Loi n°26-2020 du 5 juin 2020 relative à la cybersécurité

L'Assemblée nationale et le Sénat
ont délibéré et adopté ;

Le Président de la République promulgue la loi
dont la teneur suit :

TITRE I : DISPOSITIONS GENERALES

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

Article premier : La présente loi régit le cadre juridique national de sécurité des systèmes d'information et des réseaux de communications électroniques.

A ce titre, elle vise notamment à :

- organiser et coordonner la sécurité des systèmes d'information et des réseaux de communications électroniques ;
- instaurer la confiance des citoyens, des entreprises et des pouvoirs publics à l'égard des systèmes d'information et des réseaux de communications électroniques ;
- fixer les règles générales de protection des systèmes d'information et des réseaux de communications électroniques ;
- définir les règles applicables aux moyens, modalités et systèmes de cryptologie et réprimer les infractions y afférentes.

Article 2 : Sont exclus du champ de la présente loi :

- les systèmes d'information et les réseaux de communications électroniques utilisées en matière de défense et de sécurité nationale ;
- les moyens de cryptologie utilisés par les missions diplomatiques et consulaires visées par la convention de Vienne sur les relations diplomatiques.

Chapitre 2 : Des définitions

Article 3 : Au sens de la présente loi, 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 : activité ayant pour but la production, l'utilisation, l'importation, l'exportation ou la commercialisation des moyens de cryptologie ;
- Administration chargée des télécommunications : ministère ou ministre, selon les cas, investi pour le compte du Gouvernement, d'une compétence générale sur le secteur des télécommunications 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 ;

- Agence : agence congolaise de sécurité des systèmes et réseaux d'information créée par une loi de la République du Congo pour assurer la sécurité des systèmes d'information et des réseaux de communications électroniques ; Algorithme : suite d'opérations mathématiques élémentaires à appliquer à des données pour aboutir à un résultat désiré ;
- 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 ; constitue, notamment, une attaque active, l'atteinte à l'intégrité, à la disponibilité et à la confidentialité des données ;
- Attaque passive : acte n'altérant pas sa cible ; constitue, notamment, une attaque passive, 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 des 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, effectuer des contrôles de certification électronique, c'est-à-dire d'émission de certificats électroniques ; 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 celle-ci correspond à l'identité de la personne préalablement enregistrée ;
- Autorité de certification : autorité de confiance chargée de créer et d'attribuer des clés publiques et privées ainsi que des certificats électroniques ;
- Autorité de certification racine : organisme investi de la mission d'accréditation des autorités de certification, de la validation de la politique de certification desdites autorités accréditées, de la vérification et de la signature de leurs certificats respectifs ;
- Bi-clé : couple clé publique/clé privée utilisé dans des algorithmes de cryptographie asymétrique ;
- Certificat électronique : document électronique sécurisé par la signature électronique de la personne qui l'a émis et qui atteste après constat, la véracité de son contenu ;
- Certificat électronique qualifié : certificat électronique émis par une autorité de certificat agréée ;
- 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 la connaissance de la clé ;

- 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 offert 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 privée : clé utilisée dans les mécanismes de chiffrement asymétrique (ou chiffrement à clé publique), qui appartient à une entité et qui doit 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 ;
- Commerce électronique : activité économique par laquelle une personne propose ou assure à distance et par voie électronique la fourniture de biens et la prestation de services ;
- Communication audiovisuelle : communication au public de services de radiodiffusion télévisuelle et sonore ;
- Communications électroniques : 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 ;
- Conventions secrètes : 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 : message, sous forme de texte, de voix, de son ou d'image, envoyé par un réseau public de communication stocké sur un serveur du 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 ; conformité, des contrôles d'évaluation de l'adéquation des moyens (organisationnels, techniques, humains,

financiers) investis au regard des risques encourus, d'optimisation, de rationalité et de performance ;

