RÉPUBLIQUE DU CONGO
*Unité * Travail * Progrès*

62e ANNEE - N° 23 — Jeudi 11 juin 2020

JOURNAL OFFICIEL

DE LA REPUBLIQUE DU CONGO

paraissant le jeudi de chaque semaine à Brazzaville

DESTINATIONS	ABONNEMENTS 1 AN	6 MOIS	3 MOIS	NUMERO
REPUBLIQUE DU CONGO	24.000	12.000	6.000	500 F CFA
	Voie aérienne exclusivement			
ETRANGER	38.400	19.200	9.600	800 F CFA

¤ Annonces judiciaires et légales et avis divers : 460 frs la ligne (il ne sera pas compté moins de 5.000 frs par annonce ou avis).
Les annonces devront parvenir au plus tard le jeudi précédant la date de parution du "JO".
¤ Propriété foncière et minière : 8.400 frs le texte. ¤ Déclaration d'association : 15.000 frs le texte.

DIRECTION : TEL./FAX : (+242) 281.52.42 - BOÎTE POSTALE 2.087 BRAZZAVILLE - Email : journal.officiel@sgg.cg
Règlement : espèces, mandat postal, chèque visé et payable en République du Congo, libellé à l'ordre du ***Journal officiel*** et adressé à la direction du Journal officiel et de la documentation.

SOMMAIRE

PARTIE OFFICIELLE

- LOIS -

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.

Ils doivent par ailleurs élaborer et adopter des pratiques exemplaires et promouvoir des comportements qui tiennent compte des impératifs de sécurité et de respect des intérêts légitimes des autres usagers et détenteurs des systèmes et réseaux d'information.

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 œuvre et coordonnés de façon à en optimiser la sécurité. Les entreprises et les pouvoirs publics mettent en œuvre 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

Loi n° 27-2020 du 5 juin 2020 portant lutte contre la cybercriminalité

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 champ d'application

Article premier : La présente loi a pour objet de définir et réprimer les infractions liées aux technologies de l'information et de la communication.

Elle vise à compléter ainsi les dispositions du code pénal en vigueur.

Article 2 : Les dispositions de la présente loi sont applicables à toutes les personnes, quelle que soit leur nationalité, ayant commis une infraction par le biais des technologies de l'information et de la communication en République du Congo.

Chapitre 2 : Des définitions

Article 3 : Au sens de la présente loi, on entend par :

- Accès dérobé : mécanisme permettant de dissimuler l'accès à des données ou à un système d'information sans l'autorisation de l'utilisateur légitime ;

- Communication au public par voie électronique : toute mise à la disposition du public ou d'une catégorie de public, par un procédé de communications électroniques ou magnétiques, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature ;
- Communications électroniques : émission, transmission ou réception de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique ;
- 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 ;
- Données informatiques : toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction ;
- Données à caractère personnel : toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique ;
- Données relatives aux abonnés : toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir :

- le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;
- l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ;
- toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

- 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 ;
- Matériel xénophobe : 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 couleur, de l'ascendance ou de l'origine nationale ou ethnique ou de la religion, dans la mesure où ce dernier sert de prétexte à l'un ou à l'autre de ces éléments ou qui incite à de tels actes ;
- Pornographie infantile : toute donnée, quelle qu'en soit la nature ou la forme ou le support, représentant :

- un enfant se livrant à un comportement sexuellement explicite ;
- une personne qui apparaît comme un enfant se livrant à un comportement sexuellement explicite ;
- des images réalistes représentant un enfant se livrant à un comportement sexuellement explicite.

- Programme informatique : séquence d'instructions qui spécifie, étape par étape, les opérations à effectuer par un ordinateur ou une composante d'ordinateur pour obtenir un résultat ;
- Système d'information : ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) qui permet de collecter, de regrouper, de classifier, de traiter et de diffuser l'information ;
- Système d'informatique : tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données ;
- Technologies de l'information et de la communication : désigne les technologies employées pour recueillir, stocker, utiliser et envoyer des informations ainsi que celles qui impliquent l'utilisation des ordinateurs ou de tout système de communication, y compris de télécommunication.

TITRE II : DES INFRACTIONS LIEES AUX TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Chapitre 1 : Des atteintes à la confidentialité des systèmes d'information

Article 4 : Quiconque accède ou tente d'accéder frauduleusement à tout ou partie d'un système d'information est puni d'un emprisonnement de six moins à trois ans au plus et d'une amende d'un million (1 000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement.

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

Article 5 : Quiconque se maintient ou tente de se maintenir frauduleusement dans tout ou partie d'un système d'information est puni d'un emprisonnement de six mois au moins à trois ans au plus et d'une amende d'un million (1000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Chapitre 2 : Des atteintes à l'intégrité des systèmes d'information

Article 6 : Est puni d'un emprisonnement d'un an au moins à cinq ans au plus et d'une amende de cinq millions (5 000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement, quiconque entrave ou tente d'entraver le fonctionnement d'un système d'information.

Chapitre 3 : De l'introduction frauduleuse de données dans un système d'information

Article 7 : Quiconque introduit ou tente d'introduire frauduleusement des données dans un système d'information est puni d'un emprisonnement d'un an au moins à cinq ans au plus et d'une amende de cinq millions (5 000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Chapitre 4 : De l'interception frauduleuse de données d'un système d'information

Article 8 : Quiconque intercepte ou tente d'intercepter frauduleusement, par des moyens techniques, des données d'un système d'information lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système d'information, est puni d'un emprisonnement d'un an au moins à cinq ans au plus et d'une amende de cinq millions (5 000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Chapitre 5 : Des atteintes à l'intégrité des données d'un système d'information

Article 9 : Quiconque endommage ou tente d'endommager, efface ou tente d'effacer, détériore ou tente de détériorer, altère ou tente d'altérer, supprime ou tente de supprimer, frauduleusement des données d'un système d'information, est puni d'un emprisonnement d'un an au moins à cinq ans au plus et d'une amende de cinq millions (5 000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 10 : Quiconque produit ou fabrique un ensemble de données numérisées par l'introduction, l'effacement ou la suppression frauduleuse de données informatisées stockées, traitées ou transmises par un système d'information, 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 emprisonnement d'un an au moins à cinq ans au plus et d'une amende de cinq millions (5 000 000) à dix millions (10 000 000) de francs. CFA ou de l'une de ces deux peines seulement.

Est puni des mêmes peines quiconque, en connaissance de cause, fait usage ou tente de faire usage des données obtenues dans les conditions prévues à l'alinéa premier du présent article.

Article 11 : Est puni d'un emprisonnement d'un an au moins à cinq ans au plus et d'une amende de cinq millions (5 000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement, quiconque obtient frauduleusement, pour soi-même ou pour autrui, un avantage quelconque, par l'introduction, l'altération, l'effacement ou la suppression de données informatisées.

Chapitre 6 : Des infractions relatives aux données à caractère personnel

Article 12 : Quiconque, même par négligence, procède ou fait procéder à des traitements de données à caractère personnel sans avoir respecté les formalités préalables à leur mise en œuvre prévues par la loi sur les données à caractère personnel est puni d'un emprisonnement d'un an au moins à cinq ans au plus et d'une amende d'un million (1000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 13 : Est puni d'un emprisonnement d'un an au moins à cinq ans au plus et d'une amende d'un million (1000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement, quiconque, même par négligence, procède ou fait procéder à un traitement qui a fait l'objet d'un retrait provisoire de l'autorisation ou d'une interdiction provisoire de traitement.

Article 14 : Quiconque ne respecte pas, y compris par négligence, les normes simplifiées ou d'exonération établies à cet effet par la commission nationale pour la protection des données à caractère personnel, dans les hypothèses et conditions définies à l'article 35 de la loi relative à la protection des données à caractère personnel, est puni d'un emprisonnement d'un an au moins à cinq ans au plus et d'une amende d'un million (1000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 15 : Quiconque, hors les cas où le traitement a été autorisé dans les conditions prévues par la loi sur les données à caractère personnel, procède ou fait procéder à un traitement de données à caractère personnel incluant parmi les données sur lesquelles il porte le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, est puni d'un emprisonnement d'un an au moins à cinq ans au plus et d'une amende d'un million (1000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 16 : Est puni d'un emprisonnement d'un an au moins à cinq ans au plus et d'une amende d'un million (1000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement, quiconque procède ou fait procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures visant à préserver la sécurité des données et notamment d'empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

Article 17 : Quiconque collecte des données à caractère personnel par un moyen frauduleux, déloyal ou illicite, est puni d'un emprisonnement d'un an au moins à cinq ans au plus et d'une amende d'un million (1 000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 18 : Quiconque procède ou fait procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est puni d'un emprisonnement d'un an au moins à cinq ans au plus et d'une amende d'un million (1000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 19 : Est puni d'un emprisonnement d'un an au moins à cinq ans au plus et d'une amende d'un million (1000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement, quiconque, hors les cas prévus par la loi, met ou conserve sur support ou mémoire informatique, sans le consentement exprès de l'intéressé, des données à caractère personnel faisant apparaître, directement ou indirectement, l'origine ethnique, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales, ou qui sont relatives à la santé ou à l'orientation sexuelle de celui-ci.

Est puni des mêmes peines, quiconque, hors les cas prévus par la loi, met ou conserve sur support ou mémoire informatique des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté.

Les dispositions de l'alinéa 1 du présent article s'appliquent aux traitements non automatisés des données à caractère personnel dont la mise en œuvre ne se limite pas à l'exercice d'activités exclusivement personnelles.

Article 20 : Est puni des mêmes peines prévues à l'article 19 ci-dessus, quiconque procède au traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé :

- sans avoir préalablement informé individuellement les personnes sur le compte desquelles des données à caractère personnel sont recueillies ou transmises de leur droit d'accès, de rectification et d'opposition, de la nature des données transmises et des destinataires de celles-ci ainsi que des dispositions prises pour leur traitement, leur conservation et leur protection ;
- malgré l'opposition de la personne concernée ou, lorsqu'il est prévu par la loi, en l'absence du consentement éclairé et exprès de la personne, ou s'il s'agit d'une personne décédée, malgré le refus exprimé par celle-ci de son vivant.

