoir préalablement informé individuellement les personnes concernées de leur droit d'accès, de rectification ou d'opposition, de la nature des données transmises et des destinataires de celles-ci, soit malgré l'opposition de la personne concernée constitue un traitement non autorisé de données.

Est puni selon les peines prévues par la loi relative à la protection des données à caractère personnel quiconque procède à un traitement non autorisé de données. .

CHAPITRE III: ATTEINTES A LA PROPRIETE INTELLECTUELLE

Article 94 : Constitue une atteinte à la propriété intellectuelle au moyen d'un système d'information :

- Le fait, sans autorisation de l'auteur ou de ses ayants droit, de reproduire, de représenter ou de mettre à la disposition du public sur un système d'information ou un support numérique ou analogique, intégralement ou partiellement une œuvre de l'esprit protégée par le droit d'auteur ou un droit voisin ;
- Le fait, sans autorisation de l'auteur ou de ses ayants droit, de traduire ou d'adapter une œuvre de l'esprit par le biais d'un programme informatique ou de mettre cette traduction ou adaptation sur un système d'information ou un support numérique ou analogique à la disposition du public ;
- Le fait, sans autorisation de l'auteur ou de ses ayants droit, de reproduire, d'utiliser, de vendre, de dénaturer, de dénigrer une marque, une raison sociale, un nom commercial, un nom de domaine Internet ou tout autre signe distinctif appartenant à un tiers par le biais d'un système d'information ouvert au public ou par le biais d'un programme informatique ou sur un support numérique ou analogique;
- Le fait, en toute connaissance de cause, d'exploiter par reproduction ou par représentation une œuvre de l'esprit mise de façon illicite à disposition du public sur un réseau de communication électronique ;
- Le fait, en toute connaissance de cause, sans droit, de vendre ou de mettre à disposition du public par reproduction ou par représentation un bien ou un produit protégé par un brevet d'invention.

Article 95 : Ne constituent pas une atteinte à la propriété intellectuelle lorsqu'elles sont réalisées par le biais d'un système ou un programme informatique ou électronique :

- Les copies ou reproductions d'œuvres de l'esprit strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective, à l'exclusion des copies des œuvres d'art destinées à être utilisées pour des fins identiques ou similaires à celles pour lesquelles l'œuvre originale a été créée ;
- Les analyses et courtes citations, sous réserve que soient clairement indiqués le nom de l'auteur de l'œuvre et la source, justifiées par le caractère critique, polémique, pédagogique, scientifique ou d'information de l'œuvre à laquelle elles sont incorporées ;
- La parodie et la caricature de l'œuvre originale réalisée sans intention de nuire à l'image et à l'honorabilité de l'auteur de ladite œuvre ;
- Les copies ou reproductions provisoires présentant un caractère transitoire et accessoire lorsqu'elles sont une partie intégrante et essentielle d'un procédé technique et qu'elles ont pour objet de permettre la transmission ou l'utilisation licite de l'œuvre sur un système d'information ou électronique ;

- La reproduction et la représentation réalisée à des fins non lucratives par des personnes morales de droit public et par des établissements ouverts au public, tels que les bibliothèques, les services d'archives, les musées, les centres de documentation et les espaces culturels multimédias, en vue d'une consultation strictement personnelle de l'œuvre par des personnes atteintes d'une ou de plusieurs déficiences des fonctions motrices, physiques, sensorielles, mentales, cognitives ou psychiques dont le niveau d'incapacité est reconnu par un certificat médical dûment établi ;
- La reproduction d'une œuvre, effectuée à des fins de conservation ou destinée à préserver les conditions de sa consultation sur place par des bibliothèques accessibles au public, par des musées ou par des services d'archives, sous réserve que ceux-ci ne recherchent aucun avantage économique ou commercial ;
- La reproduction et la représentation d'œuvre de l'esprit réalisée à des fins exclusivement pédagogiques par les enseignants et les chercheurs dans le cadre strict de leurs enseignements ou de leurs recherches pour leurs élèves et étudiants ou pour d'autres enseignants et chercheurs directement concernés, sous réserve que cette reproduction ou représentation ne donne lieu à aucune exploitation commerciale ou lucrative.

