Gabon

Cybersécurité et cybercriminalité

Ordonnance n°15/PR/2018 du 23 février 2018

[*NB - Ordonnance n°00000015/PR/2018 du 23 février 2018 portant réglementation de la cybersécurité et de la lutte contre la cybercriminalité en République Gabonaise*]

Art.1.- La présente ordonnance, prise en application des dispositions de l'article 47 de la Constitution, porte réglementation de la cybersécurité et de la lutte contre la cybercriminalité en République Gabonaise.

Titre 1 - Des dispositions générales

Chapitre 1 - De l'objet et du champ d'application

Art.2.- La présente ordonnance vise la protection et la sécurité des réseaux de communications électroniques, des systèmes d'information, des transactions électroniques, de la vie privée et des mineurs dans le cyberespace.

A ce titre, elle vise notamment à :
- définir et à réprimer toute infraction commise sur le cyberespace ;
- lutter contre la fraude téléphonique ;
- fixer le tarif des télécommunications internationales ;
- 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 infrastructures essentielles de l'information ;
- promouvoir l'utilisation des technologies de sécurité de l'information en tant que moyens de protection des droits de propriété intellectuelle ;
- assurer l'équilibre entre les intérêts du secteur public et ceux du secteur privé.

Art.3.- Sont exclues du champ d'application de la présente ordonnance, les applications spécifiques utilisées en matière de défense nationale et de sécurité publique.

Art.4.- La présente ordonnance s'applique lorsque l'infraction est commise :
- sur le territoire de la République Gabonaise par un citoyen gabonais ;
- sur le territoire de la République Gabonaise par un étranger ou un apatride, contre des étrangers, des intérêts nationaux ou étrangers, et dont l'extradition n'a pas été demandée par l'autorité étrangère compétente, avant qu'un jugement définitif ne soit rendu à son encontre, par la juridiction compétente ;
- à bord d'un navire battant pavillon gabonais ou un aéronef y immatriculé ;
- à l'étranger par un gabonais ou par un étranger ayant sa résidence habituelle au Gabon.

Chapitre 2 - Des définitions

Art.5.- Au sens de la présente ordonnance, on entend par :
- accès dérobé : mécanisme permettant de dissimuler un accès à des données ou à un système informatique sans l'autorisation de l'utilisateur légitime ;
- accès illicite : accès intentionnel, sans en avoir le droit, à l'ensemble ou à une partie d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal ;
- activité de cryptologie : toute activité ayant pour but la production, l'utilisation, l'importation, l'exportation ou la commercialisation des moyens de cryptologie ;
- administration chargée des communications électroniques : ministère ou Ministre, selon les cas, investi pour le compte du Gouvernement d'une compétence générale sur le secteur des communications électroniques et des technologies de l'information et de la communication ;
- agrément : consiste à la reconnaissance formelle que le produit ou le système évalué peut protéger jusqu'à un niveau spécifié par un organisme agréé ;
- algorithme : suite d'opérations mathématiques élémentaires à appliquer à des données pour aboutir à un résultat désiré ;
- algorithme cryptologique : procédé permettant, avec l'aide d'une clé, de chiffrer et de déchiffrer des messages ou des documents ;
- algorithme asymétrique : algorithme de chiffrement utilisant une clé publique pour chiffrer et une clé privée différente de cette dernière pour déchiffrer les messages ;
- algorithme symétrique : algorithme de déchiffrement utilisant une même clé pour chiffrer et déchiffrer les messages ;
- attaque active : acte modifiant ou altérant les ressources ciblées par l'attaque tel que l'atteinte à l'intégrité, à la disponibilité et à la confidentialité des données ;
- attaque passive : acte n'altérant pas sa cible tel que l'écoute passive, l'atteinte à la confidentialité ;
- atteinte à l'intégrité : fait de provoquer intentionnellement une perturbation grave ou une interruption de fonctionnement d'un système d'information, d'un réseau de communications électroniques ou d'un équipement terminal, en introduisant,

transmettant, endommageant, effaçant, détériorant, modifiant, supprimant ou rendant inaccessibles les données ;