Article 21 : Est puni d'un emprisonnement d'un an au moins à cinq ans au plus et d'une amende d'un million (1000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement, quiconque conserve des données à caractère personnel au-delà de la durée nécessaire aux finalités pour lesquelles elles ont été collectées ou traitées, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi.

Article 22 : Quiconque détenant des données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, détourne ces informations de leur finalité telle que définie par les dispositions législatives et réglementaires sur la protection des données à caractère personnel, ou par la décision de la commission chargée de la protection des données à caractère personnel autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement, est puni d'un emprisonnement d'un an au moins à cinq ans au plus et d'une amende d'un million (1000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 23 : Est puni d'un emprisonnement d'un an au moins à cinq ans au plus et d'une amende d'un million (1000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement, quiconque recueille, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, et porte, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir.

Si la divulgation prévue à l'alinéa premier du présent article est commise par imprudence ou négligence, le responsable est puni d'un emprisonnement de six mois au moins à cinq ans au plus et d'une amende de trois cent mille (300 000) à cinq millions (5 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Dans les cas prévus aux deux alinéas du présent article, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit.

Article 24 : Est puni d'un emprisonnement de six mois au moins à deux ans au plus et d'une amende d'un million (1000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement, quiconque entrave l'action de la commission chargée de la protection des données à caractère personnel ;

- soit en refusant de communiquer à ses membres ou aux agents habilités, les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître ;
- soit en communiquant des informations qui ne sont pas conformes au contenu des enregistrements tel qu'il était au moment où la demande a été formulée ou qui ne présentent

pas ce contenu sous une forme directement accessible ;

- soit en s'opposant à l'exercice des missions confiées à ses membres ou aux agents habilités en application de la loi sur la protection des données à caractère personnel.

Chapitre 7 : De l'abus de dispositifs et de l'association de malfaiteurs informatiques

Article 25 : Quiconque produit, vend, importe, détient, diffuse, offre, cède ou met à disposition un équipement, un programme informatique, tout dispositif ou donnée conçue ou spécialement adaptée pour commettre une ou plusieurs des infractions prévues aux articles 4 à 11 de la présente loi ou un mot de passe, un code d'accès ou des données informatisées similaires permettant d'accéder à tout ou partie d'un système d'information, est puni soit des peines prévues pour l'infraction elle-même, soit en cas de pluralité d'infractions, des peines prévues pour l'infraction la plus sévèrement réprimée.

Article 26 ; Quiconque participe à une association formée ou à une entente établie en vue de préparer ou de commettre une ou plusieurs des infractions prévues par la présente loi, est puni soit des peines prévues pour l'infraction elle-même, soit en cas de pluralité d'infractions, des peines prévues pour l'infraction la plus sévèrement réprimée.

Lorsqu'elles ont été commises en bande organisée, les infractions prévues par la présente loi sont punies du maximum de la peine correspondante.

Chapitre 8 : De la pornographie infantile

Article 27 : Quiconque produit, enregistré, offre, met à disposition, diffuse, transmet une image- ou une présentation présentant un caractère de pornographie infantile par le biais d'un système d'information, commet un crime punissable de la réclusion de cinq ans au moins à dix ans au plus.

Article 28 : 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, commet un crime punissable de la réclusion de cinq ans au moins à dix ans au plus.

Article 29 : Quiconque possède une image ou une présentation présentant un caractère de pornographie infantile dans un système d'information ou dans un moyen quelconque de stockage de données informatisées, commet un crime punissable d'un emprisonnement de cinq ans au moins à dix ans au plus.

Est puni des mêmes peines, quiconque facilite l'accès à des images, des documents, du son ou une représentation présentant un caractère de pornographie à un enfant.

Article 30 : Toute personne adulte qui propose intentionnellement, par le biais des technologies de l'information et de la communication, une rencontre à un enfant, dans le but de commettre à son encontre une des infractions prévues aux articles 27, 28 et 29 de la présente loi, lorsque cette proposition a été suivie d'actes matériels conduisant à ladite rencontre, commet un crime punissable de la réclusion de cinq ans au moins à dix ans au plus.

Chapitre 9 : De la xénophobie par le biais d'un système d'information

Article 31 : Quiconque crée, télécharge, diffuse ou met à disposition, sous quelque forme que ce soit, du matériel raciste et xénophobe, par le biais d'un système d'information est puni d'un emprisonnement de six mois au moins à cinq ans au plus et d'une amende d'un million (1000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 32 : Quiconque profère une menace par le biais d'un système d'information, commet une infraction pénale envers une personne en raison de son appartenance à un groupe qui se caractérise par la couleur, l'ascendance ou l'origine nationale, ou ethnique, ou la religion dans la mesure où cette appartenance sert de prétexte à l'un ou l'autre de ces éléments, ou un groupe de personnes qui se distingue par une de ces caractéristiques, est puni d'un emprisonnement de six mois au moins à cinq ans au plus et d'une amende d'un million (1000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 33 : Quiconque profère une insulte par le biais d'un système d'information envers une personne en raison de son appartenance à un groupe qui se caractérise par la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion, ou l'opinion politique dans la mesure où cette appartenance sert de prétexte à l'un ou l'autre de ces éléments, ou un groupe de personnes qui se distingue par une de ces caractéristiques est puni d'ùn emprisonnement de six mois au moins à cinq ans au plus et d'une amende d'un million (1000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 34 : Quiconque diffuse ou met à disposition par le biais d'un système d'information, du matériel qui nie, minimise de manière grossière, approuve ou justifie des actes constitutifs de génocide ou de crimes contre l'humanité tels que définis par le droit international et reconnus comme tel par une décision définitive d'un tribunal international établi par des instruments internationaux pertinents et dont la juridiction est reconnue, est puni d'un emprisonnement de six mois au moins à cinq ans au plus et d'une amende d'un million (1000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 35 : Le tribunal peut, concomitamment à la condamnation, prononcer la confiscation des matériels, équipements, instruments, programmes informatiques ou tous dispositifs ou données appartenant au condamné et ayant servi à commettre

les infractions prévues aux articles 4 à 34 de la présente loi.

Chapitre 10 : Des infractions liées aux activités des prestataires de services de communication au public par voie électronique

Article 36 : Quiconque présente un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion par un prestataire de service de communication au public par voie électronique, alors qu'il sait cette information inexacte, est puni d'un emprisonnement de six mois au moins à un an au plus et d'une amende de deux cent mille (200 000) à un million (1 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 37 : Tout prestataire de service de communication au public par voie électronique qui ne satisfait pas à l'obligation de mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance les données illicites telles, l'incitation à la haine raciale, la pornographie infantile, le terrorisme ou à l'obligation d'informer promptement les autorités publiques compétentes de toutes activités illicites qui lui sont signalées et qu'exercent les destinataires de leurs services, est puni d'un emprisonnement de six mois au moins à un an au plus et d'une amende de cent mille (100 000) à cinq cent mille (500 000) francs CFA ou de l'une de ces deux peines seulement.

Article 38 : Tout prestataire de services de communication au public par voie électronique qui ne satisfait pas à l'obligation de conservation des données permettant l'identification de quiconque a contribué à la création du contenu, ou de l'un des contenus des services dont il est prestataire, est puni d'un emprisonnement de six mois au moins à un an au plus et d'une amende de cent mille (100 000) à cinq cent mille (500 000) francs CFA ou de l'une de ces deux peines seulement.

Les peines prévues à l'alinéa premier du présent article s'appliquent lorsque le prestataire de services de communication par voie électronique ne défère pas à la demande d'une autorité judiciaire d'obtenir communication des données visées au même alinéa.

Article 39 : Toute personne dont l'activité est d'éditer un service de communication au public en ligne qui ne met pas à la disposition du public et dans un standard ouvert, les informations requises par les dispositions du même article susvisé, est punie d'un emprisonnement de six mois au moins à un an au plus et d'une amende de deux cent mille (200 000) à deux millions (2 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Est puni des mêmes peines, tout prestataire de services de communication au public par voie électronique qui ne fournit pas les moyens techniques permettant de satisfaire aux conditions d'identification ci-après :

- pour les personnes physiques, leurs noms, prénoms, domiciles et numéros de téléphone et, si elles sont assujetties aux formalités d'inscription au registre de commerce et du crédit immobilier, les numéros de leurs inscriptions ;
- pour les personnes morales, leurs dénominations ou leurs raisons sociales et leurs sièges sociaux, leurs numéros de téléphone et, s'il s'agit d'entreprises assujetties aux formalités d'inscription au registre du commerce et du crédit immobilier ou au répertoire national des entreprises et associations, les numéros de leurs sièges sociaux ;
- le nom du directeur ou du codirecteur de la publication du service de communication au public par voie électronique et, le cas échéant., celui du responsable de la rédaction.

Article 40 : Toute personne nommée ou désignée dans un service de communication au public par voie électronique qui ne publie pas la réponse découlant de l'exercice du droit de réponse vingt-quatre heures après la réception de la demande, est punie d'une amende de deux cent mille (200 000) à deux millions (2 000 000) de francs CFA, sans préjudice de toutes autres peines prévues par Ia législation en vigueur.

Article 41 : Toute personne exerçant une activité dans le domaine du commerce électronique qui ne satisfait pas aux obligations d'information relatives au maintien de l'ordre et de la sécurité publics, à la préservation des intérêts de la défense nationale, à la protection des enfants, de la vie privée, de la santé publique ou des consommateurs, est punie d'un emprisonnement de six mois au moins à un an au plus et d'une amende de cent mille (100 000) à cinq cent mille (500 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 42 : Tout fournisseur de biens ou de services par voie électronique qui manifeste un refus de rembourser les montants reçus d'un consommateur qui exerce son droit de rétractation est puni d'un emprisonnement de six mois au moins à un an au plus et d'une amende de deux cent mille (200 000) à deux millions (2 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 43 : Quiconque trompe ou tente de tromper, par des manœuvres frauduleuses, l'acheteur sur l'identité, la nature ou l'origine du bien vendu, en livrant un bien autre que celui commandé et acheté par le consommateur, est puni d'un emprisonnement de trois mois au moins à un an au plus et d'une amende de cinq cent mille (500 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces peines seulement.

