ASSEMBLEE NATIONALE

CINQUIEME LEGISLATURE

SECRETARIAT GENERAL

Direction des Services Législatifs

Division des Séances et Huissiers

Année 2018
Séance plénière du 06/12/2018

REPUBLIQUE TOGOLAISE

Travail-Liberté-Patrie

LOI N° 2018-026

SUR LA CYBERSECURITE ET LA LUTTE CONTRE LA CYBERCRIMINALITE

PRESIDENCE DE LA REPUBLIQUE

REPUBLIQUE TOGOLAISE
Travail-Liberté-Patrie

LOI N° 2018-026

SUR LA CYBERSECURITE ET LA LUTTE CONTRE LA CYBERCRIMINALITE

L'Assemblée nationale a délibéré et adopté ;
Le Président de la République promulgue la loi dont la teneur suit :

TITRE PREMIER - DISPOSITIONS GENERALES

Article premier : Objet et champ d'application

La présente loi régit le cadre de cybersécurité en République togolaise. Elle met en place un dispositif permettant de prévenir et de faire face aux menaces et risques numériques tout en garantissant la promotion et le développement des technologies de l'information et de la communication.

La présente loi vise également à assurer une protection pénale du système de valeurs de la société de l'information au Togo en mettant en place les mécanismes juridiques et institutionnels appropriés à la lutte contre la cybercriminalité. Elle définit et réprime ainsi les infractions liées à l'utilisation des technologies de l'information et de la communication en République togolaise.

Article 2 : Définitions

Au sens de la présente loi et de ses textes d'application, les différentes expressions suivantes sont définies comme suit :

1) 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 ;

2) Algorithme : suite d'opérations mathématiques élémentaires à appliquer à des données pour aboutir à un résultat désiré ;

3) Algorithme symétrique : algorithme de déchiffrement utilisant une même clé pour chiffrer et déchiffrer les messages ;

4) Algorithme asymétrique : algorithme de chiffrement utilisant une clé publique pour chiffrer et une clé privée (différente) pour déchiffrer les messages ;

5) Attaque active : acte modifiant ou altérant les ressources ciblées par l'attaque (atteinte à l'intégrité, à la disponibilité et à la confidentialité des données) ;

6) Attaque passive : acte n'altérant pas sa cible (écoute passive, atteinte à la confidentialité) ;

7) 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 ;

8) 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 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 ;

9) Authentification : critère de sécurité défini par un processus mis en œuvre notamment pour vérifier l'identité d'une personne physique ou morale et s'assurer que l'identité correspond à l'identité de cette personne préalablement enregistrée ;

10) Chiffrement : toute technique qui consiste à transformer des données numériques en un format inintelligible en employant des moyens de cryptologie ;

11) 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 ;

12) 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 ;

13) Clé publique : clé servant au chiffrement d'un message dans un système asymétrique et donc librement diffusé ;

14) Clé secrète : clé connue de l'émetteur et du destinataire servant de chiffrement et de déchiffrement des messages et utilisant le mécanisme de chiffrement symétrique ;

15) 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 ;

16) Code de conduite : ensemble de règles, notamment les chartes d'utilisation, en conformité avec la présente loi, afin d'instaurer un usage correct des ressources informatiques, des réseaux et des communications électroniques de la structure concernée et homologué par l'Instance de contrôle et de protection des données à caractère personnel ;

17) Commerce électronique : activité commerciale exercée à titre habituel principal ou accessoire, par laquelle une personne effectue ou assure par voie électronique la fourniture de biens, de services et d'informations ou données sous forme électronique, même s'ils ne sont pas rémunérés par ceux qui les reçoivent ; est également considéré comme commerce électronique, tout service consistant à fournir des informations en ligne, des communications commerciales, des outils de recherche, d'accès ou de

récupération de données, d'accès à un réseau de communications ou d'hébergement d'informations, même s'ils ne sont pas rémunérés par ceux qui les reçoivent ;

18) Communication au public par voie électronique : toute mise à disposition du public ou de catégories de public, par un procédé de communication électronique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée ;

19) Communication électronique : les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique ou optique ;

20) Communication électronique indirecte : tout message de texte, de voix, de son, d'image envoyé via un réseau de communications électroniques et stocké sur le réseau ou sur un terminal de communication jusqu'à réception dudit message ;

21) 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 ;

22) 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 ;

23) Contenu illicite : contenu portant atteinte à la dignité humaine, à la vie privée, à l'honneur ou à la sécurité nationale ;

24) Conventions secrètes : les 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 ;

25) Consentement de la personne concernée : toute manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire ou conventionnel accepte que ses données à caractère personnel fassent l'objet d'un traitement manuel ou électronique ;

26) Courrier électronique : tout message, sous forme de texte, de voix, de son ou d'image, envoyé par un réseau public de communications électroniques, stocké sur un serveur du réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier le récupère ;

27) Cryptage : utilisation de codes ou signaux non usuels permettant la conservation des informations à transmettre en des signaux incompréhensibles par les tiers ;

28) Cryptanalyse : ensemble des moyens qui permet d'analyser une information préalablement chiffrée en vue de la déchiffrer ;

29) Cryptogramme : message chiffré ou codé ;

30) 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 ;

31) Cryptologie : la science relative à la protection et à la sécurité des informations notamment pour la confidentialité, l'authentification, l'intégrité et la non répudiation ;

32) Cryptologie (Moyens de) : l'ensemble des outils scientifiques et techniques (matériel ou logiciel) qui permettent de chiffrer et/ou de déchiffrer ;

33) Cryptologie (Prestation de) : toute opération visant la mise en œuvre, pour le compte de soi ou d'autrui, des moyens de cryptologie ;

34) Cryptologie (Activité de) : toute activité ayant pour but la production, l'utilisation, l'importation, l'exportation ou la commercialisation des moyens de cryptologie ;