- audit de sécurité : examen méthodique des composantes et des acteurs de la sécurité, de la politique, des mesures, des solutions, des procédures et des moyens mis en œuvre par une organisation, pour sécuriser son environnement ;
- authentification : critère de sécurité défini par un processus mis en œuvre notamment pour vérifier l'identité d'une personne physique ou morale et s'assurer que l'identité fournie correspond à l'identité de cette personne préalablement enregistrée ;
- autorité compétente : autorité de régulation des communications électroniques ou opérateur public chargé des infrastructures numériques et des fréquences ;
- bi-clé : couple clé publique et clé privée utilisé dans des algorithmes de cryptographie asymétrique ;
- chiffrement : toute technique, tout procédé grâce auquel sont transformées à l'aide d'une convention secrète appelée clé, des données numériques, des informations claires en informations inintelligibles par des tiers n'ayant pas connaissance de la clé ;
- chiffrement par bloc : chiffrement opérant sur des blocs d'informations claires et sur des informations chiffrées ;
- chiffrer : action visant à assurer la confidentialité d'une information, à l'aide de Codes secrets, pour la rendre inintelligible à des tiers, en utilisant des mécanismes offerts en cryptographie ;
- clé : dans un système de chiffrement, elle correspond à une valeur mathématique, un mot, une phrase qui permet, grâce à l'algorithme de chiffrement, de chiffrer ou de déchiffrer un message ;
- clé de chiffrement : série de symboles commandant les opérations de chiffrements et de déchiffrement ;
- clé privée : clé utilisée dans les mécanismes de chiffrement asymétrique ou chiffrement à clé publique, appartenant à une entité et devant être secrète ;
- clé publique : clé servant au chiffrement d'un message dans un système asymétrique et donc librement diffusé ;
- clé sécrète : clé connue de l'émetteur et du destinataire servant de chiffrement et de déchiffrement des messages et utilisant le mécanisme de chiffrement symétrique ;
- code source : ensemble des spécifications techniques, sans restriction d'accès ni de mise en œuvre, d'un logiciel ou protocole de communication, d'interconnexion, d'échange ou d'un format de données ;
- communication électronique : émission, transmission ou réception, de signes, de signaux, d'écrits, d'images ou de sons par voie électronique ;
- confidentialité : maintien du secret des informations et des transactions afin de prévenir la divulgation non autorisée d'informations aux non destinataires permettant la lecture, l'écoute, la copie illicite d'origine intentionnelle ou accidentelle durant leur stockage, traitement ou transfert ;
- contenu : ensemble d'informations relatives aux données appartenant à des personnes physiques ou morales, transmises ou reçues à travers les réseaux de communications électroniques et les systèmes d'information ;

- contenu illicite : contenu portant atteinte à la dignité humaine, à la vie privée, à l'honneur ou à la sécurité nationale ;
- convention secrète : accord de volontés portant sur des clés non publiées nécessaires à la mise en œuvre d'un moyen ou d'une prestation de cryptologie pour les opérations de chiffrement ou de déchiffrement ;
- courrier électronique : tout message sous forme de texte, de voix, de son ou d'image envoyé par un réseau public ou privé de communication, qui peut être stocké dans le réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère ;
- cryptage : utilisation de Codes ou signaux non usuels permettant la conservation des informations à transmettre en des signaux incompréhensibles par les tiers ;
- cryptanalyse : opération qui vise à rétablir une information inimitable en information claire sans connaître la clé de chiffrement qui a été utilisée ;
- cryptogramme : message chiffré ou codé ;
- cryptographie : application des mathématiques permettant d'écrire l'information, de manière à la rendre inintelligible à ceux ne possédant pas les capacités de la déchiffrer ;
- cryptologie : science relative à la protection et à la sécurité des informations notamment pour la confidentialité, l'authentification, l'intégrité et la non répudiation des données transmises ;
- cybercriminalité : ensemble des infractions s'effectuant à travers le cyberspace par des moyens autres que ceux habituellement mis en œuvre, et de manière complémentaire à la criminalité classique ;
- cybersécurité : ensemble de mesures de prévention, de protection et de dissuasion d'ordre technique, organisationnel, juridique, financier, humain, procédural et autres actions permettant d'atteindre les objectifs de sécurité fixés à travers les réseaux de communications électroniques, les systèmes d'information et pour la protection de la vie privée des personnes ;
- cyberespace : ensemble de données numérisées constituant un univers d'informations et un milieu de communication lié à l'interconnexion mondiale d'équipements de traitement automatisé de données numériques ;
- déni de service : attaque par saturation d'une ressource du système d'information ou du réseau de communications électroniques, afin qu'il s'effondre et ne puisse plus réaliser les services attendus de lui ;
- déni de service distribué : attaque simultanée des ressources du système d'information ou du réseau de communications électroniques, afin de les saturer et amplifier les effets d'entrave ;
- disponibilité : critère de sécurité permettant que les ressources des réseaux de communications électroniques, des systèmes d'information ou des équipements terminaux soient accessibles et utilisables selon les besoins (le facteur temps) ;
- données informatiques : représentation de faits, d'informations ou de notions sous une forme susceptible d'être traitée par un équipement terminal, y compris un programme permettant à ce dernier d'exécuter une fonction ;
- données de connexion : ensemble d'informations relatives au processus d'accès dans une communication électronique ;