- Cryptanalyse : ensemble des moyens qui permet d'analyser une information préalablement chiffrée en vue de la déchiffrer ;
- 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. Elle désigne aussi la science relative à la protection et à la sécurité des informations, notamment pour la confidentialité, l'authentification, l'intégrité et la non-répudiation ;
- Cybercriminalité : ensemble des 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 ;
- Déclaration des pratiques de certification : ensemble des pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'autorité de certification compétente applique dans le cadre de la fourniture de ce service et en conformité avec la (les) politique (s) de certification qu'elle s'est engagée (s) à respecter ;
- Déchiffrement : opération inverse du chiffrement ;
- 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) ;
- Dispositif de création de signature électronique : ensemble d'équipements et /ou logiciels privés de cryptage, homologués par une autorité compétente, configurés pour la création d'une signature électronique ;
- Dispositif de vérification de signature électronique : ensemble d'équipements et/ou logiciels publics de cryptage, homologués par une autorité compétente, permettant la vérification par une autorité de certification d'une signature électronique ;
- Données : représentation de faits, d'informations ou de notions sous une forme susceptible d'être traitée par un équipement terminal, y compris un programme permettant à ce dernier d'exécuter une fonction ;
- Données de connexion : ensemble de données relatives au processus

d'accès dans une communication électrique ;

- 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 sous-jacent ;
- Equipement terminal : appareil, installation ou ensemble d'installations destiné à être connecté à un point de terminaison d'un système d'information et émettant, recevant, traitant, ou stockant des données d'information ;
- 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 les prestations consistant entièrement ou principalement en la fourniture de communications électroniques ;
- Gravité de l'impact : appréciation du niveau de gravité d'un incident, pondéré par sa fréquence d'apparition ;
- Information : tout élément de connaissance susceptible d'être représenté à l'aide de conventions pour être utilisé, conservé, traité ou communiqué. L'information peut être exprimée sous forme écrite, visuelle, sonore, numérique, etc. ;
- 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 (modifiées ou détruites) d'une façon tant intentionnelle qu'accidentelle, de manière à assurer leur exactitude, leur fiabilité et leur pérennité ;
- 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, sans droit et sans autorisation, 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 droit, 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 (sites web les plus visités, mots de passe, etc.) 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 ;
- Message clair : version intelligible d'un message et compréhensible par tous ;
- Moyens de cryptographie : ensemble d'outils scientifiques et techniques, notamment le matériel ou les logiciels conçus ou modifiés pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser une opération inverse avec ou sans convention secrète afin de garantir la sécurité du stockage ou de la transmission de données, et d'assurer leur confidentialité et le contrôle de leur intégrité ;
- Non-répudiation : critère de sécurité assurant la disponibilité de preuves qui peuvent être opposées à un tiers et utilisées pour prouver la traçabilité d'une communication électronique qui a eu lieu ;
- Politique de certification : ensemble de règles identifiées, définissant les exigences auxquelles l'autorité de certification se conforme dans la mise en place de ses prestations et indiquant l'applicabilité d'un service de certification à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes ;
- Politique de sécurité : référentiel de sécurité établi par une organisation, reflétant sa stratégie de sécurité et spécifiant les moyens de la réaliser ;
- Prestation de cryptographie : opération visant la mise en œuvre, pour le compte d'autrui ou de soi, de moyens de cryptographie ;
- Prestation 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, actif ou passif et, le cas échéant, les équipements de commutation et de routage et les autres ressources qui permettent l'acheminement des signaux par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques comprenant les réseaux satellitaires, les réseaux terrestres fixes (avec commutation de circuits ou de paquets, y compris Internet) et mobiles, les systèmes utilisant le réseau électrique, pour autant qu'ils servent à la transmission de signaux, les réseaux utilisés pour la radiodiffusion sonore et télévisuelle et les réseaux câblés de télévision, quel que soit le type d'information transmise ;
- Sécurité : situation dans laquelle quelqu'un, quelque chose n'est exposé à aucun danger. Mécanisme destiné à prévenir un événement dommageable, ou à limiter les effets ;
- Service de certification : prestation fournie par une autorité de certification ;
- Service de communications électroniques ; prestation consistant entièrement ou principalement en la fourniture de communications électroniques à l'exclusion des contenus des services de

communications audiovisuelles ;