Article 96 :L'auteur d'une œuvre de l'esprit ou ses ayants droit peuvent faire obstacle à la copie de l'œuvre en limitant le droit de copie reconnue par la présente loi, notamment, par la mise en œuvre de mesures techniques de protection lorsque la mise en œuvre du droit de copie porte atteinte à l'exploitation normale de l'œuvre ou cause un préjudice injustifié aux intérêts de l'auteur.

On entend par mesure technique de protection, toute technologie, dispositif, composant qui, dans le cadre normal de son fonctionnement, accomplit la fonction de contrôle des utilisations de l'œuvre ou de limitation des copies de l'œuvre considérée.

L'usager doit être clairement informé de l'existence des mesures techniques de protection sur l'œuvre qu'il acquiert ou utilise et sur les fonctions de ces mesures techniques, notamment si elles interdisent ou non l'usage de l'œuvre sur d'autres systèmes d'information ou d'exploitation.

Article 97 : Le titulaire d'un service d'accès à Internet ou à tout réseau de communication électronique est tenu de veiller à ce que cet accès ne soit pas utilisé à des fins manifestement illicites, notamment de reproduction ou de représentation d'œuvres de l'esprit sans l'autorisation de leurs auteurs ou leurs ayants droit.
En cas de non-respect de cette obligation, il peut être poursuivi pour complicité par fourniture de moyen.

Article 98 : Sont punies d'une peine d'emprisonnement d'un à dix ans et d'une amende de 500.000 à 10.000.000 de francs comoriens, toutes les atteintes à la propriété intellectuelle commises au moyen d'un système d'information.

UNION DES COMORES
LE PRESIDENT

CHAPITRE IV : AGISSEMENTS ILLICITES SUR LES RÉSEAUX DE COMMUNICATION ÉLECTRONIQUE

Article 99 :L'organisation des jeux d'argent sur les réseaux de communication électronique est placée sous un régime de droits exclusifs de l'Etat concédés à un nombre restreint d'opérateurs.

Article 100 : Tout jeu d'argent en ligne non organisé par l'Etat ou non concédé à un opérateur par l'Etat est illicite.

Article 101 : Est puni d'une peine d'emprisonnement d'un à cinq ans et d'une amende de 5.00.000 à 10.000.000 de francs comoriens, quiconque sans autorisation, organise des jeux d'argent illicites en ligne caractérisés par la tenue de jeux de hasard, de loterie illicite, de publicité de loterie prohibée, de prise de paris illicite sur les réseaux de communication électronique.

Article 102 : Sont interdits les transferts d'argent par cartes de paiement ou par virement ou par tout autre moyen de paiement effectué par des personnes physiques ou morales dans le cadre de jeux d'argent illicites sur les réseaux de communication électronique.
Les établissements bancaires ou financiers exerçant sur le territoire national veillent au respect de cette interdiction. Ces établissements notifient aux autorités compétentes toute violation constatée ou tentative de violation de cette interdiction.

Article 103 : Est puni d'une peine d'emprisonnement de cinq ans et d'une amende de 2.000.000 à 10.000.000 de francs comoriens, quiconque ne respecte pas l'interdiction de transfert d'argent.

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

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

Article 104 : Les juridictions nationales sont compétentes pour constater ou punir les infractions lorsque les activités de jeux d'argent illicites sont offertes à partir du territoire national ou sont accessibles aux utilisateurs des réseaux de communication électronique à partir du territoire national et qu'il existe un lien suffisant, substantiel ou significatif entre la prestation illicite offerte aux utilisateurs des réseaux de communication en ligne et le territoire national, notamment, par la langue utilisée, la monnaie employée, les produits proposés, le nom de domaine utilisé par le site proposant ladite prestation.

CHAPITRE V : RESPONSABILITÉ DES PRESTATAIRES TECHNIQUES DE SERVICES EN LIGNE

Article 105 :L'accès au service internet à partir d'un cybercafé situé sur le territoire national est soumis à l'identification préalable des usagers.

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

Article 106 : Le mineur de moins de dix ans ne peut accéder à un cybercafé qu'accompagné d'un adulte.

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

Article 107 : Les personnes dont l'activité est d'offrir un accès à des services de communication en ligne informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposent au moins un de ces moyens.

Article 108 : Est puni d'une peine d'amende de 1.00.000 à 10.000.000 de francs comoriens, quiconque ne respecte pas l'obligation d'information et de mise à disposition de moyens techniques de filtrage.