- données de trafic : données ayant trait à une communication électronique indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type du service réseau sous-jacent ;
- équipement terminal : tout équipement destiné à être connecté directement ou indirectement à un point de terminaison d'un réseau en vue de la transmission, du traitement ou de la réception d'informations ;
- fiabilité : aptitude d'un système d'information ou d'un réseau de communications électroniques à fonctionner sans incident pendant un temps suffisamment long ;
- fournisseur des services de communications électroniques : personne physique ou morale fournissant à titre principal des prestations de communications électroniques ;
- gateway internationale physique : plateforme de télécommunication internationale unique permettant la gestion et la régulation technique et financière de l'ensemble des télécommunications voix et données entrant et sortant du territoire national gabonais ;
- gravité de l'impact : appréciation du niveau de gravité d'un incident, pondéré par sa fréquence d'apparition ;
- infrastructure critique : installation, système ou partie de celui-ci, à la fois publics et privés, indispensables au maintien des fonctions vitales de l'Etat et de la société ;
- intégrité des données : critère de sécurité définissant l'état d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal qui est demeuré intact et permet de s'assurer que les ressources n'ont pas été altérées ;
- interception illégale : accès sans en avoir le droit ou l'autorisation, aux données d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal ;
- interception légale : accès autorisé aux données d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal ;
- intrusion par intérêt : accès intentionnel et sans droit dans un réseau de communications électroniques ou dans un système d'information, dans le but soit de nuire soit de tirer un bénéfice économique, financier, industriel, sécuritaire ou de souveraineté ;
- intrusion par défi intellectuel : accès intentionnel, sans en avoir le droit ou l'autorisation, dans un réseau de communications électroniques ou dans un système d'information, dans le but de relever un défi intellectuel pouvant contribuer à l'amélioration des performances du système de sécurité de l'organisation ;
- logiciel trompeur : logiciel effectuant des opérations sur un équipement terminal d'un utilisateur sans informer préalablement cet utilisateur de la nature exacte des opérations que ce logiciel va effectuer sur son équipement terminal ou sans demander à l'utilisateur s'il consent à ce que le logiciel procède à ces opérations ;
- logiciel espion : type particulier de logiciel trompeur collectant les informations personnelles auprès d'un utilisateur du réseau de communications électroniques ;
- logiciel potentiellement indésirable : logiciel représentant des caractéristiques d'un logiciel trompeur ou d'un logiciel espion ;
- matériel raciste et xénophobe : tout support numérique qui préconise ou encourage la haine, la discrimination ou la violence, contre une personne ou un groupe de

personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion ;
- moyens de cryptologie : ensemble d'outils scientifiques et techniques permettant de chiffrer ou de déchiffrer ;
- non répudiation : critère de sécurité assurant la disponibilité de preuves qui peuvent être opposées à un tiers et utilisées pour démonter la traçabilité d'une communication électronique qui a eu lieu ;
- opérateur : toute personne morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques ;
- politique de sécurité : référentiel de sécurité établi par une organisation, reflétant sa stratégie de sécurité et spécifiant les moyens de la réaliser ;
- pornographie enfantine : toute donnée quelle qu'en soit la nature ou la forme ou le support représentant :
- un mineur se livrant à un comportement sexuellement explicite ;
- des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite ;
- prestation de cryptographie : opération visant à la mise en œuvre, pour le compte d'autrui ou de soi, de moyens de cryptographie ;
- prestataire de services de cryptologie : toute personne, physique ou morale, qui fournit une prestation de cryptologie ;
- prospection directe : tout envoi de tout message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services ;
- réseau de communications électroniques : système de transmission permettant l'acheminement de signaux par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques ;
- sécurité : situation dans laquelle quelqu'un, quelque chose n'est exposé à aucun danger. Mécanisme destiné à prévenir un événement dommageable, ou à limiter les effets ;
- système de détection : système permettant de détecter les incidents qui pourraient conduire aux violations de la politique de sécurité et permettant de diagnostiquer des intrusions potentielles ;
- système d'information : ensemble organisé de ressources permettant de collecter, regrouper, classifier, traiter et diffuser l'information ;
- système informatique : tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure un traitement automatisé de données ;
- vulnérabilité : défaut de sécurité dans l'architecture d'un réseau de communications électroniques ou dans la conception d'un système d'information se traduisant par une violation de la politique de sécurité.

Art.6.- Les termes et expressions non définis dans la présente ordonnance, conservent leurs définitions ou significations données par les textes en vigueur.

Art.7.- Le cadre institutionnel de la cybersécurité comprend :

- le Ministère de l'Economie Numérique chargé d'élaborer et mettre en œuvre la politique nationale de cybersécurité en collaboration avec les autres administrations et organismes compétents ;
- le service public personnalisé chargé du contrôle et du suivi des activités liées à la sécurité des systèmes d'informations et des réseaux de communication ;
- l'organe consultatif et d'orientation de la mise en œuvre des politiques nationales en matière de cybersécurité.

Les autres attributions des organes visés à l'alinéa 1er ci-dessus sont fixées par voie réglementaire.

Titre 2 - De la cybersécurité

Chapitre 1 - De la protection des infrastructures critiques

Art.8.- Le Ministre chargé de l'Economie Numérique élabore des normes et des procédures relatives aux politiques de sécurité et plans de rétablissement, sur avis de l'organisme en charge d'alertes et de réponses aux attaques des systèmes d'informations, créés par voie réglementaire.

Toute autre compétence s'exerce selon les dispositions de la loi n°05/2001 du 27 juin 2001 portant réglementation du secteur des télécommunications, notamment en ce qui concerne l'implantation de la gateway internationale physique.