- Signataire : personne physique agissant pour son propre compte ou pour celui de la personne physique ou morale qu'elle représente, qui met à contribution un dispositif de création de signature électronique ;
- Signature électronique : signature obtenue par un algorithme de chiffrement asymétrique permettant d'authentifier l'émetteur d'un message et d'en vérifier l'intégrité ;
- Signature électronique avancée : signature électronique obtenue à l'aide d'un certificat électronique qualifié ;
- Standard ouvert : protocole de communication, d'interconnexion ou d'échange et format de données interopérable, dont les spécifications techniques sont publiques et sans restriction d'accès ni de mise en œuvre ;
- 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 : dispositif isolé ou groupe de dispositifs interconnectés ou apparentés, assurant par lui-même ou par un ou plusieurs de ses éléments, conformément à un programme, un traitement automatisé de données ;
- Vulnérabilité : défaut de sécurité dans l'architecture d'un réseau de communications électronique, ou dans la conception d'un système d'information, se traduisant soit intentionnellement, soit accidentellement par une violation de la politique de sécurité, dans l'architecture d'un réseau de communications électroniques, dans la conception d'un système d'information.

Les termes et expressions non définis dans cette loi, conservent leurs définitions ou significations données par les lois et règlements en vigueur ainsi que par les instruments juridiques internationaux auxquels le Congo a souscrits, notamment, la convention de l'union internationale des télécommunications, le règlement des radiocommunications et le règlement des télécommunications internationales.

Chapitre 3 : Des principes généraux de la cybersécurité

Article 4 : Quiconque, citoyens, entreprises, organisations ou pouvoirs publics, faisant usage des systèmes et réseaux d'information, doit prendre les mesures adéquates pour protéger et prévenir tout risque encouru par les tiers du fait de cet usage.

Quiconque développe, possède, fournit, gère, maintient et utilise des systèmes et réseaux d'information, est responsable et comptable de leur sécurité et par ailleurs tenu d'examiner et d'évaluer en permanence ses propres politiques, pratiques, mesures et procédures pour s'assurer qu'elles sont adaptées à leur environnement.

Article 5 : Quiconque développe, possède, fournit, gère, maintient et utilise des systèmes et réseaux d'information doit tout mettre en œuvre pour prévenir, détecter et répondre aux incidents de sécurité.

Article 6 : Les usagers et détenteurs des systèmes et réseaux d'information doivent échanger les informations qu'ils détiennent sur les menaces et les vulnérabilités des réseaux et systèmes d'information de manière appropriée et doivent mettre en place des procédures permettant une coopération rapide et efficace pouvant prévenir et détecter les incidents de sécurité.

Article 7 : La sécurité des systèmes et réseaux d'information est assurée dans le respect des valeurs garanties par les lois et règlements en vigueur et notamment, la liberté d'échanger des opinions et des idées, la libre circulation de l'information, la confidentialité de l'information et des communications, la protection adéquate des données à caractère personnel, l'ouverture et la transparence.

Article 8 : Quiconque fait ou détient des systèmes d'information doit procéder à des évaluations des risques, notamment les principaux facteurs internes et externes, tels la technologie, les facteurs physiques et humains, les politiques et services de tierces parties ayant des implications sur la sécurité.

Cette évaluation des risques tient compte des préjudices aux intérêts d'autrui ou causé par autrui, rendus possibles par l'interconnexion des systèmes d'information.

Article 9 : Les systèmes et réseaux d'information sont conçus, mis en oeuvre et coordonnés de façon à en optimiser la sécurité. Les entreprises et les pouvoirs publics mettent en oeuvre les moyens nécessaires en vue d'atteindre le degré de sécurité numérique souhaité en premier lieu grâce à l'autorégulation.

Les mesures de protection et les solutions adoptées à cet effet, sont à la fois techniques et non techniques, et proportionnées à la valeur de l'information dans les systèmes et réseaux d'information de l'organisation.

Pour l'utilisateur final, la conception et la mise en œuvre de la sécurité consistent essentiellement à sélectionner et configurer des produits et services pour leurs systèmes.

Article 10 : La gestion de la sécurité est fondée sur l'évaluation des risques. Elle couvre tous les niveaux des activités, tous les aspects des opérations des personnes visées aux articles 8 et 9 ci-dessus et inclut, par anticipation, les réponses aux menaces identifiables ou prévisibles ainsi que la prévention, la détection et la résolution des incidents, la reprise des systèmes, la maintenance permanente, le contrôle et l'audit.