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

Article 109 : Les personnes physiques ou morales qui offrent un accès à des services de communication en ligne ou qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent voir leur responsabilité civile ou pénale engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services :

- Si elles n'avaient effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ;

- Si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible ;
- Si le retrait de ces données n'a pas été ordonné par un tribunal.

UNION DES COMORES
LE PRESIDENT

Article 110 : La connaissance des faits litigieux est présumée acquise par les personnes **mentionnées** à l'article précédent, lorsqu'il leur est notifié par la victime ou par une personne intéressée, les activités illicites ou les faits et circonstances faisant apparaître ce caractère. Pour être prise en compte la notification doit comporter les éléments suivants :

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

Article 111 : La procédure de notification des faits ou d'activités illicites prévue à l'article précédent n'a pas pour effet d'engager la responsabilité d'une des personnes concernées par les exceptions prévues à l'article 109 de la présente loi.

Article 112 : Est puni d'une peine d'emprisonnement d'un à cinq ans et d'une amende de 1.00.000 à 5.000.000 de francs comoriens, le fait, pour toute personne de présenter de mauvaise foi aux personnes mentionnées à l'article 109 de la présente loi, un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion.

Article 113 : Les personnes mentionnées à l'article 109 de la présente loi ne sont pas soumises à une obligation de surveillance des informations qu'elles transmettent ou stockent, ni à une obligation de recherche des faits ou des circonstances révélant des activités illicites.

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

Article 114 : Les fournisseurs d'accès internet sont tenus de mettre en place un dispositif facilement accessible et visible sur leur site Internet permettant à toute personne de porter à leur connaissance ce type d'activités illicites et sont tenus de rendre publics les moyens consacrés à cette lutte.

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

Tout manquement aux obligations définies ci-dessus est puni d'une peine d'emprisonnement d'un à cinq ans et d'une amende de1.00.000 à 5.000.000 de francs comoriens.

UNION DES COMORES
LE PRESIDENT

Article 115 :L'autorité judiciaire peut prescrire, à toute personne mentionnée à l'article 109 de la présente loi, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication électronique.

Tout manquement aux prescriptions judiciaires définies ci-dessus est puni d'une peine d'emprisonnement d'un an à cinq ans et d'une amende de 1.00.000 à 5.000.000 de francs comoriens.

Article 116 : Les personnes mentionnées à l'article 109 de la présente loi sont tenues de détenir et de conserver sur une période de trois ans les données informatiques de nature à permettre l'identification de quiconque a contribué à la création d'un contenu ou de l'un des contenus des services dont elles sont prestataires conformément aux dispositions légales ou réglementaires relatives à la protection des données à caractère personnel.

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

Article 117 : Les personnes mentionnées à l'article 109 de la présente loi sont aussi tenues de mettre à la disposition du public en ligne leurs propres données permettant de les identifier lorsque leurs services sont offerts à partir du territoire national ou sont accessibles à partir de ce territoire et destinés aux utilisateurs des réseaux de communication en ligne dudit territoire.

Ces données d'identification doivent comporter les éléments suivants :

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

Toutefois, les personnes éditant à titre non professionnel un service de communication électronique peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination sociale et l'adresse de la personne mentionnée à l'article 110 de la présente loi sous réserve d'avoir satisfait auprès de cette dernière à son obligation d'identification telle que prévue ci-dessus.

Article 118 : Est puni d'une peine d'emprisonnement de un an à cinq ans et d'une amende de 1.00.000 à 5.000.000 de francs comoriens le fait pour une personne physique ou le dirigeant de droit ou de fait d'une personne morale exerçant l'une des activités mentionnées à l'article 68 de la présente loi de ne pas satisfaire aux obligations définies par le présent chapitre.

UNION DES COMORES
LE PRESIDENT

Article 119 : 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 civile ou pénale engagée en raison de ces contenus que dans l'un des cas suivants :

- Lorsqu'elle est à l'origine de la demande de transmission litigieuse ;
- Lorsqu'elle sélectionne le destinataire de la transmission ;
- Lorsqu'elle sélectionne ou modifie les contenus faisant l'objet de la transmission.