Art.9.- Chaque département ministériel identifie les infrastructures critiques, relevant de son secteur.

Cette identification fait l'objet d'un arrêté classé secret défense. Cet arrêté est notifié à l'opérateur d'infrastructure critique dans les mêmes formes.

Art.10.- L'opérateur d'infrastructure critique est tenu de prendre toutes dispositions utiles en vue d'organiser et d'assurer la sécurité de ladite infrastructure dans les conditions fixées par voie réglementaire.

Chapitre 2 - De la protection des réseaux de communications électroniques

Art.11.- Les opérateurs des réseaux de communications électroniques et les fournisseurs de services de communications électroniques doivent prendre toutes les mesures techniques et administratives nécessaires pour garantir la sécurité des services offerts et mettre en place tous les procédés et moyens techniques permettant de lutter contre la fraude téléphonique internationale.

Pour ce faire, les opérateurs devront prendre les mesures d'interconnexion à la plateforme mise en place par la gateway internationale physique décidée et convenue par l'autorité compétente en la matière.

A ce titre, ils sont notamment tenus d'informer les usagers :
- du danger encouru en cas d'utilisation de leurs réseaux ;
- des risques particuliers de violation de la sécurité ; -de l'existence de moyens techniques permettant d'assurer la sécurité de leurs communications.

Les dispositions du présent article sont complétées par voie réglementaire.

Art.12.- Les opérateurs de réseaux et les fournisseurs de services de communications électroniques ont l'obligation de :
- conserver les données de connexion et de trafic pendant une période de dix ans ;
- installer des mécanismes de surveillance de trafic des données de leurs réseaux. Ces données peuvent être accessibles lors des investigations judiciaires.

La responsabilité des opérateurs de réseaux et celles des fournisseurs de services de communications électroniques est engagée si l'utilisation des données suscitées, porte atteinte aux libertés individuelles des usagers.

Les opérateurs de réseaux de communications électroniques sont tenus de disposer d'un centre de gestion opérationnel de leurs infrastructures sur le territoire national.

Chapitre 3 - De la protection des systèmes d'informations

Art.13.- Les exploitants des systèmes d'informations prennent toutes les mesures techniques et administratives afin de garantir la sécurité des services offerts. A ce titre, ils se dotent de systèmes normalisés leur permettant d'identifier, évaluer, traiter et gérer en continu les risques liés à la sécurité des systèmes d'informations.

Ils sont également tenus de mettre en place des mécanismes techniques pour faire face aux atteintes préjudiciables à la disponibilité permanente des systèmes, à leur intégrité, à leur authentification, à leur non répudiation par des utilisateurs tiers, à la confidentialité des données et à la sécurité physique.

Les mécanismes prévus à l'alinéa 2 ci-dessus, font l'objet d'approbation et de visa conforme par l'autorité compétente.

Les systèmes d'informations font l'objet de protection contre d'éventuels rayonnements et d'intrusions qui peuvent compromettre l'intégrité des données transmises et contre toute autre attaque externe.

Art.14.- Les personnes morales dont l'activité est d'offrir un accès à des systèmes d'informations sont notamment tenues d'informer les usagers :
- du danger encouru dans l'utilisation des systèmes d'informations non sécurisés ;

- de la nécessité d'installer des dispositifs de contrôle parental ;
- des risques particuliers de violation de sécurité ;
- de l'existence de moyens techniques permettant de restreindre l'accès à certains services et de leur proposer au moins l'un de ces moyens.

Art.15.- Les exploitants des systèmes d'informations informent les utilisateurs de l'interdiction faite d'utiliser le réseau de communications électroniques pour diffuser des contenus illicites ou tout autre acte qui peut entamer la sécurité des réseaux ou des systèmes d'informations.

L'interdiction porte également sur la conception de logiciel trompeur, espion, potentiellement indésirable ou de tout autre outil conduisant à un comportement frauduleux.

Art.16.- Les exploitants des systèmes d'informations ont l'obligation de :

- conserver les données de connexion et de trafic de leurs systèmes d'informations pendant une période de dix ans ; -installer des mécanismes de surveillance de contrôle d'accès aux données de leurs systèmes d'informations pour les besoins d'investigations judiciaires.

Les installations des exploitants des systèmes d'informations peuvent faire l'objet de perquisition ou de saisie sur ordre d'une autorité judiciaire dans les conditions prévues par la présente ordonnance.

Art.17.- Les exploitants des systèmes d'informations évaluent, révisent leurs systèmes de sécurité et introduisent en cas de nécessité, les modifications appropriées dans leurs pratiques, mesures et techniques de sécurité en fonction de l'évolution des technologies.

Les exploitants des systèmes d'informations et leurs utilisateurs peuvent coopérer pour l'élaboration et la mise en œuvre des pratiques, mesures et techniques de sécurité de leurs systèmes.

Art.18.- Les réseaux de communications électroniques et les systèmes d'informations sont soumis à un régime d'audit de sécurité obligatoire et périodique de leurs systèmes de sécurité selon les modalités fixées par voie réglementaire.