Article 11 : Les usagers et détenteurs des systèmes et réseaux d'information doivent en garantir la sécurité de façon constante pour faire face à l'évolution des risques. Ils mettent en place des dispositifs d'évaluation continue des risques et introduisent les modifications appropriées dans les politiques, pratiques, mesures et procédures de sécurité.

TITRE II : DES ACTIVITES DE SECURITE DES SYSTEMES D'INFORMATION ET DES RESEAUX DE COMMUNICATIONS ELECTRONIQUES

Chapitre 1 : De l'audit obligatoire

Article 12 : Les systèmes d'information et les réseaux de communications électroniques relevant des divers organismes publics sont soumis à un régime d'audit obligatoire et périodique de la sécurité des systèmes d'information, à l'exception des systèmes d'information et des réseaux de communications électroniques appartenant aux ministères en charge de la défense nationale et de la sécurité publique, ainsi que ceux des missions diplomatiques et consulaires.

Sont également soumis à un régime d'audit obligatoire et périodique de la sécurité informatique, les systèmes d'information et les réseaux de communications électroniques des organismes dont la liste sera fixée par voie réglementaire.

Article 13 : 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 sont fixés par voie réglementaire.

Article 14 : Lorsque les organismes concernés n'effectuent pas l'audit obligatoire et périodique, l'agence avertit l'organisme concerné qui doit effectuer l'audit dans un délai de trois mois à compter de la date de cet avertissement.

A l'expiration de ce délai sans résultat, l'agence nationale de sécurité des systèmes d'information est tenue de désigner, aux frais de l'organisme concerné, un expert chargé de l'audit sus indiqué.

Article 15 : Les organismes publics et privés visés dans la présente loi sont liés par un devoir de collaboration vis-à-vis de l'agence et des experts chargés de l'audit.

Ils mettent ainsi à la disposition de l'agence nationale de sécurité des systèmes d'information tous les documents et dossiers relatifs à la sécurité informatique.

Chapitre 2 : Des auditeurs

Article 16 : L'opération d'audit est effectuée par des experts, personnes physiques ou morales, préalablement agréés par l'agence.
Les conditions et les procédures d'agrément de ces experts sont fixées par voie réglementaire.

Article 17 : Les agents de l'agence nationale de sécurité des systèmes d'information et les experts chargés des opérations d'audit sont soumis au secret professionnel. Ils préservent la confidentialité des informations dont ils ont eu connaissance lors de l'exercice de leurs missions.

Est passible des sanctions prévues par le code pénal quiconque divulgue, participe ou incite à la divulgation des informations visées à l'alinéa premier du présent article.

Chapitre 3 : Des perturbations constatées

Article 18 : Tout exploitant d'un système d'information ou d'un réseau de communications électroniques, qu'il soit organisme public ou privé, informe, sans délai, l'agence de toute attaque, intrusion et autres perturbations susceptibles d'entraver le fonctionnement d'un autre système d'information ou réseaux de communications électroniques, afin de lui permettre de prendre les mesures nécessaires pour y faire face.

L'exploitant se conforme aux mesures arrêtées par l'agence pour mettre fin à ces perturbations.

Article 19 : Dans les cas prévus à l'article 18 ci-dessus et afin de protéger les systèmes d'information et les réseaux de communications électroniques, l'agence peut prononcer l'isolement du système d'information ou du réseau de communications électroniques concerné jusqu'à ce que les perturbations cessent. Le ministre chargé des technologies de l'information et de la communication en est informé sans délai.

Concernant les exceptions prévues à l'article 12 de la présente loi, des procédures adéquates sont arrêtées en coordination avec les ministres de la défense nationale, de la sécurité et des technologies de l'information et de la communication.

Chapitre 4 : De la protection des réseaux de communications électroniques

Article 20 : Les opérations des réseaux de communications électroniques et les fournisseurs de services de communications électroniques prennent toutes les mesures techniques et administratives utiles pour garantir la sécurité des services offerts.

A cet effet, ils sont tenus d'informer les usagers :

- des dangers encourus lors de l'utilisation de leurs réseaux ;
- des risques particuliers de violation de la sécurité, notamment les dénis de service, le ré-routage anormal, le trafic et les ports inhabituels, les écoutes passives et actives, les intrusions et tout autre risque ;
- le cas échéant, de l'inexistence de moyens techniques permettant d'assurer la sécurité de leurs communications.