Chapitre 11 : Des infractions relatives à la publicité par voie électronique

Article 44 : Toute publicité, sous quelque forme que ce soit, accessible par un service de communication

électronique, est clairement identifiée comme tel. A défaut, elle comporte la mention « publicité » de manière lisible, apparente et non équivoque.

La personne physique ou morale pour le compte de laquelle la publicité est faite doit être clairement identifiée.

Les offres promotionnelles, telles que les annonces de réduction de prix, les offres conjointes ou tout autre cadeau, ainsi que les concours ou les jeux promotionnels, adressés par courrier électronique, sont clairement identifiables comme tel et les conditions pour en bénéficier sont aisément accessibles et présentées de manière précise et non équivoque sur l'objet du courrier dès leur réception par leur destinataire, ou en cas d'impossibilité technique, dans le corps du message.

Les concours ou jeux promotionnels sont clairement identifiables comme tels et leurs conditions de participation comprenant, le cas échéant, le numéro d'autorisation dont le prestataire doit disposer, sont aisément accessibles et présentées de manière précise et non équivoque.

Les publicités qui font partie d'un service de la société de l'information fourni par un membre d'une profession réglementée, ou qui constituent un tel service, sont autorisées, sous réserve du respect des règles professionnelles visant, notamment, l'indépendance, la dignité et l'honneur de la profession ainsi que le secret professionnel et la loyauté envers les clients et les autres membres de la profession,

Quiconque contrevient aux dispositions ci-dessus, est puni d'un emprisonnement de six mois au moins à deux ans au plus et d'une amende de cent mille (100 000) à cinq cent mille (500 000) francs CFA ou de l'une de ces deux peines seulement.

Chapitre 12 : Des infractions liées à la prospection directe

Article 45 : L'utilisation du courrier électronique, de télécopieurs ou de systèmes automatisés d'appel et de communication sans intervention humaine, notamment d'automates d'appel, à des fins de publicité, n'est autorisée que moyennant le consentement préalable, libre, spécifique et informé du destinataire des messages.

Quiconque contrevient aux dispositions ci-dessus, est puni d'un emprisonnement de six mois au moins à deux ans au plus et d'une amende de cent mille (100 000) à cinq cent mille (500 000) francs CFA ou de l'une de ces deux peines seulement.

Article 46 : Quiconque émet, dans les cas autorisés, à des fins de prospection directe, des messages au moyen d'automates d'appel, télécopieurs et courriers électroniques, sans indiquer de coordonnées valables auxquelles le destinataire puisse utilement transmettre une demande tendant à obtenir que ces communications cessent, est puni d'un emprisonnement de six mois au moins à deux ans au plus et d'une amende de cent mille (100 000) à cinq cent mille (500 000) francs CFA ou de l'une de ces deux peines seulement.

Est puni des mêmes peines fixées à l'alinéa premier du présent article, quiconque dissimule ou tente de dissimuler l'identité de la personne pour le compte de laquelle la communication est émise et de mentionner un objet sans rapport avec la prestation ou le service proposé.

Article 47 : Tout prestataire qui ne satisfait pas à la demande d'un destinataire de faire cesser l'envoi de messages, à des fins de prospection directe, au moyen d'automates d'appel, télécopieurs ou courriers électroniques, est puni d'un emprisonnement de six mois au moins à deux ans au plus et d'une amende de cent mille (100 000) à cinq cent mille (500 000) francs CFA ou de l'une de ces deux peines seulement.

Chapitre 13 : Des infractions relatives à la cryptologie

Article 48 : Tout prestataire de service de cryptologie qui ne satisfait pas à l'obligation de communiquer à l'agence nationale de sécurité des systèmes d'information une description des caractéristiques techniques du moyen de cryptologie ainsi que le code source des logiciels utilisés, est puni d'un emprisonnement de six mois au moins à deux ans au plus et d'une amende de quatre cent mille (400 000) à deux millions (2 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 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 auprès de l'agence nationale de sécurité des systèmes d'information, est puni d'un emprisonnement de six mois au moins à cinq ans au plus et d'une amende de quatre cent mille (400 000) à cinq millions (5 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 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 de l'agence nationale de sécurité des systèmes d'information est puni d'un emprisonnement d'un an au moins à cinq ans au plus et d'une amende d'un million (1000 000) à vingt millions (20 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 51 : Quiconque fournit des prestations de cryptologie sans avoir obtenu préalablement l'agrément de l'agence nationale de sécurité des systèmes d'information est puni d'un emprisonnement d'un an au moins à cinq ans au plus et d'une amende d'un million (1000 000) à vingt millions (20 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 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 au moins à cinq ans au plus et d'une amende d'un million (1000 000) à vingt millions, (20 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 53 : Quiconque fait obstacle à l'exercice de la mission de contrôle de l'agence nationale de sécurité des systèmes d'information est puni d'un emprisonnement d'un an au moins à cinq ans au plus et d'une amende d'un million (1000 000) à vingt millions (20 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 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 ans au moins à cinq ans au plus et d'une amende de deux millions (2 000 000) à trente millions (30 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Chapitre 14 : De l'adaptation des infractions portant sur les biens aux technologies de l'information et de la communication

Article 55 : Quiconque commet un vol, au sens du code pénal, par le biais des technologies de l'information et de la communication est puni d'un emprisonnement de six mois au moins à cinq ans au plus et d'une amende de quatre cent mille (400 000) à cinq millions (5 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 56 : Quiconque extorque des fonds, des valeurs, une signature, un écrit, un acte, un titre ou une pièce quelconque contenant ou opérant obligation, disposition ou décharge, par le biais des technologies de l'information et de la communication, est puni d'un emprisonnement de six mois au moins à cinq ans au plus et d'une amende de quatre cent mille (400 000) à cinq millions (5 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 57 : Quiconque commet un abus de confiance tel que défini par le code pénal par le biais des technologies de l'information et de la communication, encourt une peine qui peut être au double de celle prévue par le code pénal.

Article 58 : Lorsque l'escroquerie est commise par le biais des technologies de l'information et de la communication, les peines prévues dans le code pénal peuvent être portées au double.

Article 59 : Quiconque trompe ou tente de tromper le destinataire de produits ou de services par le biais des technologies de l'information et de la communication sur l'objèt, l'origine, la nature, la qualité substantielle, la quantité, la teneur ou la composition est puni d'un emprisonnement de six mois au moins à cinq ans au plus et d'une amende de quatre cent mille (400 000) à cinq millions (5 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 60 : Quiconque recèle, en tout ou partie, les choses enlevées, détournées ou obtenues à l'aide d'un crime ou d'un délit, par le biais des technologies de l'information et de la communication, est puni d'un emprisonnement de six mois au moins à cinq ans au plus et d'une amende de quatre cent mille (400 000) à cinq millions (5 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 61 : Quiconque acccomplit intentionnellement un ou plusieurs agissements qualifiés de blanchiment de capitaux, au sens du Règlement n° 01/CEMAC/UMAC/CM du 11 avril 2016 portant prévention et répression du blanchiment des capitaux et du financement du terrorisme et de la prolifération en Afrique centrale, par le biais des technologies de l'information et de la communication, commet un crime punissable de la réclusion de cinq ans au moins à dix ans au plus.

Article 62 : Quiconque accomplit intentionnellement un acte qui constitue une infraction de terrorisme, au sens du Règlement n° 01/CEMAC/UMAC/CM du 11 avril 2016 portant prévention et répression du blanchiment des capitaux et du financement du terrorisme et de la prolifération en Afrique centrale, par le biais des technologies de l'information et de la communication, commet un crime punissable de la réclusion de cinq ans au moins à dix ans au plus.

Article 63 : Quiconque copie ou tente de copier frauduleusement des données informatiques au préjudice d'un tiers est puni d'un emprisonnement de six mois au moins à cinq ans au plus et d'une amende de quatre cent mille (400 000) à cinq millions (5 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 64 : Quiconque, sciemment, recèle, en tout ou partie, des données informatiques enlevées, détournées ou obtenues à l'aide d'un crime ou d'un délit, est puni d'un emprisonnement de six mois au moins à cinq ans au plus et d'une amende de quatre cent mille (400 000) à cinq millions (5 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 65 : Quiconque extorque ou tente d'extorquer des données informatiques dans les conditions définies par le code pénal, est puni d'un emprisonnement de six mois au moins à cinq ans au plus et d'une amende de quatre cent mille (400 000) à cinq millions (5 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 66 : L'application des dispositions des articles 62 à 64 de la présente loi ne fait pas obstacle à la prise en compte des circonstances aggravantes découlant de l'utilisation des technologies de l'information et de la communication prévues aux articles 54 à 59 de la présente loi.

Chapitre 15 : Des infractions commises par tout moyen de diffusion publique

Article 67 : Sont considérés comme moyens de diffusion publique : la radiodiffusion, la télévision, le cinéma, la presse, l'affichage, l'exposition, la distribution d'écrits ou d'images de toutes natures, les discours, chants, cris ou menaces proférés dans les lieux ou réunions

publics, tout procédé technique destiné à atteindre le public et généralement tout moyen de communication numérique par voie électronique.

Article 68 : Est puni d'un emprisonnement de six mois au moins à cinq ans au plus et d'une amende de cinq cent mille (500 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement, quiconque

- fabrique ou détient en vue d'en faire commerce, distribution, location, affichage ou exposition ;
- importe ou fait importer, exporte ou fait exporter, transporte ou fait transporter, sciemment aux mêmes fins ;
- affiche, expose ou projette aux regards du public ;
- vend, loue, met en vente ou en location, même non publiquement ;
- offre, même à titre gratuit, même non publiquement sous quelque forme que ce soit, directement ou par moyen détourné ;
- distribue ou remet en vue de leur distribution par un moyen quelconque, tous imprimés, tous écrits, dessins, affiches, gravures, peintures, photographies, films ou clichés, matrices ou reproductions photographiques, emblèmes, tous objets ou images contraires aux bonnes moeurs.

Article 69 : Lorsque les faits visés à l'article 68 ci-dessus ont un caractère pornographique, le maximum de la peine est prononcé.