Article 120 : Toute personne assurant dans le seul but de rendre plus efficace leur transmission ultérieure, une activité de stockage automatique, intermédiaire et temporaire des contenus qu'un prestataire transmet ne peut voir sa responsabilité civile ou pénale engagée à raison de ces contenus que si :

- Elle a modifié ces contenus et ne s'est pas conformée à leurs conditions d'accès et aux règles usuelles concernant leur mise à jour ou a entravé l'utilisation licite et usuelle de la technologie utilisée pour obtenir des données ;
- Elle n'a pas agi avec promptitude pour retirer les contenus qu'elle a stockés ou pour en rendre l'accès impossible, dès qu'elle a effectivement eu connaissance soit du fait que les contenus transmis initialement ont été retirés du réseau, soit du fait que l'accès aux contenus transmis initialement a été rendu impossible, soit du fait que les autorités judiciaires ont ordonné de retirer du réseau les contenus transmis initialement ou d'en rendre l'accès impossible.

CHAPITRE VI : ADAPTATION DES INFRACTIONS CLASSIQUES AUXTECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Article 121 : Est puni de dix à vingt ans d'emprisonnement et de 5.00.000 à 10.000.000 de francs comoriens d'amende, le fait pour toute personne de créer, de diffuser ou de mettre à disposition sous quelque forme, que ce soient des écrits, messages, photos, sons, vidéos, dessins ou toute autre représentation d'idées ou de théories, de nature raciste, séparatiste ou xénophobe, par le biais d'un système d'information.

Article 122 : Est puni de deux à cinq ans d'emprisonnement et de 5.00.000 à 20.000.000 de francs comoriens d'amende, le fait pour toute personne de menacer autrui de mort ou de violence par le biais d'un système d'information.

Lorsque la menace a un caractère raciste, xénophobe, ethnique, religieux, séparatiste ou fait référence à un groupe qui se caractérise par la race, la couleur, l'ascendance, l'insularité ou l'origine nationale ou ethnique, la peine d'emprisonnement est de dix à vingt ans et l'amende est de 2.000.000à 40.000.000 de francs comoriens.

Article 123 : Est constitutif d'un acte de complicité des atteintes volontaires à l'intégrité de la personne, le fait d'enregistrer sciemment, par quelque moyen que ce soit, sur tout support que ce soit, des images relatives à la commission d'infractions.

Le fait de diffuser l'enregistrement de telles images est puni de cinq à dix ans d'emprisonnement et de 5.000.000 à 10.000.000 de francs comoriens d'amende.

Le présent article n'est pas applicable lorsque l'enregistrement ou la diffusion résulte de l'exercice normal d'une profession ayant pour objet d'informer le public ou est réalisé afin de servir de preuve en justice.

Article 124 : Est puni d'un à cinq ans d'emprisonnement et de 5.00.000 à10.000.000 de francs comoriens d'amende, le fait pour toute personne de proférer ou d'émettre toute expression outrageante, tout terme de mépris ou toute invective qui ne renferme l'imputation d'aucun fait, par le biais d'un système d'information.

Article 125 : Est puni de trois à cinq ans d'emprisonnement et de 75.000.000 à 100.000.000 de francs comoriens d'amende, le fait pour toute personne de nier, d'approuver ou de justifier, intentionnellement, des actes constitutifs , de génocide ou de crimes contre l'humanité par le biais d'un système d'information.

Article 126 : Est puni d'un mois à cinq ans d'emprisonnement et de 1.000.000 à 20.000.000 de francs comoriens d'amende, le fait pour une personne de produire, de mettre à la disposition d'autrui ou de diffuser des données de nature à troubler l'ordre public ou à porter atteinte à la dignité humaine par le biais d'un système d'information.

Article 127 : Le fait de diffuser ou de mettre à la disposition d'autrui, au moyen d'un ou sur un réseau de communication électronique ou un système d'information, sauf à destination des professionnels, un mode d'emploi ou des procédés permettant la fabrication d'engins de destruction de nature à porter atteinte à la vie, aux biens ou à l'environnement, élaborés à partir de poudre ou de substances explosives, de matières nucléaires, biologiques ou chimiques, ou à partir de tout autre produit destiné à l'usage domestique, industriel ou agricole est puni de un à cinq ans d'emprisonnement et de 5.000.000 à 20.000.000 de francs comoriens d'amende.

Lorsque ces procédés ont permis la commission de meurtre ou d'assassinat, la peine est de vingt ans d'emprisonnement et d'une amende de 20 000 000 à 50 000 000 de francs comoriens.