Article 21 : Les opérateurs de réseaux de communications électroniques et les fournisseurs de service de communications électroniques conservent les données de connexion et de trafic pendant une période de dix ans.

Les opérateurs de réseaux de communications électroniques et les fournisseurs de services de communications électroniques installent 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 de communications électroniques et celle des fournisseurs de service de communications électroniques sont engagées si l'utilisation des données prévues à l'alinéa 2 du présent article porte atteinte aux libertés et droits fondamentaux des usagers.

Chapitre 5 : De la protection des systèmes d'information

Article 22 : Les exploitants des systèmes d'information se dotent de systèmes normalisés leur permettant d'identifier, d'évaluer, de traiter et de gérer en permanence les risques liés à la sécurité des systèmes d'information dans le cadre des services offerts directement ou indirectement au public.

Les exploitants des systèmes d'information mettent 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 du présent article, font l'objet d'une approbation et d'un visa conforme de l'agence nationale de sécurité des systèmes d'information.

Les plateformes des systèmes d'information font l'objet de protection contre d'éventuels rayonnements et des intrusions qui pourraient compromettre l'intégrité des données transmises et contre toute attaque externe notamment par un système de détection d'intrusions.

Article 23 : Les personnes morales dont l'activité est d'offrir un accès à des systèmes d'information informent les usagers :

- des dangers encourus, notamment par les particuliers, en cas d'utilisation de systèmes d'information non sécurisés ;
- de la nécessité d'installer des dispositifs de contrôle parental ;
- des risques particuliers de violations de sécurité, notamment la famille générique des virus ;
- de l'existence de moyens techniques permettant de restreindre l'accès à certains services et de leur proposer au moins l'un de ces moyens, notamment l'utilisation des systèmes d'exploitation les plus récents, les outils antivirus et contre les logiciels espions et trompeurs, l'activation de pare-feux personnels ou de systèmes de détection d'intrusions et l'activation des mises à jour automatiques.

Article 24 : Les exploitants des systèmes d'information informent les utilisateurs de l'interdiction faite d'utiliser le réseau de communications électroniques pour diffuser des contenus illicites ou d'accomplir tout autre acte de nature à entamer la sécurité des réseaux ou des systèmes d'information.

L'interdiction porte également sur la conception de logiciels trompeurs, de logiciels espions, de logiciels potentiellement indésirables ou de tout autre outil conduisant à un comportement frauduleux.

Article 25 : Les exploitants des systèmes d'informations ont l'obligation de conserver les données de connexion et de trafic de leurs systèmes d'information pendant une période de dix ans.

Les exploitants des systèmes d'information sont tenus d'installer des mécanismes de surveillance et de contrôle d'accès aux données de leurs systèmes d'information.

Les données conservées sont accessibles lors des investigations judiciaires. Les installations des exploitants des systèmes d'information peuvent faire l'objet de perquisition ou de saisie sur décision d'une autorité judiciaire, dans les conditions prévues par les lois et règlements en vigueur.

Article 26 : Les exploitants des systèmes d'information 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'information et leurs utilisateurs peuvent coopérer entre eux pour l'élaboration et la mise en œuvre des pratiques, mesures et techniques de sécurité de leurs systèmes.

Article 27 : Les fournisseurs de contenus des réseaux de communications électroniques et systèmes d'information sont tenus d'assurer la disponibilité des contenus, ainsi que celle des données stockées dans leurs installations. Ils mettent en place des filtres pour faire face aux atteintes préjudiciables aux données personnelles et à la vie privée des utilisateurs.

TITRE III : DU REGIME DE LA CRYPTOLOGIE

Chapitre 1 : Des régimes juridiques des moyens et prestations de cryptologie

Article 28 : L'utilisation des moyens et prestations de cryptologie est libre :

- 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 massage transmis ;
- lorsque la fourniture, le transfert depuis ou vers un pays membre de la CEEAC ou de la 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 un organisme agréé conformément aux dispositions des articles 34 et 35 de la présente loi, et dans les conditions fixées par décret.

Article 29 : Les modalités d'utilisation de la taille de certaines clés sont fixées par décret, sans préjudice de l'application des dispositions de l'article 28 ci-dessus.