Chapitre 4 - De la protection des contenus

Art.19.- Tout opérateur est tenu d'héberger une copie de ses données sur le territoire national selon les conditions et modalités fixées par voie réglementaire.

Art.20.- Les opérateurs et exploitants des réseaux de communications électroniques et des systèmes d'informations assurent la confidentialité des communications acheminées à travers les réseaux de communications électroniques et les systèmes d'informations y compris les données relatives au trafic.

Art.21.- Il est interdit à toute personne physique ou morale d'écouter, intercepter, stocker les communications et les données relatives au trafic y afférent, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés, sauf en cas d'autorisation légale.

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

Art.22.- L'enregistrement des communications et des données de trafic y afférent, effectué dans le cadre professionnel en vue de fournir la preuve numérique d'une communication électronique, est autorisé dans les conditions fixées par la présente ordonnance.

Art.23.- Les prestataires ou fournisseurs des services de communications électroniques, sont tenus d'informer leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services, de les sélectionner ou de leur proposer au moins un de ces moyens.

Art.24.- Les fournisseurs de contenus des réseaux de communications électroniques et systèmes d'informations sont tenus de :

- assurer la disponibilité des contenus, ainsi que celle des données stockées dans leurs installations selon les modalités fixées par voie réglementaire ;
- mettre en place des filtres pour faire face aux atteintes préjudiciables aux données personnelles et à la vie privée des utilisateurs ;
- conserver les contenus ainsi que les données stockées dans leurs installations pendant une durée de dix ans ; -mettre en place des filtres pour faire face aux atteintes préjudiciables aux données personnelles et à la vie privée des utilisateurs.

Art.25.- L'utilisation des réseaux de communications électroniques et des systèmes d'informations aux fins de stocker les informations ou d'accéder à des informations stockées dans un équipement terminal d'une personne physique ou morale, ne peut se faire qu'avec son consentement préalable.

Art.26.- L'émission des messages électroniques à des fins de prospection en dissimulant l'identité de l'émetteur au nom duquel la communication est faite, ou sans indiquer une adresse valide à laquelle le destinataire peut transmettre une demande visant à obtenir l'arrêt de ces informations est interdite.

L'émission des messages électroniques usurpant l'identité d'autrui est interdite.

Art.27.- Les personnels des opérateurs des réseaux de communications électroniques ou des fournisseurs de services de communications électroniques sont astreints au secret professionnel quant aux réquisitions reçues.

Chapitre 5 - De la cryptologie

Art.28.- L'utilisation, la fourniture, l'importation et l'exportation des moyens de cryptologie assurant exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont libres notamment :

- lorsque le moyen ou la prestation de cryptologie ne permet pas d'assurer des fonctions de confidentialité, notamment lorsqu'il ne peut avoir comme objet que d'authentifier une communication ou d'assurer l'intégrité du message transmis ;
- lorsque la fourniture, le transfert depuis ou vers un pays membre de la CEEAC-CEMAC, l'importation et l'exportation des moyens de cryptologie permet d'assurer exclusivement des fonctions d'authentification ou de contrôle d'intégrité ;
- lorsque le moyen ou la prestation assure des fonctions de confidentialité et n'utilise que des conventions secrètes gérées selon les procédures et par l'autorité compétente de cryptologie.

Art.29.- Les modalités d'utilisation de la taille de certaines clés sont fixées par voie réglementaire.

Art.30.- La fourniture ou l'importation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité est soumise à une déclaration préalable auprès de l'autorité compétente de cryptologie.

Le prestataire ou la personne procédant à la fourniture ou à l'importation d'un service de cryptologie tient à la disposition de l'autorité compétente de cryptologie une description des caractéristiques techniques de ce moyen de cryptologie, ainsi que le Code source des logiciels utilisés.

Les prestataires de services de cryptologie sont assujettis au secret professionnel.

Un texte réglementaire précise les modalités d'application du présent article.

Titre 3 - De la cybercriminalité

Chapitre 1 - De la procédure

Art.31.- En cas d'infraction cybernétique, les Officiers de Police Judiciaire à compétence générale et les agents habilités par l'autorité compétente, procèdent aux enquêtes conformément aux dispositions des textes en vigueur.

Avant leur entrée en fonction, les agents habilités par l'autorité compétente prêtent serment, devant le Tribunal de Première Instance compétent.

Il peuvent, lors des investigations, accéder aux moyens de transport, à tout local à usage professionnel, à l'exclusion des domiciles privés, en vue de rechercher, de constater les

infractions, de demander la communication de tous les documents professionnels et en prendre copie, recueillir, sur convocation ou sur place, les renseignements et justificatifs.

Art.32.- Les perquisitions en matière de cybercriminalité sont susceptibles de porter sur les objets, documents et données qui peuvent être des supports physiques ou des copies réalisées en présence des personnes qui assistent à la perquisition.

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

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

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

Art.33.- Les perquisitions et les saisies sont effectuées conformément aux dispositions des textes en vigueur.