Le condamné peut, en outre, faire l'objet, pour une durée ne dépassant pas six mois, d'une interdiction d'exercer, directement ou par personne interposée, en droit ou en fait, des fonctions de direction de toute entreprise d'impression, d'édition ou de groupage et de distribution de journaux et de publication périodiques.

Quiconque contrevient à l'interdiction visée ci-dessus est puni des peines prévues au présent article.

Chapitre 16 : Des atteintes au droit d'auteur et aux droits voisins

Article 70 : Quiconque commet délibérément, à une échelle commerciale et au moyen d'un système d'information, une atteinte au droit d'auteur et aux droits voisins définis par la loi sur le droit d'auteur et les droits voisins, conformément aux obligations que l'Etat a souscrites, à l'exception de tout droit moral conféré par ces conventions, est puni d'un emprisonnement de six mois au moins à cinq ans ou plus et d'une amende de cinq cent mille (500 000) à dix millions (10 00000) de francs CFA ou de l'une de ces deux peines seulement.

Article 71 : Quiconque porte atteinte au droit patrimonial ou au droit moral de l'auteur d'une création informatique, à savoir un programme informatique ou une base de données tels que définis par la loi sur le droit d'auteur et les droits voisins, est puni d'un emprisonnement de six mois au moins à cinq ans au plus et d'une amende de cinq cent mille (500 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Chapitre 17 : De l'usurpation d'identité numérique

Article 72 : Quiconque usurpe l'identité d'un tiers ou une ou plusieurs données permettant de l'identifier, en vue de troubler se tranquillité ou celle d'autrui ou de porter atteinte à son honneur, à sa considération ou à ses intérêts, est puni d'un emprisonnement de six mois au moins à cinq ans au plus et d'une amende de cinq cent mille (500 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Chapitre 18 : Du refus d'assistance

Article 73 : Quiconque, autre que le mis en cause, omet intentionnellement, sans excuse légitime ou justification de se conformer à une réquisition judiciaire donnée, est puni d'un emprisonnement de six mois au moins à trois ans au plus et d'une amende de trois cent mille (300 000) à cinq millions (5 000 000) de francs CFA ou l'une de ces deux peines seulement.

Article 74 : Tout fournisseur de service qui, intentionnellement, sans excuse légitime ou justification, divulgue les informations relatives à une enquête criminelle, alors qu'il a reçu, dans le cadre de cette enquête, une injonction stipulant explicitement que la confidentialité doit être maintenue ou qu'elle résulte de la loi, est puni d'un emprisonnement de six mois au moins à trois ans au plus et d'une amende de trois cent mille (300 000) à cinq millions (5 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Chapitre 19 : Des atteintes à la défense et à la sécurité nationale

Article 75 : Est coupable de trahison et puni des travaux forcés à perpétuité tout Congolais ou étranger qui :

- livre à une puissance étrangère ou à ses agents, sous quelque forme ou par quelque moyen que ce soit un renseignement, objet, document, procédé, une donnée numérisée ou un fichier informatisé qui doit être tenu secret dans l'intérêt de la défense et de la sécurité nationale ;
- s'assure, par quelque moyen que ce soit, la possession d'un tel renseignement, objet, document, procédé, d'une telle donnée informatisée ou d'un tel fichier informatisé en vue de le livrer à une puissance étrangère ou à ses agents ;
- détruit ou laisse détruire un tel renseignement, objet, document, procédé, une telle donnée numérisée ou un tel fichier informatisé en vue de favoriserr une puissance étrangère.

Article 76 : Est coupable de trahison puni des travaux forcés à perpétuité tout Congolais ou tout étranger

qui, dans l'intention de les livrer à tout pays tiers, rassemblera des renseignements, objets, documents, procédés, données ou fichiers informatisés dont la réunion et l'exploitation sont de nature à nuire à la défense et à la sécurité nationale.

Article 77 : Est puni de la peine de réclusion de cinq ans au moins à dix ans au plus, tout Congolais ou étranger qui, sans intention de trahison ou d'espionnage ;

- s'assure, étant sans qualité, la possession d'un renseignement, objet, document, procédé, des données ou fichiers informatisés qui doivent être tenus secrets dans l'intérêt de la défense et de la sécurité nationale ou dont la connaissance pourrait conduire à la découverte d'un secret de la défense et de la sécurité nationale ;
- détruit, soustrait, laisse détruire ou soustraire, reproduit ou laisse reproduire un tel renseignement, objet, document, procédé, une telle donnée ou un tel fichier informatisé ;
- porte ou laisse porter à la connaissance d'une personne non qualifiée ou du public un tel renseignement, objet, document, procédé, de tels données ou fichiers informatisés, ou en étend la divulgation.

Chapitre 20 : De la responsabilité pénale des personnes morales

Article 78 : Les personnes morales autres que l'Etat, les collectivités locales et les établissements publics sont pénalement responsables des infractions prévues par la présente loi, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé :

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

Article 79 : Les personnes morales visées à l'article 78 ci-dessus peuvent être tenues pour responsables lorsque l'absence de surveillance ou de contrôle de la part de leurs organes ou représentants a rendu possible la commission des infractions établies en application de la présente loi pour le compte de ladite personne morale par une personne physique agissant sous leur autorité.

Article 80 : La responsabilité des personnes morales telle que définie aux articles 78 et 79 de la présente loi n'exclut pas celle des personnes physiques auteurs ou complices des même faits.

Article 81 : Peuvent être prononcées contre les personnes » morales, les peines suivantes :

- l'amende égale au quintuple de celle prévue pour les personnes physiques par la loi qui réprime l'infraction ;
- la dissolution, lorsque la personne morale a été créée ou détournée de son objet pour commettre les faits incriminés ;
- l'interdiction définitive ou temporaire ne pouvant dépasser une durée de cinq ans, d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ;
- la fermeture définitive ou temporaire ne pouvant dépasser une durée de cinq ans, d'un ou plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
- l'exclusion des marchés publics à titre définitif ou pour une durée de cinq ans au plus ;
- l'interdiction à titre définitif ou pour une durée de cinq ans au plus de faire appel public à l'épargne ;
- l'interdiction pour une durée de cinq ans au plus d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés, ou d'utiliser des cartes de paiement ;
- 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 de la décision prononcée ou la diffusion de celle-ci soit par la presse écrite soit par tout moyen de communication au public par voie électronique.

Chapitre 21 : De l'adaptation de certaines sanctions aux technologies de l'information et de la communication

Article 82 : En cas de condamnation pour une infraction commise par le biais des technologies de l'information et de la communication, la juridiction peut prononcer à titre de peines complémentaires l'interdiction d'émettre des messages de communication numérique, l'interdiction, à titre provisoire ou définitif, de l'accès au site ayant servi à commettre l'infraction, ou l'injonction d'en couper l'accès par tous moyens techniques disponibles ou même en interdire l'hébergement.

Le juge peut faire injonction à toute personne légalement responsable du site ayant servi à commettre l'infraction ou à toute personne qualifiée de mettre en œuvre les moyens techniques de nature à garantir l'interdiction d'accès, d'hébergement ou la coupure de l'accès au site incriminé.

Article 83 : Quiconque viole les interdictions prononcées par le juge, en application de l'article 82 ci-dessus, est puni d'un emprisonnement de six mois au moins à trois ans au plus et d'une amende de trois cent mille (300 000) à cinq millions (5000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 84 : En cas de condamnation à une infraction commise par le biais des technologies de l'information et de la communication, le juge peut, à titre complémentaire, ordonner la diffusion au frais du condamné, par extrait, de la décision sur ce même support.

Lorsqu'elle est ordonnée, la publication prévue à l'alinéa premier du présent article est exécutée dans les quinze jours suivant le jour où la condamnation est devenue définitive, sous peine d'un emprisonnement de six mois au moins à trois ans au plus et d'une amende de trois cent mille (300 000) à cinq millions (5 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 85 : Dans les cas prévus aux articles 12 à 23 de la présente loi, le juge peut ordonner l'effacement de tout ou partie des données à caractère personnel faisant l'objet du traitement ayant donné lieu à l'infraction.

Article 86 : Sans préjudice des dispositions des articles 48 à 54 de la présente loi, peuvent être prononcées, pour les infractions liées à la cryptologie, les peines complémentaires suivantes :

- la confiscation des outils qui ont servi à commettre l'infraction ou qui en sont le produit ;
- l'interdiction d'exercer une fonction publique ou une activité professionnelle liée à la cryptologiee pour une durée de cinq ans au plus ;
- la fermeture de l'un ou des établissements de l'entreprise ayant servi à commettre les faits incriminés pour une durée de cinq ans au plus ;
- l'exclusion des-marchés publics pour une durée de cinq ans au plus.

Les peines complémentaires s'appliquent à toute personne physique ou morale coupable de l'une des infractions visées au présent article.

TITRE III : DE LA PROCEIDURE EN MATIERE D'INFRACTIONS COMMISES PAR LE BIAIS DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Chapitre 1 : De la preuve électronique en matière pénale

Article 87 : L'écrit électronique en matière pénale est admis pour établir les infractions à la loi pénale sous réserve qu'un tel élément de preuve soit apporté au cours des débats et discuté devant le juge et que puisse être dûment identifiée la personne de qui il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.

Chapitre 2 : De la perquisition et saisie informatique

Article 88 : Lorsque des données stockées dans un système d'information ou dans un support permettant de conserver des données informatisées sur le territoire congolais sont utiles à la manifestation de la vérité, le procureur de la République ou le juge d'instruction peut ordonner une perquisition ou accéder à un système d'information ou à une partie de celui-ci ou dans un autre système d'information, dès lors que ces données sont accessibles à partir du système initial ou disponible pour le système initial.

S'il est préalablement établi que ces données, accessibles à partir du système initial ou disponible pour le système initial, sont stockées dans un autre système d'information situé en dehors du territoire national, elles sont recueillies par le procureur de la République ou le juge d'instruction, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur.

Article 89 : Lorsque le procureur de la République ou le juge d'instruction découvre dans un système d'information 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 procureur de la République ou 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 5 de la présente loi dans le système d'information ou aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système d'information et de garantir leur intégrité.