Article 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'agence nationale de sécurité des systèmes d'information.

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

Article 31 : Le prestataire ou la personne procédant à la fourniture ou à l'importation d'un service de cryptologie tient à la disposition de l'agence nationale de sécurité des systèmes d'information une description des caractéristiques techniques de ce moyen de cryptologie, ainsi que le code source des logiciels utilisés.

Article 32 : Les prestataires de services de cryptologie sont soumis au secret professionnel.

Article 33 : Sauf dispositions contraires, l'exportation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité est soumise à autorisation de l'agence nationale de sécurité des systèmes d'information.

Chapitre 2 : De l'agrément des organismes exerçant des prestations de cryptologie

Article 34 : Les organismes exerçant des prestations de cryptologie doivent être agréés par l'agence nationale de sécurité des systèmes d'information.

Article 35 : Les conditions de délivrance de l'agrément aux organismes exerçant des prestations de cryptologie ainsi que leurs obligations sont définies par voie réglementaire.

Chapitre 3 : De la responsabilité des prestataires de services de cryptologie

Article 36 : Les prestataires de services de cryptologie à des fins de confidentialité sont responsables du préjudice causé dans le cadre desdites prestations 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.

Les prestataires de services de cryptologie sont responsables vis-à-vis des personnes qui se sont raisonnablement fiées à leur produit, du préjudice résultant de leur faute intentionnelle ou de leur négligence.

Toute clause contraire aux dispositions du présent article est réputée non écrite.

Article 37 : Les prestataires de services de cryptologie sont exonérés de toute responsabilité à l'égard des personnes qui font un usage non autorisé de leur produit.

Chapitre 4 : Des sanctions administratives

Article 38 : Lorsqu'un prestataire de service de cryptologie, même à titre gratuit, ne respecte pas les obligations auxquelles il est assujetti en application de la présente loi, l'agence nationale de sécurité des systèmes d'information peut, après une procédure contradictoire, prononcer :

- l'interdiction d'utiliser ou de mettre en circulation le moyen de cryptologie concerné ;
- le retrait provisoire, pour une durée de trois mois, de l'agrément accordé ;
- le retrait définitif de l'agrément ;
- des amendes dont le montant est fixé par voie réglementaire en

fonction de la gravité des manquements commis et en relation avec les avantages ou les profits tirés de ces manquements.

Chapitre 5 : Des sanctions pénales

Article 39 : Les infractions aux dispositions de la présente loi sont prévues et réprimées par le code pénal ainsi que par la loi relative à la lutte contre la cybercriminalité.

TITRE IV : DISPOSITIONS TRANSITOIRES ET FINALES

Article 40 : Les agréments et les déclarations de fourniture, d'importation et d'exportation de moyens de cryptographie délivrés par les autorités compétentes demeurent valables jusqu'à l'expiration du délai prévu par celles-ci.

Article 41 : Les personnes assurant des prestations de cryptologie ou exerçant des activités de cryptologie disposent d'un délai de six mois à compter de la date d'entrée en vigueur de la présente loi, pour régulariser leur situation auprès de l'agence nationale de sécurité des systèmes d'information.

Article 42 : La présente loi, qui abroge toutes dispositions antérieures contraires, sera publiée au Journal officiel et exécutée comme loi de l'Etat.

Fait à Brazzaville, le 5 juin 2020

Par le Président de la République,
Denis SASSOU-N'GUESSO

Le Premier ministre, chef du Gouvernement,
Clément MOUAMBA

Le ministre des postes, des télécommunications et de l'économie numérique,
Léon Juste IBOMBO

Le ministre d'Etat, ministre du commerce, des approvisionnements et de la consommation,
Alphonse Claude NSILOU

Pour le ministre des finances et du budget, en mission :
Le ministre délégué auprès du ministre des finances et du budget, chargé du budget,
Ludovic NGATSE

Le ministre de l'intérieur et de la décentralisation,
Raymond Zéphirin MBOULOU

Le ministre de la défense nationale,
Charles Richard MONDJO

Le ministre de la justice et des droits humains et de la promotion des peuples autochtones,
Aimé Ange Wilfrid BININGA

Le ministre des affaires étrangères, de la coopération et des Congolais de l'étranger,
Jean-Claude GAKOSSO