Art.34.- Lorsqu'il apparaît que les données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait l'objet d'opérations de transformation empêchant d'accéder en clair ou sont de nature à compromettre les informations qu'elles contiennent, le Procureur de la République, le Juge d'Instruction ou la juridiction de jugement peuvent réquisitionner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair desdites données.

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

Art.35.- La réquisition prévue à l'article 33 ci-dessus peut être faite à tout expert. Dans ce cas, son exécution est faite conformément aux dispositions du Code de Procédure Pénale relatives à la commission d'expert.

Art.36.- Les autorités judiciaires peuvent donner commission rogatoire tant nationale qu'internationale, à toute personne morale ou physique pour rechercher les éléments constitutifs des infractions de cyber criminalité, dont au moins l'un des éléments constitutifs a été commis sur le territoire national ou dont l'un des auteurs ou complices se trouve dans ledit territoire.

Sous réserve des règles de réciprocité entre le Gabon et les pays étrangers liés par un accord de coopération judiciaire, les commissions rogatoires sont exécutées conformément aux dispositions des textes en vigueur.

Art.37.- Les personnes physiques ou morales qui fournissent des prestations de cryptographie visant à assurer une fonction de confidentialité, sont tenues de remettre aux Officiers de Police Judiciaire ou aux agents habilités, sur leur demande, les

conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies.

Les Officiers de Police Judiciaire et agents habilités peuvent demander aux fournisseurs des prestations visés à l'alinéa 1er ci-dessus de mettre eux-mêmes en œuvre ces conventions.

Art.38.- Lorsque les nécessités de l'enquête ou de l'instruction le justifient, l'audition ou l'interrogatoire d'une personne ou la confrontation entre plusieurs personnes, peuvent être effectuées en plusieurs points du territoire national se trouvant reliés par des moyens de communications électroniques garantissant la confidentialité de la transmission.

Dans chacun des lieux un Procès-verbal des opérations effectuées est dressé, celles-ci peuvent faire l'objet d'enregistrement audiovisuel ou sonore.

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

Les modalités d'application du présent article sont définies par voie réglementaire.

Chapitre 2 - Des infractions et des sanctions

Art.39.- Quiconque accède frauduleusement à tout ou partie d'un système informatique, y compris par tout moyen favorisant ou organisant la fraude téléphonique internationale, sera puni d'un emprisonnement de deux à dix ans et d'une amende de vingt à cent millions de francs CFA ou de l'une de ces deux peines seulement.

L'accès frauduleux visé à l'alinéa 1er ci-dessus comprend également le dépassement d'un accès autorisé.

Art.40.- Quiconque se maintient frauduleusement dans tout ou partie d'un système informatique sera puni d'un emprisonnement de deux à cinq ans et d'une amende de vingt à cinquante millions de francs CFA ou de l'une de ces deux peines seulement.

Art.41.- Quiconque entrave, par quelque moyen que ce soit, le fonctionnement d'un système informatique sera puni d'un emprisonnement de deux à cinq ans et d'une amende de vingt à cinquante millions de francs CFA ou de l'une de ces deux peines seulement.

Art.42.- Quiconque introduit frauduleusement des données informatiques dans un système informatique sera puni d'un emprisonnement de cinq à dix ans et d'une amende de cinquante à cent millions de francs CFA ou de l'une de ces deux peines seulement.

Art.43.- Quiconque intercepte frauduleusement par des moyens techniques des données informatiques lors de leur transmission non publique à destination, en provenance ou à

l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques, sera puni d'un emprisonnement de cinq à dix ans et d'une amende de cinquante à cent millions de francs CFA ou de l'une de ces deux peines seulement.

Art.44.- Quiconque endommage, supprime, extrait frauduleusement des données informatiques sera puni d'un emprisonnement de cinq à dix ans et d'une amende de cinquante à cent millions de francs CFA ou de l'une de ces deux peines seulement.

Art.45.- Quiconque fait intentionnellement, usage des données obtenues dans les conditions énoncées par les dispositions des articles ci-dessus sera puni d'un emprisonnement de cinq à dix ans et d'une amende de cinquante à cent millions de francs CFA ou de l'une de ces deux peines seulement.

Art.46.- Quiconque importe, détient, offre, cède, vend ou met à disposition, sous quelque forme que ce soit, un programme informatique, un mot de passe, un Code d'accès ou toutes données informatiques similaires conçues ou spécialement adaptées, pour permettre d'accéder, à un réseau de communications électroniques ou un système d'information sera puni d'un emprisonnement de cinq à dix ans et d'une amende de cinquante à cent millions de francs CFA ou de l'une de ces deux peines seulement.

Sera également puni des peines prévues à l'alinéa 1er ci-dessus, quiconque intentionnellement provoque une perturbation grave, notamment par fraude, ou une interruption d'un réseau de communications électroniques ou d'un système d'information.

Art.47.- Quiconque introduit, altère, supprime frauduleusement des données informatiques authentiques, sera puni d'un emprisonnement de deux à cinq ans et d'une amende de vingt à cinquante millions de francs CFA ou de l'une de ces deux peines seulement.