Lorsque, pour des raisons techniques ou en raison du volume des données, la mesure prévue à l'alinéa 2 du présent article ne peut être prise, le procureur de la République ou le juge d'instruction utilise les moyens techniques appropriés pour empêcher l'accès à ces données dans le système d'information, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système d'information, de même que pour garantir leur intégrité.

Article 90 : 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'y accéder en clair ou sont de nature à compromettre les informations qu'elles contiennent, le procureur de la République ou le juge d'instruction peut réquisitionner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair desdites données.

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

Article 91 : Les personnes physiques ou morales qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité sont tenues de remettre aux officiers de police judiciaire ou aux agents habilités de l'agence nationale de sécurité des systèmes d'information, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies.

Les officiers de police judiciaire et les agents habilités de l'agence nationale de sécurité des systèmes d'information peuvent demander aux fournisseurs des prestations visés à l'alinéa 1 ci-dessus de mettre eux-mêmes en œuvre ces conventions, sauf si ceux-ci démontrent qu'ils ne sont pas en mesure de satisfaire à de telles réquisitions.

Article 92 : 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 d'informations ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, le procureur de la République ou 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.

Article 93 : Le procureur de la République informe le responsable du système d'information de la recherche effectuée dans le système d'information et lui communique une copie des données qui ont été copiées, rendues inaccessibles ou retirées.

Article 94 : Le juge compétent peut à tout moment, d'office ou sur la demande de l'intéressé, ordonner, main levée de la saisie.

Article 95 : L'officier de police judiciaire peut, pour les nécessités de l'enquête et de l'exécution d'une délégation judiciaire, procéder aux opérations prévues aux articles 88 à 99 de la présente loi.

Chapitre 3 : De l'interception de données informatisées relatives au contenu

Article 96 : Si les nécessités de l'enquête l'exigent, le procureur de la République ou 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 d'information ou obliger un fournisseur de services, dans le cadre de ses capacités techniques, à collecter ou à enregistrer lesdites données informatisées, en application de moyens techniques existants, ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer ces données.

Article 97 : Le fournisseur de services désigné à l'article 91 de la présente loi est tenu de garder le secret sur les informations reçues.

Toute violation du secret est punie des peines applicables à l'infraction de violation du secret professionnel, conformément au code pénal.

Chapitre 4 : De la conservation rapide des données informatiques stockées

Article 98 : Si les nécessités de l'enquête l'exigent, notamment lorsqu'il y a des raisons de penser que des données informatisées archivées dans un système d'information sont particulièrement susceptibles de perte ou de modification, le procureur de la République ou le juge d'instruction peut faire injonction à toute personne de conserver et de protéger l'intégrité des données en sa possession ou sous son contrôle, pendant une durée de deux ans maximum, pour la bonne marche des investigations judiciaires.

Le gardien des données ou toute autre personne chargée de les conserver, est tenu de garder le secret sur la mise en œuvre desdites procédures, sous peine des sanctions pénales encourues en matière de-violation du secret professionnel.

Chapitre 5 : De l'injonction de produire

Article 99 : Si les nécessités de l'enquête l'exigent, le procureur de la République ou le juge d'instruction peut faire injonction à toute personne présente sur le territoire congolais de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système d'information ou un support de stockage informatique.

L'injonction de produire peut être adressée, dans les mêmes conditions susmentionnées, à un fournisseur de services offrant des prestations au Congo, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

Chapitre 6 : De la collecte en temps réel des données relatives au trafic

Article 100 : Si les nécessités de l'enquête l'exigent, le procureur de la République ou le juge d'instruction peut utiliser les moyens techniques appropriés pour collecter ou enregistrer, en temps réel, les données relatives au trafic associées à des communications spécifiques, transmises au moyen d'un système d'information.

Le procureur de la République ou le juge d'instruction peut également obliger un fournisseur de services, dans le cadre de ses capacités techniques, à collecter ou à enregistrer, en application des moyens techniques existant, ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données visées à l'alinéa premier du présent article.

Article 101 : Le fournisseur de service désigné à l'alinéa 2 de l'article 100 ci-dessus est tenu de garder le secret sur les informations reçues.

Toute violation du secret est punie des peines applicables à l'infraction de violation du secret professionnel, conformément au code pénal.

Chapitre 7 : De l'utilisation de logiciels à distance

Article 102 : Si les nécessités de l'enquête l'exigent et qu'il y a des motifs raisonnables de croire que des

preuves essentielles ne peuvent pas être collectées suivant les modalités prévues par la présente loi, le juge peut, sur demande, autoriser à l'officier du ministère public ou à un officier de police à utiliser un logiciel à distance et à l'installer dans le système d'information du mis en cause afin de recueillir les éléments de preuve pertinents.

La demande visée à l'alinéa premier du présent article doit contenir les informations suivantes :

- la personne mise en cause, avec, si possible, ses nom et adresse ;
- la description du système d'information ciblé ;
- la description de la mesure envisagée, l'étendue et la durée de l'utilisation ;
- les raisons de la nécessité de l'utilisation du logiciel.

Chapitre 8 : Des mesures particulières concernant la protection des données à caractère personnel

Article 103 : Dans le cas où le juge ordonne, conformément aux dispositions de l'article 85 de 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, les membres et les agents de la commission chargée de la protection des données à caractère personnel sont habilités à constater l'effacement de ces données.

Article 104 : Durant la période allant de l'instruction à l'audience et dans les cas où l'infraction poursuivie concerne les articles 12 à 23 de la présente loi, le procureur de la République ou le juge peut appeler le président de la commission chargée de la protection des données à caractère personnel ou son représentant à déposer ses observations ou à les développer oralement à l'audience.

TITRE IV : DE LA COOPERATION ET DE L'ENTRAIDE JUDICIAIRE INTERNATIONALE

Chapitre 1 : De la coopération internationale

Article 105 : Les modalités d'établissement des conventions de coopération en matière de cybersécurité et de lutte contre la cybercriminalité sont déterminées par voie réglementaire.

Chapitre 2 : De l'entraide judiciaire

Article 106 : A moins qu'une convention internationale à laquelle la République du Congo est partie n'en dispose autrement, les demandes d'entraide émanant des autorités judiciaires congolaises et destinées aux autorités judiciaires étrangères sont transmises par l'intermédiaire du ministère en charge des affaires étrangères.

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

Article 107 : Les demandes d'entraide émanant des autorités judiciaires étrangères et destinées aux autorités judiciaires congolaises sont présentées par la voie diplomatique par le gouvernement étranger intéressé.

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

Article 108 : Les modalités et les conditions de transmission des demandes d'entraide émanant des autorités judiciaires étrangères et destinées aux autorités judiciaires congolaises, ainsi que les règles de procédure régissant leur exécution sont précisées par voie réglementaire

TITRE V : DISPOSITION FINALE

Article 109 : La présente loi 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

- DECRET ET ARRETES -

A - TEXTES GENERAUX

PREMIER MINISTRE, CHEF DU GOUVERNEMENT

Décret n° 2020-145 du 5 juin 2020 portant mise en place d'une commission interministérielle chargée d'assister le Gouvernement dans le choix des gestionnaires délégués des ouvrages de production, de transport, et de distribution du service public de l'électricité

Le Premier ministre, chef du Gouvernement,

Vu la Constitution ;
Vu la loi n° 14-2003 du 10 avril 2003 portant code de l'électricité ;
Vu le décret n° 2010-123 du 19 février 2010 relatif aux attributions du ministre de l'énergie et de l'hydraulique ;
Vu le décret n° 2017-247 du 17 juillet 2017 fixant les modalités de délégation de gestion du service public de l'électricité ;
Vu le décret n° 2017-371 du 21 août 2017 portant nomination du Premier ministre, chef du Gouvernement ;
Vu le décret n° 2017-373 du 22 août 2017 portant nomination des membres du Gouvernement ;
Vu le décret n° 2019-269 du 17 septembre 2019 mettant fin aux fonctions d'un ministre et nommant un nouveau ministre ;
Vu le décret n° 2020-57 du 16 mars 2020 mettant fin aux fonctions d'un ministre et nommant un nouveau ministre ;
Vu le décret n° 2020-58 du 16 mars 2020 portant nomination d'un nouveau ministre délégué,

Décrète :

Article premier : II est mis en place, sous l'autorité du Premier ministre, chef du Gouvernement, une commission interministérielle chargée d'assister le Gouvernement dans le choix des gestionnaires délégués des ouvrages de production, de transport et de distribution du service public de l'électricité.

Article 2 : La commission interministérielle est l'organe de passation des marchés et d'évaluation des offres.

Article 3 : La commission interministérielle comprend une commission de passation des marchés et une sous-commission d'analyse des offres.

Article 4 : La commission des marchés est l'organe chargé de l'ouverture des plis, l'approbation des résultats de l'analyse et de l'évaluation des candidatures, des offres ou des propositions. Elle délibère sous la forme d'un procès-verbal sur les travaux de la sous-commission d'analyse.

Article 5 : La commission de passation des marchés est composée comme suit :

président : le conseiller à l'énergie du Premier ministre ;
rapporteur : le directeur général de l'énergie ;

membres :

- le directeur général du portefeuille public ;
- le représentant du ministère chargé des finances ;
- le représentant du ministère chargé de l'énergie ;
- le directeur général d'énergie électrique du Congo, s.a.

Article 6 : La sous-commission d'analyse des offres est chargée de l'analyse détaillée et de l'évaluation des candidatures, des offres ou des propositions et de leur classement.

Article 7 : La sous-commission d'analyse des offres est composée comme suit :

président : le conseiller à l'énergie du ministre en charge de l'énergie ;
rapporteur : le représentant du ministère chargé du portefeuille public ;

membres :

- le représentant du ministère chargé des finances ;
- le représentant de la direction générale de l'énergie ;
- le représentant de l'agence de régulation du secteur de l'électricité (ARSEL) ;
- le représentant de la société de patrimoine du secteur de l'électricité (Energie Electrique du Congo s.a.) ;
- le secrétaire permanent de la cellule de gestion des marchés publics (CGMP) du ministère chargé de l'énergie.

Article 8 : Les frais de fonctionnement de la commission interministérielle sont à la charge du budget de l'Etat.