Article 128 : Est puni de un à cinq ans d'emprisonnement et de 5.000.000 à 20.000.000 de francs comoriens d'amende, le fait pour toute personne de diffuser ou de mettre à disposition d'autrui, par le biais d'un système d'information, des procédés ou des informations d'incitation au suicide.

Article 129 : Est puni de six mois à deux ans d'emprisonnement et de 1.000.000 à 5.000.000 de francs comoriens d'amende, le fait pour toute personne de communiquer ou de divulguer par le biais d'un système d'information, une fausse information tendant à faire croire qu'une destruction, une dégradation ou une détérioration de biens ou une atteinte aux personnes a été commise ou va être commise.

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

UNION DES COMORES
LE PRESIDENT

Article 130 : Est puni de cinq à dix ans d'emprisonnement et de 5.000.000 à 20.000.000 de francs comoriens d'amende, le fait pour toute personne de menacer de commettre par le biais d'un système d'information, une destruction, une dégradation ou une détérioration de biens ou une atteinte aux personnes, lorsqu'elle est matérialisée par un écrit, une image, un son, une vidéo ou toute autre donnée.

Article 131: Est coupable de trahison et puni de l'emprisonnement à vie, le fait pour un Comorien :

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

Article 132 : Est coupable d'espionnage et puni de l'emprisonnement à vie, le fait pour un étranger :

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

Article 133 : Toute personne morale, à l'exception de l'Etat, est pénalement responsable des infractions prévues par la présente loi, lorsqu'elles sont commises pour son compte par ses représentants.

La responsabilité des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits.
La peine encourue par les personnes morales responsables est le double de l'amende prévue pour la personne physique ayant commis l'infraction.

Article 134 : En cas de condamnation au titre de la présente loi, outre la publication de la condamnation ordonnée et exécutée, conformément à l'**article 75 du Code pénal**, le juge peut prononcer, à titre complémentaire, la confiscation spéciale, la privation de droits et l'interdiction de séjour prévus respectivement aux articles 63, 66 et 80 du Code pénal.

UNION DES COMORES
LE PRESIDENT

CHAPITRE VII : PROCEDURE PENALE EN MATIERE DE CYBERCRIMINALITE

Article 135 : Les officiers de police judiciaire définis à l'article 16 du nouveau Code pénale, les experts agréés auprès des tribunaux et toute autre personne dont les compétences sont requises, serment préalablement prêté, peuvent procéder aux opérations prévues par la présente loi.

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

Article 136 : Les données relatives aux abonnés doivent être conservées par les fournisseurs de services. Cette obligation impose aux fournisseurs de services de conserver et de protéger l'intégrité desdites données pendant une durée de dix ans.

Lorsqu'il est impossible de retrouver l'auteur d'une communication électronique pour défaut de conservation des données relatives aux abonnés, le fournisseur des services encourt une peine d'amende de 10.000.000 à 50.000.000 de francs comoriens.

Article 137 : Lorsque dans le cadre d'une enquête ou d'une instruction, il y a des raisons de penser que des données informatiques spécifiées, y compris des données relatives aux abonnés et au trafic, stockées au moyen d'un système d'information, sont susceptibles de perte ou de modification, l'autorité compétente procède ou fait procéder à la conservation immédiate desdites données.

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

Article 138 :L'autorité compétente, sur réquisition du procureur ou ordonnance du juge d'instruction, peut requérir :

- De toute personne physique ou morale, l'obligation de communiquer des données spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système d'information ou un support de stockage informatique;
- d'un fournisseur des services, de communiquer les données spécifiées relatives au trafic et aux abonnés en sa possession ou sous son contrôle.

Article 139 :L'autorité compétente peut, au cours d'une perquisition effectuée dans les conditions prévues par le code de procédure pénale, accéder à un système d'information ou à un support de stockage numérique et à des données intéressant l'enquête en cours et stockées dans ledit système ou ledit support se trouvant sur les lieux de la perquisition.

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

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

UNION DES COMORES
LE PRESIDENT

Article 140 :L'autorité compétente peut, dans les conditions prévues par le Code de procédure pénale, procéder à la saisie des systèmes informatiques, des supports de stockage informatique ou procéder à la copie des données informatiques nécessaires à la manifestation de la vérité.