Art.48.- Tout prestataire de services de cryptologie qui ne satisfait pas à l'obligation de communiquer la description des caractéristiques techniques du moyen de cryptologie dans les conditions prévues par la présente ordonnance, est puni d'un emprisonnement de trois mois à deux ans et d'une amende de cinq cent mille à deux millions de francs CFA ou de l'une de ces deux peines seulement.

Art.49.- Quiconque fournit ou importe un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sans satisfaire à l'obligation de déclaration préalable, est punie d'un emprisonnement de six mois à cinq ans et d'une amende de un à cinq millions de francs CFA ou de l'une de ces deux peines seulement, sans préjudice des dispositions fiscales en vigueur.

Art.50.- Quiconque exporte un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sans avoir obtenu préalablement l'autorisation, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de un à cinq millions de francs CFA ou de l'une de ces deux peines seulement, sans préjudice des dispositions fiscales en vigueur.

Art.51.- Quiconque fournit des prestations de cryptologie sans avoir obtenu préalablement l'agrément de la Commission Nationale de Cryptologie prévu à l'article 30 de la présente ordonnance, est puni d'un emprisonnement d'un an à cinq ans et d'une amende d'un million à vingt millions de francs CFA ou de l'une de ces deux peines seulement.

Art.52.- Quiconque met à la disposition d'autrui un moyen de cryptologie ayant fait l'objet d'une interdiction d'utilisation et de mise en circulation, est puni d'un emprisonnement d'un an à cinq ans et d'une amende d'un million à vingt millions de francs CFA ou de l'une de ces deux peines seulement.

Art.53.- Quiconque fait obstacle à l'exercice de la mission de contrôle de la Commission Nationale de Cryptologie est puni d'un emprisonnement d'un à trois mois et d'une amende de cent à cinq cent mille francs CFA ou de l'une de ces deux peines seulement.

Art.54.- Quiconque met en place un accès dérobé à des données ou à un système d'information sans l'autorisation de l'utilisateur légitime, est puni d'un emprisonnement de deux à cinq ans et d'une amende de deux à trente millions de francs CFA ou de l'une de ces deux peines seulement.

Art.55.- Quiconque produit, enregistre, met à disposition, transmet, importe ou exporte de la pornographie enfantine par le biais d'un système informatique sera puni d'un emprisonnement de cinq à dix ans et d'une amende de cinquante à cent millions de francs CFA ou de l'une de ces deux peines seulement.

Art.56.- Quiconque se procure de la pornographie enfantine par le biais d'un système informatique, sera puni d'un emprisonnement de deux à cinq ans et d'une amende de cinq à vingt millions de francs CFA ou de l'une de ces deux peines seulement.

Art.57.- Quiconque détient de la pornographie enfantine dans un système informatique, sera puni d'un emprisonnement de deux à cinq ans et d'une amende de cinq à vingt millions de francs CFA ou de l'une de ces deux peines seulement.

Art.58.- Quiconque facilite l'accès ou diffuse à des mineurs des images, des documents, du son ou une représentation à caractère pornographique, sera puni d'un emprisonnement de cinq à dix ans et d'une amende de cinq à dix millions de francs CFA ou de l'une de ces deux peines seulement.

Art.59.- Quiconque propose, par voie électronique, une rencontre à un enfant mineur, dans le but de commettre à son encontre une des infractions prévues par les articles 55 à 58 ci-dessus, sera puni d'un emprisonnement de deux ans et d'une amende de vingt millions de francs CFA ou de l'une de ces deux peines seulement.

Art.60.- Quiconque propose ou met à disposition par voie électronique tout produit ou substance illicite, sera puni d'un emprisonnement de deux à cinq ans et d'une amende de cinq à dix millions de francs CFA ou de l'une de ces deux peines seulement.

Art.61.- Quiconque crée, télécharge, diffuse ou met à disposition sous quelque forme que ce soit, par voie électronique des contenus racistes ou xénophobes, sera puni d'un emprisonnement de trois mois à dix ans et d'une amende de un à dix millions de francs CFA ou de l'une de ces deux peines seulement.

Art.62.- Quiconque profère une menace ou une insulte par voie électronique, envers une personne en raison de son appartenance à un groupe, une race, une couleur, une ascendance, une religion ou une origine, sera puni d'un emprisonnement de trois mois à dix ans et d'une amende de dix à trente millions de francs CFA ou de l'une de ces deux peines seulement.

Art.63.- Quiconque diffuse ou met à disposition par voie électronique des données qui nient, minimisent de manière grossière, approuvent ou justifient des actes constitutifs de génocide ou de crimes contre l'humanité tels que définis par le droit international, sera puni d'un emprisonnement de cinq à dix ans et d'une amende de dix à trente millions de francs CFA ou de l'une de ces deux peines seulement.