Article 9 : Le présent décret sera enregistré et publié au Journal officiel de la République du Congo.

Fait à Brazzaville, le 5 juin 2020

Le Premier ministre, chef du Gouvernement,

Clément MOUAMBA

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'énergie et de l'hydraulique,

Serge Blaise ZONIABA

MINISTERE DES AFFAIRES SOCIALES ET DE L'ACTION HUMANITAIRE

Arrêté n° 6145 du 8 juin 2020 instituant un comité pluri-acteurs chargé de la certification des données issues de l'identification et de l'enregistrement des ménages vulnérables par les autorités locales

Le ministre des affaires sociales
et de l'action humanitaire,

Le ministre de l'intérieur et de la décentralisation,

et

Le ministre des finances et du budget,

Vu la Constitution ;
Vu le décret n° 2017-371 du 21 août portant nomination du Premier ministre, chef du Gouvernement ;
Vu le décret n° 2017-373 du 22 août 2017 portant nomination des membres du Gouvernement ;
Vu le décret n° 2017-404 du 10 octobre 2017 relatif aux attributions du ministre de l'intérieur et de la décentralisation ;
Vu le décret n° 2017-413 du 10 octobre 2017 relatif aux attributions du ministre des affaires sociales et de l'action humanitaire ;
Vu le décret n° 2020-57 du 16 mars 2020 mettant fin aux fonctions d'un ministre et nommant un nouveau ministre ;
Vu le décret n° 2020-58 du 16 mars 2020 portant nomination d'un nouveau ministre délégué ;
Vu le décret n° 2020-88 du 27 mars 2020 portant organisation des intérims des membres du Gouvernement ;
Vu les mesures prises par le Gouvernement sur le coronavirus (COVID-19-P),

Arrêtent :

Article premier : Il est institué, sous la supervision du ministre des affaires sociales et de l'action humanitaire et du ministre de l'intérieur et de la décentralisation, un comité pluri-acteurs chargé de la certification des données issues de l'identification et de l'enregistrement des ménages vulnérables par les autorités locales.

Article 2 : Le comité pluri-acteurs est composé des représentants des entités suivantes :

I. Ministère des affaires sociales et de l'action humanitaire

- unité de gestion du projet Lisungi ;
- directeurs départementaux des affaires sociales.

I. Ministère de l'intérieur et de la décentralisation

- administrateurs-maires d'arrondissements et des communautés urbaines ;
- sous-préfets ;
- maires de communes.

III. Les élus nationaux et locaux des circonscriptions électorales ou administratives concernées.

IV. Confessions religieuses

V. Société civile

Article 3 : Le comité pluri-acteurs est placé sous l'autorité du sous-préfet au niveau du district, de l'administrateur-maire au niveau de l'arrondissement ou de la communauté urbaine et du maire pour ce qui est de la commune.

Article 4 : Les frais de fonctionnement du comité pluri-acteurs sont imputables au budget de l'Etat.

Article 5 : Le présent arrêté sera enregistré et publié au Journal officiel de la République du Congo.

Fait à Brazzaville, le 8 juin 2020

Le ministre des affaires sociales
et de l'action humanitaire,

Antoinette DINGA-DZONDO

Le ministre de l'intérieur et de la décentralisation,

Raymond Zéphirin MBOULOU

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

B -TEXTES PARTICULIERS

MINISTERE DES FINANCES ET DU BUDGET

NOMINATION

Arrêté n° 6143 du 8 juin 2020. portant nomination du personnel du secrétariat permanent du conseil national de mise en œuvre de l'initiative pour la Transparence dans les Industries Extractives

Le ministre des finances et du budget,

Vu la Constitution ;
Vu le décret n° 2019-394 du 28 décembre 2019 portant nomination du secrétaire permanent du comité national de mise en œuvre de l'initiative pour la Transparence dans les Industries Extractives ;
Vu le décret n° 2019-383 du 27 décembre 2019 portant création, attributions, organisation et fonctionnement du Comité national de mise en œuvre de l'Initiative pour la Transparence dans les Industries Extractives ;
Vu le décret n° 2017-371 du 21 août 2017 portant nomination du Premier ministre, chef du Gouvernement ;
Vu le décret n°2017-373 du 22 août 2017 portant nomination des membres du Gouvernement ;
Vu le décret n° 2017-406 du 10 octobre 2017 relatif aux attributions du ministre des finances et du budget ;

Vu le décret n° 2020-58 du 16 mars 2020 portant nomination d'un ministre délégué ;
Vu le décret n° 2020-87 du 27 mars 2020 relatif aux attributions du ministre délégué auprès du ministre des finances et du budget, chargé du budget ;
Vu le décret n° 2020-88 du 27 mars 2020 portant organisation des intérims des membres du Gouvernement ;
Vu l'arrêté n° 5381/MFB/CAB du 19 mars 2020 portant organisation du secrétariat permanent du conseil national de mise en œuvre de l'initiative pour la Transparence dans les Industries Extractives,

Arrête :

Article premier : Les personnes suivantes, sont nommées conformément aux dispositions en vigueur.

Pour l'unité technique et opérationnelle :

- chef de l'unité technique opérationnelle, chargé du suivi et évaluation : M. **MOUTOU (Jean-Claude)** ;

- chargé de projet communication : M. **ATONDI MOMMONDJO (Lecas)** ;

- chargé de projet collecte de données et conciliation : Mme **NGANGOULA (Charlotte)** ;

- chargé de projet suivi des recommandations : Mme **MACKAYA (Carole)**.

Pour l'unité de gestion administrative :

- chef de l'unité de gestion administrative : M. **MOYIKOLI (Perrys)**, cumulativement chargé des systèmes d'information et du site internet ;

- responsable administratif et financier : M. **BANDA (Armel Serge)** ;

- comptable : Mme **NKOUNGOU (Christelle Daisy)** ;

- documentaliste : Mme **OBO (Beutch Carina)**;

- chargé des relations publiques : Mme **KAMARA (Fatou) ;**

- chef d'équipe du personnel d'appui : Mme **NDOURA POUHAUT (Taraise)**

Article 2 : Les intéressés percevront les primes et indemnités prévues par les textes en vigueur.

Article 3 : Le présent arrêté qui entre en vigueur à compter de la date de prise de fonctions des intéressés, sera enregistré, publié au Journal officiel et communiqué partout où besoin sera.

Fait à Brazzaville, le 8 juin 2020

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

MINISTERE DE L'ENERGIE ET DE L'HYDRAULIQUE

AGREMENT

Arrêté n° 6075 du 5 juin 2020 portant attribution d'agrément pour l'exercice des activités de prestations de services et travaux dans le secteur de l'énergie électrique à la société CEGELEC-TPI

Le ministre de l'énergie et de l'hydraulique,

Vu la Constitution ;
Vu la loi n° 14-2003 du 10 avril 2003 portant code de l'électricité ;
Vu le décret n° 2010-808 du 31 décembre 2010 fixant les conditions et les modalités d'exercice des activités de travaux et prestations de services dans le secteur de l'énergie électrique ;
Vu l'arrêté n° 7178/MEH/CAB du 31 octobre 2017 fixant les attributions, la composition et le fonctionnement de la commission ainsi que la procédure d'octroi des agréments du secteur de l'électricité ;
Vu le rapport de la direction générale de l'energie en date du 20 janvier 2020 ;
Vu le procès-verbal de la commission d'agrément en date du 15 mai 2020,

Arrête :

Article premier : Il est attribué à la société CEGELEC-TPI, enregistrée sous le n° RCCM CG/PNR/16 B 848, domiciliée au 250 de l'avenue du Havre, Pointe-Noire, Congo, un agrément pour l'exercice des activités de prestations de services et travaux dans le secteur de l'énergie électrique.

Article 2 : La société CEGELEC-TPI peut soumissionner aux appels d'offres et exercer toute activité de prestations de services et travaux dans le secteur de l'énergie électrique sur l'ensemble du territoire national.

Article 3 : La validité de l'agrément est de trois (3) ans, à compter de sa date de signature.

Article 4 : Le présent agrément ne peut être ni cédé, ni loué, ni transmis à un tiers.

Article 5 : Tout changement affectant le statut de la société agréée devra être notifié sous quinzaine au ministre de l'énergie et de l'hydraulique.

Article 6 : La société CEGELEC-TPI est tenue de respecter les dispositions du présent arrêté ainsi que l'ensemble de la réglementation relative au secteur de l'électricité au Congo.

Sans préjudice des autres voies de droit et de recours, le non-respect de ces dispositions peut entraîner la suspension ou le retrait de l'agrément, après mise en demeure préalable, conformément aux dispositions de l'article 62 du code de l'électricité.

Article 7 : La direction générale de l'énergie est chargée, en ce qui la concerne, de veiller au respect, par la société agréée, des prescriptions du présent arrêté.

Article 8 : Le présent arrêté qui abroge toutes les dispositions antérieures sera enregistré et publié au Journal officiel de la République du Congo.

Fait à Brazzaville, le 5 juin 2020

Serge Blaise ZONIABA

Arrêté n° 6079 du 5 juin 2020 portant attribution d'agrément pour l'exercice des activités de prestations de services et travaux hydrauliques à la société Central BTP

Le ministre de l'énergie et de l'hydraulique,

Vu la Constitution ;
Vu la loi n° 13-2003 du 10 avril 2003 portant code de l'eau ;
Vu le décret n° 2010-809 du 31 décembre 2010 fixant les conditions et les modalités d'exercice des activités de travaux et prestations de services dans le secteur de l'eau et assainissement ;
Vu l'arrêté n° 7179/MEH/CAB du 31 octobre 2017 fixant les attributions, la composition et le fonctionnement de la commission d'agrément ainsi que la procédure d'octroi des agréments du secteur de l'eau ;
Vu le rapport de la direction générale de l'hydraulique en date du 24 février 2020 ;
Vu le procès-verbal de la commission d'agrément en date du 26 mars 2020,

Arrête :

Article premier : Il est attribué à la société Central BTP, enregistrée sous le n° RCCM CG/BZV/01-2009-B12-00015, domiciliée au n° 179, avenue de La Base, Brazzaville (Congo), un agrément pour l'exercice des activités de prestations de services et travaux hydrauliques.