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

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

Article 141 :L'autorité compétente, sur réquisition du procureur ou ordonnance du juge d'instruction, est habilitée :

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

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

Article 142 : Est puni d'une peine d'emprisonnement de trois à six mois et de1.000.000 à 5.000.000 de francs comoriens d'amende, quiconque refuse de déférer à la demande du procureur ou du juge d'instruction.

Lorsqu'il s'agit d'une personne morale, elle encourt une peine d'amende de 10.000.000 à 100.000.000 de francs comoriens.

Article 143 : Lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données informatisées sur le territoire comorien, sont utiles à la manifestation de la vérité, le juge d'instruction 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 autre système informatique situé en dehors du territoire national, elles sont recueillies par le juge d'instruction sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur.

UNION DES COMORES
LE PRESIDENT

Article 144 : Lorsque le juge d'instruction découvre dans un système informatique des données stockées qui sont utiles pour la manifestation de la vérité, mais que la saisie du support ne paraît pas souhaitable, ces données, de même que celles qui sont nécessaires pour les comprendre, sont copiées sur des supports de stockage informatique pouvant être saisis et placés sous scellés.

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

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

Le juge d'instruction 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 145 : Si les nécessités de l'information l'exigent, le juge d'instruction peut utiliser les moyens techniques appropriés pour collecter ou enregistrer en temps réel, les données relatives au contenu de 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, en application de moyens techniques existant, ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer lesdites données informatisées. Le fournisseur d'accès est tenu de garder le secret.

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

Article 146 : L'officier de police judiciaire peut, pour les nécessités de l'enquête ou de l'exécution d'une délégation judiciaire, procéder aux opérations prévues par la présente loi.

Article 147 : L'écrit électronique en matière pénale est admis comme mode de preuve au même titre que l'écrit sur support papier.

UNION DES COMORES
UNION DES COMORES
LE PRESIDENT

Article 148 : Dans les cas prévus par la présente loi, l'effacement de tout ou partie des données à caractère personnel faisant l'objet du traitement ayant donné lieu à l'infraction peut être ordonné. Les membres et les agents de la CNIL sont habilités à constater l'effacement de ces données.

Article 149 : Le procureur de la République avise le président de la CNIL de toutes les poursuites relatives aux infractions aux présentes dispositions et, le cas échéant, des suites qui leur sont données. Il l'informe de la date et de l'audience de jugement.

La juridiction d'instruction ou de jugement peut appeler le président de la CNIL ou son représentant à déposer ses observations ou à les développer oralement à l'audience.

Le juge compétent peut à tout moment, d'office ou sur la demande de l'intéressé, ordonner mainlevée de la saisie.

TITRE III : DISPOSITIONS FINALES

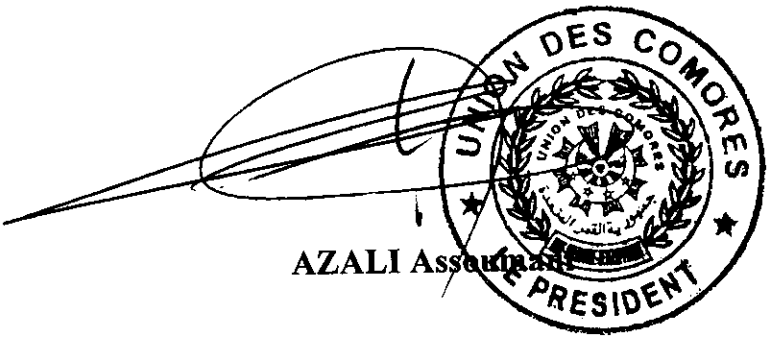
Article 150 : Les dispositions de la loi N°20-038/AU portant Code pénal, notamment celles qui régissent la lutte contre la cybercriminalité (articles 449 à 505) et celles du Code de procédure pénale, s'appliquent aux infractions en lien avec la présente loi, dans la mesure où elles ne sont pas contraires à ses dispositions.

Article 151 : Les modalités d'application de la présente loi seront précisées par décret.

Article 152 : La présente loi sera exécutée comme loi de l'Union des Comores.»

.

ARTICLE 2 : Le présent décret sera enregistré, publié au Journal Officiel de l'Union des Comores et communiqué partout où besoin sera.



AZALI Assoumani