Art.64.- Sera puni d'un emprisonnement de trois à cinq ans et d'une amende de cinq à dix millions de francs CFA ou de l'une de ces deux peines seulement, quiconque aura volontairement :

- utilisé un système informatique protégé pour relayer ou retransmettre des courriers électroniques multiples dans l'intention de tromper ou d'induire en erreur, quant à l'origine de ces messages les destinataires ou tout prestataire de services de courriers électroniques ou de services internet ;
- falsifié matériellement les informations se trouvant dans les en-têtes de messages électroniques multiples et déclenche leur transmission ;
- déclenché la transmission de courriers électroniques multiples à partir ou par l'intermédiaire d'un système informatique.

Art.65.- Quiconque usurpe l'identité numérique d'un tiers ou une ou plusieurs données permettant de l'identifier, dans l'intention de nuire à autrui, sera puni d'un emprisonnement de un à cinq ans et d'une amende de cinq à dix millions de francs CFA ou de l'une de ces deux peines seulement.

Art.66.- Toute atteinte aux biens, aux personnes, aux droits d'autrui commise par voie électronique est punie des peines prévues par le Code Pénal.

Art.67.- L'escroquerie, l'abus de confiance, le recel, le chantage, l'extorsion de fonds et le vol commis par voie électronique sont punis des peines prévues par le Code Pénal.

Art.68.- Toute tentative qui aura été manifestée par un commencement d'exécution, si elle n'a pas été suspendue ou si elle n'a manqué son effet que par des circonstances indépendantes de la volonté de son auteur est considéré comme l'infraction elle-même.

Art.69.- Le complice d'une des infractions prévues par la présente ordonnance sera puni comme l'auteur.

Art.70.- Pour toute récidive aux infractions prévues par la présente ordonnance, les peines sont portées au double.

Art.71.- Les infractions aux dispositions de la présente ordonnance, lorsqu'elles sont commises en bande organisée sont punies de la réclusion criminelle à temps.

Art.72.- Les auteurs d'atteintes aux dispositions de la présente ordonnance sont passibles des peines complémentaires suivantes :

- la dissolution, lorsque la personne morale s'est détournée de son objet pour commettre les faits incriminés ;
- l'interdiction provisoire ou définitive d'exercer ;
- la fermeture provisoire ou définitive d'un ou de plusieurs des établissements de l'entreprise ;
- l'exclusion provisoire ou définitive de soumissionner ; -l'interdiction provisoire ou définitive de faire appel public à l'épargne ;
- l'interdiction pour une durée de cinq ans au plus d'émettre des chèques à des tiers ;
- la confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit ;
- l'affichage ou la diffusion de la décision prononcée aux frais de l'auteur des faits.

Titre 4 - De la coopération judiciaire internationale

Art.73.- L'autorité compétente peut, sous réserve de réciprocité, fournir sur demande d'une autorité compétente étrangère, l'entraide judiciaire en vue de la recherche et la constatation des infractions pénales prévues par la présente ordonnance.

L'entraide judiciaire concerne les mesures de perquisition, de saisie ou de conservation du système d'information ou de données.

Art.74.- La demande d'entraide formulée doit notamment préciser :

- l'autorité compétente requérante ;
- l'infraction faisant l'objet de l'enquête ou des poursuites, ainsi qu'un exposé des faits ;
- le système d'information ou les données informatiques faisant l'objet de la demande de perquisition, de saisie ou de conservation et leur relation avec l'infraction ;
- toutes les informations disponibles pour identifier la personne visée ;
- la nécessité des mesures de perquisition, de saisie ou de conservation du système d'information ou de données concernés.

Art.75.- Les demandes d'entraide émanant des autorités judiciaires gabonaises et destinées aux autorités judiciaires étrangères sont transmises par l'intermédiaire du Ministère en charge des Affaires Etrangères.

Les pièces d'exécution sont renvoyées aux autorités de l'Etat requérant par la même voie.

Art.76.- Les demandes d'entraide émanant des autorités judiciaires étrangères sont transmises au Ministère de la Justice qui saisit le procureur général compétent.

Art.77.- L'irrégularité de la transmission de la demande d'entraide ne peut constituer une cause de nullité des actes accomplis en exécution de cette demande.

Art.78.- Lorsque l'exécution d'une demande d'entraide émanant d'une autorité judiciaire étrangère est de nature à porter atteinte à l'ordre public ou aux intérêts essentiels de la Nation, le Ministre en charge de la Justice notifie l'autorité requérante de ce qu'il ne peut être donné suite à sa demande.

Art.79.- Les autres modalités relatives à la procédure d'entraide judiciaire sont fixées par les textes particuliers.

Titre 5 - Des dispositions diverses et finales

Art.80.- L'autorité nationale compétente en matière de lutte contre la cybercriminalité doit adhérer aux organismes régionaux et internationaux en la matière.

Art.81.- Il ne peut être accordé de sursis pour les infractions prévues par la présente ordonnance.

Art.82.- Des textes réglementaires déterminent, en tant que de besoin, les dispositions de toute nature nécessaires à l'application de la présente ordonnance.

Art.83.- La présente ordonnance sera enregistrée, publiée selon la procédure d'urgence et exécutée comme loi de l'Etat.