Article 2 : La société Central BTP peut soumissionner aux appels d'offres et exercer toute activité de prestations de services et travaux hydrauliques sur l'ensemble du territoire national.

Article 3 : La validité de l'agrément est de trois (3) ans, à compter de la date de signature.

Article 4 : Le présent agrément ne peut être ni cédé, ni loué, ni transmis à un tiers.

Article 5 : Tout changement affectant le statut de la société agréée devra être notifié sous quinzaine au ministre de l'énergie et de l'hydraulique.

Article 6 : La société Central BTP est tenue de respecter les dispositions du présent arrêté ainsi que l'ensemble de la réglementation relative au secteur de l'eau au Congo.

Sans préjudice des autres voies de droit et de recours, le non-respect de ces dispositions peut entrainer la suspension ou le retrait de l'agrément, après mise en demeure préalable, conformément aux dispositions de l'article 93 du code de l'eau.

Article 7 : La direction générale de l'hydraulique est chargée, en ce qui la concerne, de veiller au respect par la société agréée des dispositions du présent arrêté.

Article 8 : Le présent arrêté qui abroge toutes dispositions antérieures contraires sera enregistré et publié au Journal officiel de la République du Congo.

Fait à Brazzaville, le 5 juin 2020

Serge Blaise ZONIABA

Arrêté n° 6080 du 5 juin 2020 portant attribution d'agrément pour l'exercice des activités de prestations de services et travaux hydrauliques à la société Nocotec

Le ministre de l'énergie et de l'hydraulique,

Vu la Constitution ;
Vu la loi n° 13-2003 du 10 avril 2003 portant code de l'eau ;
Vu le décret n° 2010-809 du 31 décembre 2010 fixant les conditions et les modalités d'exercice des activités de travaux et prestations de services dans le secteur de l'eau et assainissement ;
Vu l'arrêté n° 7179/MEH/CAB du 31 octobre 2017 fixant les attributions, la composition et le fonctionnement de la commission d'agrément ainsi que la procédure d'octroi des agréments du secteur de l'eau ;
Vu le rapport de la direction générale de l'hydraulique en date du 24 janvier 2020 ;
Vu le procès-verbal de la commission d'agrément en date du 26 mars 2020,

Arrête :

Article premier : Il est attribué à la société Nocotec, enregistrée sous le n° RCCM CG/BZV/07B 255, domiciliée au n° 28 bis, rue Oyo, Talangaï, Brazzaville (Congo), un agrément pour l'exercice des activités de prestations de services et travaux hydrauliques.

Article 2 : La société Nocotec peut soumissionner aux appels d'offres et exercer toute activité de prestations de services et travaux hydrauliques sur l'ensemble du territoire national.

Article 3 : La validité de l'agrément est de trois (3) ans, à compter de la date de signature.

Article 4 : Le présent agrément ne peut être ni cédé, ni loué, ni transmis à un tiers.

Article 5 : Tout changement affectant le statut de la société agréée devra être notifié sous quinzaine, au ministre de l'énergie et de l'hydraulique.

Article 6 : La société Nocotec est tenue de respecter les dispositions du présent arrêté ainsi que l'ensemble de la réglementation relative au secteur de l'eau au Congo.

Sans préjudice des autres voies de droit et de recours, le non-respect de ces dispositions peut entraîner la suspension ou le retrait de l'agrément, après mise en demeure préalable, conformément aux dispositions de l'article 93 du code de l'eau.

Article 7 : La direction générale de l'hydraulique est chargée, en ce qui la concerne, de veiller au respect par la société agréée des dispositions du présent arrêté.

Article 8 : Le présent arrêté qui abroge toutes dispositions antérieures contraires sera enregistré et publié au Journal officiel de la République du Congo.

Fait à Brazzaville, le 5 juin 2020

Serge Blaise ZONIABA

Arrêté n° 6081 du 5 juin 2020 portant attribution d'agrément pour l'exercice des activités de prestations de services et travaux hydrauliques à la société Alan Services

Le ministre de l'énergie et de l'hydraulique,

Vu la Constitution ;
Vu la loi n°13-2003 du 10 avril 2003 portant code de l'eau ;
Vu le décret n°2010-809 du 31 décembre 2010 fixant les conditions et les modalités d'exercice des activités de travaux et prestations de services dans le secteur de l'eau et assainissement ;
Vu l'arrêté n° 7179/MEH/CAB du 31 octobre 2017 fixant les attributions, la composition et le fonctionnement de la commission d'agrément ainsi que la procédure d'octroi des agréments du secteur de l'eau ;
Vu le rapport de la direction générale de l'hydraulique en date du 26 février 2020 ;
Vu le procès-verbal de la commission d'agrément en date du 26 mars 2020,

Arrête :

Article premier : Il est attribué à la société Alan Services, enregistrée sous le n°RCCM CG/BZV/17 A 21975, domiciliée au n° 110, rue Mayama, Moungali, Brazzaville (Congo), un agrément pour l'exercice des activités de prestations de services et travaux hydrauliques.

Article 2 : La société Alan Services peut soumissionner aux appels d'offres et exercer toute activité de prestations de services et travaux hydrauliques sur l'ensemble du territoire national.

Article 3 : La validité de l'agrément est de trois (3) ans, à compter de la date de signature.

Article 4 : Le présent agrément ne peut être ni cédé, ni loué, ni transmis à un tiers.

Article 5 : Tout changement affectant le statut de la société agréée devra être notifié sous quinzaine, au ministre de l'énergie et de l'hydraulique.

Article 6 : La société Alan Services est tenue de respecter les dispositions du présent arrêté ainsi que l'ensemble de la réglementationn relative au secteur de l'eau au Congo.

Sans préjudice des autres voies de droit et de recours, le non-respect de ces dispositions peut entraîner la suspension ou le retrait de l'agrément, après mise en demeure préalable, conformément aux dispositions de l'article 93 du code de l'eau.

Article 7 : La direction générale de l'hydraulique est chargée, en ce qui la concerne, de veiller au respect par la société agréée des dispositions du présent arrêté.

Article 8 : Le présent arrêté qui abroge toutes dispositions antérieures contraires sera enregistré et publié au Journal officiel de la République du Congo.

Fait à Brazzaville, le 5 juin 2020

Serge Blaise ZONIABA

Arrêté n° 6082 du 5 juin 2020 portant attribution d'agrément pour l'exercice des activités de prestations de services et travaux hydrauliques à la société Africa Solaire

Le ministre de l'énergie et de l'hydraulique,

Vu la Constitution ;
Vu la loi n° 13-2003 du 10 avril 2003 portant code de l'eau ;
Vu le décret n° 2010-809 du 31 décembre 2010 fixant les conditions et les modalités d'exercice des activités de travaux et prestations de services dans le secteur de l'eau et assainissement ;
Vu l'arrêté n° 7179/MEH/CAB du 31 octobre 2017 fixant les attributions, la composition et le fonctionnement de la commission d'agrément ainsi que la procédure d'octroi des agréments du secteur de l'eau ;
Vu le rapport de la direction générale de l'hydraulique en date du 27 février 2020 ;
Vu le procès-verbal de la commission d'agrément en date du 26 mars 2020,

Arrête :

Article premier : Il est attribué à la société Africa Solaire, enregistrée sous le n° RCCM CG/BZV/10 B-2004, domiciliée au n° 351, rue Moukoukoulou, Moungali, Brazzaville (Congo), un agrément pour l'exercice des activités de prestations de services et travaux hydrauliques.

Article 2 : La société Africa Solaire peut soumissionner

aux appels d'offres et exercer toute activité de prestations de services et travaux hydrauliques sur l'ensemble du territoire national.

Article 3 : La validité de l'agrément est de trois (3) ans, à compter de la date de signature.

Article 4 : Le présent agrément ne peut être ni cédé, ni loué, ni transmis à un tiers.

Article 5 : Tout changement affectant le statut de la société agréée devra être notifié sous quinzaine, au ministre de l'énergie et de l'hydraulique.

Article 6 : La société Africa Solaire est tenue de respecter les dispositions du présent arrêté ainsi que l'ensemble de la réglementation relative au secteur de l'eau au Congo.

Sans préjudice des autres voies de droit et de recours, le non-respect de ces dispositions peut entraîner la suspension ou le retrait de l'agrément, après mise en demeure préalable, conformément aux dispositions de l'article 93 du code de l'eau.

Article 7 : La direction générale de l'hydraulique est chargée, en ce qui la concerne, de veiller au respect par la société agréée des dispositions du présent arrêté.

Article 8 : Le présent arrêté qui abroge toutes dispositions antérieures contraires sera enregistré et publié au Journal officiel de la République du Congo.

Fait à Brazzaville, le 5 juin 2020

Serge Blaise ZONIABA

Arrêté n° 6083 du 5 juin 2020 portant attribution d'agrément pour l'exercice des activités de prestations de services et travaux hydrauliques à la société ISD

Le ministre de l' énergie et de l'hydraulique,

Vu la Constitution ;
Vu la loi n° 13-2003 du 10 avril 2003 portant code de l'eau ;
Vu le décret n° 2010-809 du 31 décembre 2010 fixant les conditions et les modalités d'exercice des activités de travaux et prestations de services dans le secteur de l'eau et assainissement ;
Vu l'arrêté n° 7179/MEH/CAB du 31 octobre 2017 fixant les attributions, la composition et le fonctionnement de la commission d'agrément ainsi que la procédure d'octroi des agréments du secteur de l'eau ;
Vu le rapport de la direction générale de l'hydraulique en date du 11 mars 2020 ;
Vu le procès-verbal de la commission d'agrément en date du 26 mars 2020,

Arrête :

Article premier : Il est attribué à la société ISD, enregistrée sous le n°RCCM CG/BZV/07 B 371, domiciliée au n° 169, avenue de l'amitié, Ravin de la mission, centre-ville, Brazzaville (Congo), un agrément pour les prestations de services et travaux hydrauliques sur l'ensemble du territoire national.

Article 2 : La société ISD peut soumissionner aux appels d'offres et exercer toute activité de prestations de services et travaux hydrauliques sur l'ensemble du territoire national.

Article 3 : La validité de l'agrément est de trois (3) ans, à compter de la date de signature.

Article 4 : Le présent agrément ne peut être ni cédé, ni loué, ni transmis à un tiers.

Article 5 : Tout changement affectant le statut de la société agréée devra être notifié sous quinzaine, au ministre de l'énergie et de l'hydraulique.

Article 6 : La société ISD est tenue de respecter les dispositions du présent arrêté ainsi que l'ensemble de la réglementation relative au secteur de l'eau au Congo.

Sans préjudice des autres voies de droit et de recours, le non-respect de ces dispositions peut entraîner la suspension ou le retrait de l'agrément, après mise en demeure préalable, conformément aux dispositions de l'article 93 du code de l'eau.

Article 7 : La direction générale de l'hydraulique est chargée, en ce qui la concerne, de veiller au respect par la société agréée des dispositions du présent arrêté.

Article 8 : Le présent arrêté qui abroge toutes dispositions antérieures contraires sera enregistré et publié au Journal officiel de la République du Congo.

Fait n Brazzaville, le 5 juin 2020

Serge Blaise ZONIABA

AGREMENT
(RENOUVELLEMENT)

Arrêté n° 6076 du 5 juin 2020 portant renouvellement d'agrément pour l'exercice des activités de prestations de services et travaux dans le secteur de l'énergie électrique à la société ISD

Le ministre de l'énergie et de l'hydraulique,

Vu la Constitution ;
Vu la loi n°14-2003 du 10 avril 2003 portant code de l'électricité ;
Vu le décret n°2010-808 du 31 décembre 2010 fixant les conditions et les modalités d'exercice des activités de travaux et prestations de services dans le secteur de l'énergie électrique ;
Vu l'arrêté n° 7178/MEH/CAB du 31 octobre 2017 fixant les attributions, la composition et le fonctionnement de la commission ainsi que la procédure

d'octroi des agréments du secteur de l'électricité ;
Vu le procès-verbal de la commission d'agrément en date du 15 mai 2020,

Arrête :

Article premier : Il est attribué en renouvellement, à la société ISD, enregistrée sous le n° RCCM CG/BZV/07-8371, domiciliée sur l'avenue Cardinal Emile Biayenda, Brazzaville, Congo, un agrément pour l'exercice des activités de prestations de services et travaux dans le secteur de l'énergie électrique.

Article 2 : La société ISD peut soumissionner aux appels d'offres et exercer toute activité de prestations de services et travaux dans le secteur de l'énergie électrique sur l'ensemble du territoire national.

Article 3 : La validité de l'agrément est de trois (3) ans, à compter de sa date de signature.

Article 4 : Le présent agrément ne peut être ni cédé, ni loué, ni transmis à un tiers.

Article 5 : Tout changement affectant le statut de la société agréée devra être notifié sous quinzaine au ministre de l'énergie et de l'hydraulique.

Article 6 : La société ISD est tenue de respecter les dispositions du présent arrêté ainsi que l'ensemble de la réglementation relative au secteur de l'électricité au Congo.

Sans préjudice des autres voies de droit et de recours, le non-respect de ces dispositions peut entrainer la suspension ou le retrait de l'agrément, après mise en demeure préalable, conformément aux dispositions de l'article 62 du code de l'électricité.

Article 7 : La direction générale de l'énergie est chargée, en ce qui la concerne, de veiller au respect par la société agréée des prescriptions du présent arrêté.

Article 8 : Le présent arrêté qui abroge toutes dispositions antérieures contraires sera enregistré et publié au journal officiel de la République du Congo.

Fait à Brazzaville, le 5 juin 2020

Serge Blaise ZONIABA.

Arrêté n° 6077 du 5 juin 2020 portant renouvellement d'agrément pour l'exercice des activités de prestations de services et travaux dans le secteur de l'énergie électrique à la société CELEC

Le ministre de l'énergie et de l'hydraulique,

Vu la Constitution ;
Vu la loi n° 14-2003 du 10 avril 2003 portant code de l'électricité ;
Vu le décret n° 2010-808 du 31 décembre 2010 fixant les conditions et les modalités d'exercice des activités de travaux et prestations de services dans le secteur de l'énergie électrique ;
Vu l'arrêté n° 7178/MEH/CAB du 31 octobre 2017 fixant les attributions, la composition et le fonctionnement de la commission ainsi que la procédure d'octroi des agréments du secteur de l'électricité ;
Vu le procès-verbal de la commission d'agrément en date du 15 mai 2020,

Arrête :

Article premier : Il est attribué en renouvellement, à la société CELEC, enregistrée sous le n° RCCM CG/BZV/11 B 3079, domiciliée au 179 de l'avenue Foch centre-ville, Brazzaville, un agrément pour l'exercice des activités de prestations de services et travaux dans le secteur de l'énergie électrique.

Article 2 : La société CELEC peut soumissionner aux appels d'offres et exercer toute activité de prestations de services et travaux dans le secteur de l'énergie électrique, sur l'ensemble du territoire national.

Article 3 : La validité de l'agrément est de trois (3) ans, à compter de sa date de signature.

Article 4 Le présent agrément ne peut être ni cédé, ni loué, ni transmis à un tiers.

Article 5 : Tout changement affectant le statut de la société agréée devra être notifié sous quinzaine au ministre de l'energie et de l'hydraulique.

Article 6 : La société CELEC est tenue de respecter les dispositions du présent arrêté ainsi que l'ensemble de la réglementation relative au secteur de l'électricité au Congo.

Sans préjudice des autres voies de droit et de recours, le non-respect de ces dispositions peut entrainer la suspension ou le retrait de l'agrément, après mise en demeure préalable, conformément aux dispositions de l'article 62 du code de l'électricité.

Article 7 : La direction générale de l'énergie est chargée, en ce qui la concerne, de veiller au respect, par la société agréée, des prescriptions du présent arrêté.

Article 8 : Le présent arrêté qui abroge toutes dispositions antérieures contraires sera enregistré et publié au Journal officiel de la République du Congo.

Fait à Brazzaville, le 5 juin 2020

Serge Blaise ZONIABA

Arrêté n° 6078 du 5 juin 2020 portant renouvellement d'agrément pour l'exercice des activités de prestations de services et travaux dans le secteur de l'énergie électrique à la société CEGELEC CG

Le ministre de l'énergie et de l'hydraulique,

Vu la Constitution ;

Vu la loi n° 14-2003 du 10 avril 2003 portant code de l'électricité ;
Vu le décret n° 2010-808 du 31 décembre 2010 fixant les conditions et les modalités d'exercice des activités de travaux et prestations de services dans le secteur de l'énergie électrique ;
Vu l'arrêté n° 7178/MEH/CAB du 31 octobre 2017 fixant les attributions, la composition et le fonctionnement de la commission ainsi que la procédure d'octroi des agréments du secteur de l'électricité ;
Vu le rapport de la direction générale de l'energie en date du 20 janvier 2020 ;
Vu le procès-verbal de la commission d'agrément en date du 15 mai 2020,

Arrête :

Article premier : Il est attribué en renouvellement, à la société CEGELEC-CG, enregistrée sous le n° RCCM CG/PNR/10 B 1711, domiciliée au 250 de l'avenue du Havre Pointe-Noire, Congo, un agrément pour l'exercice des activités de prestations de services et travaux, dans le secteur de l'énergie électrique.

Article 2 : La société CEGELEC-CG peut soumissionner aux appels d'offres et exercer toute activité de prestations de services et travaux dans le secteur de l'énergie électrique sur l'ensemble du territoire national.

Article 3 : La validité de l'agrément est de trois (3) ans, à compter de sa date de signature.

Article 4 : Le présent agrément ne peut être ni cédé, ni loué, ni transmis à un tiers.

Article 5 : Tout changement affectant le statut de la société agréée devra être notifié sous quinzaine au ministre de l'énergie et de l'hydraulique.

Article 6 : La société CEGELEC-CG est tenue de respecter les dispositions du présent arrêté ainsi que l'ensemble de la réglementation relative au secteur de l'électricité au Congo.

Sans préjudice des autres voies de droit et de recours, le non-respect de ces dispositions peut entraîner la suspension ou le retrait de l'agrément, après mise en demeure préalable, conformément aux dispositions de l'article 62 du code de l'électricité.

Article 7 : La direction générale de l'énergie est chargée, en ce qui la concerne, de veiller au respect, par la société agréée, des prescriptions du présent arrêté.

Article 8 : Le présent arrêté qui abroge toutes dispositions antérieures contraires sera enregistré et publié au Journal officiel de la République du Congo.

Fait à Brazzaville, le 5 juin 2020

Serge Blaise ZONIABA

PARTIE NON OFFICIELLE

- ANNONCE -

DECLARATION D'ASSOCIATIONS

Création

Département de Brazzaville

Année 2019

Récépissé n° 060 du 25 février 2019. Déclaration à la préfecture du département de Brazzaville de l'association dénommée : "***ENFANCE MEURTRIE SANS FRONTIERE***", en sigle "***E.M.S.F***". Association à caractère *social*. *Objet* : créer et encourager toute initiative lieu au bien-être physique, moral, social et culturel des enfants meurtris et dispersés ; raviver l'amour dans les cœurs de ces enfants ; mener des actions d'entraide sociale et humanitaire à leur endroit ; créer les centres d'accueil et de formations pour ces enfants. *Siège social* : 15, rue Bihani Sivori, quartier Diata, arrondissement 1 Makélékélé, Brazzaville. *Date de la déclaration : 25 janvier 2019*.

Récépissé n° 343 du 20 novembre 2019. Déclaration à la préfecture du département de Brazzaville de l'association dénommée : "***ESSENCE CONGO***". Association à caractère *socio-culturel* et *éducatif*. Objet : sensibiliser, prévenir et éduquer les jeunes filles sur les maladies sexuellement transmissibles ; promouvoir et développer l'autonomisation de la jeune fille par l'entrepreneuriat féminin. Siège social : case P 14 28, Soprogi Massengo, arrondissement 9 Djiri, Brazzaville. *Date de la déclaration :* 7 novembre 2019.

Imprimé dans les ateliers
de l'imprimerie du Journal officiel
B.P.: 2087 Brazzaville