35) Cybercriminalité : ensemble des infractions s'effectuant à travers le cyberespace par des moyens autres que ceux habituellement mis en œuvre, et de manière complémentaire à la criminalité classique ;

36) Cybersécurité : capacité des réseaux de communications électroniques et des systèmes d'information à résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou traitées, et des services connexes que lesdits réseaux ou systèmes d'information offrent ou rendent accessibles. La cybersécurité est assurée par la mise en œuvre d'un ensemble de mesures de prévention, de protection et de dissuasion d'ordre technique, organisationnel, juridique, financier, humain, procédural et autres actions ;

37) Déchiffrement : opération inverse du chiffrement ;

38) 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 ;

39) 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 ;

40) Dépasser un accès autorisé : le fait d'accéder à un système d'information et d'utiliser un tel accès pour obtenir ou modifier des données dans une partie de l'ordinateur où le titulaire n'est pas autorisé d'accéder ;

41) 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) ;

42) Dispositif de création de signature électronique : ensemble d'éléments logiciels ou matériels permettant la création d'une signature électronique ;

43) Dispositif de vérification de signature électronique : ensemble d'éléments logiciels ou matériels permettant la vérification d'une signature électronique ;

44) Dommage : toute atteinte à l'intégrité ou à la disponibilité des données, d'un programme, d'un système ou d'une information ;

45) 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 ;

46) 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 ;

47) Données de connexion : ensemble de données relatives au processus d'accès dans une communication électronique ;

48) 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 ;

49) Données informatisées : toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique ;

50) Données sensibles : toutes les données à caractère personnel relatives à l'origine raciale ou ethnique, aux opinions ou activités religieuses, philosophiques, politiques, syndicales, à la vie sexuelle, à la santé, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives ;

51) Double criminalité : une infraction punie à la fois dans l'État où un suspect est détenu et dans l'État demandant que le suspect soit remis ou transféré ;

52) 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 ;

53) Equipement d'interception : tout appareil ou dispositif d'interception de communications électroniques ou de captation de données informatiques ;

54) Fournisseur des services de communications électroniques : personne physique ou morale fournissant les prestations consistant entièrement ou principalement en la fourniture de communications électroniques ;

55) Gravité de l'impact : appréciation du niveau de gravité d'un incident, pondéré par sa fréquence d'apparition ;

56) Information : tout élément de connaissance susceptible d'être représenté et exprimé sous forme écrite, visuelle, sonore, numérique, ou autre à l'aide de conventions pour être utilisé, conservé, traité ou communiqué ;

57) Infrastructure essentielle : réseau de communications électroniques ou système d'information indispensable à la fourniture des services essentiels ;

58) 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 ;

59) 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 ;

60) Interception légale : accès autorisé aux données d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal ;

61) Interconnexion des données à caractère personnel : tout mécanisme de connexion consistant en la mise en relation de données traitées pour une finalité déterminée avec d'autres données traitées pour des finalités identiques ou non, ou liées par un ou plusieurs responsables de traitement ;

62) Intrusion par intérêt : accès intentionnel et sans droit dans un réseau de communications électroniques ou dans un système d'information, dans le but soit de nuire soit de tirer un bénéfice économique, financier, industriel, sécuritaire ou de souveraineté ;

63) Intrusion par défi intellectuel : accès intentionnel et 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 ;

64) 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 ;

65) Logiciel potentiellement indésirable : logiciel représentant des caractéristiques d'un logiciel trompeur ou d'un logiciel espion ;

66) 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 ;

67) Message clair : version intelligible d'un message et compréhensible par tous ;

68) Mineur ou Enfant : toute personne physique âgée de moins de 18 ans au sens de la Charte Africaine sur les droits et le bien-être de l'Enfant et de la convention des Nations Unies sur les droits de l'enfant ;

69) Moyen de cryptographie : équipement ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser 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 ;

70) Moyen de paiement électronique : moyen permettant à son titulaire d'effectuer des opérations de paiement électronique ;

71) 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 ;

72) Opérateur de services essentiels : tout opérateur, public ou privé, offrant des services essentiels au fonctionnement de la société ou de l'économie et dont la continuité pourrait être gravement affectée par des incidents touchant les réseaux de communications électroniques ou systèmes d'information nécessaires à la fourniture desdits services ;

73) Politique de sécurité : référentiel de sécurité établi par une organisation, reflétant sa stratégie de sécurité et spécifiant les moyens de la réaliser ;

74) Pornographie infantile : toute représentation visuelle d'un comportement sexuellement explicite y compris toute photographie, film, vidéo, image que ce soit fabriquée ou produite par voie électronique, mécanique ou par autres moyens où :

   a) la production de telles représentations visuelles implique un mineur ;

   b) ces représentations visuelles sont une image numérique, une image d'un ordinateur ou une image générée par un ordinateur où un mineur est engagé dans un comportement sexuellement explicite ou lorsque des images de leurs organes sexuels sont produites ou utilisées à des fins principalement sexuelles et exploitées à l'insu de l'enfant ou non ;

   c) cette représentation visuelle a été créée, adaptée ou modifiée pour qu'un mineur s'engage dans un comportement sexuellement explicite ;

75) Prestataire de services de cryptologie : toute personne, physique ou morale, qui fournit une prestation de cryptologie ;

76) Personne concernée : toute personne physique qui fait l'objet d'un traitement des données à caractère personnel ;

77) Prospection directe : tout envoi de message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services ; elle vise aussi toute sollicitation effectuée au moyen de l'envoi de message, quel qu'en soit le support ou la nature notamment commerciale, politique ou caritative, destinée à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services ;

78) Raciste et xénophobe en matière des technologies de l'information et de la communication : tout matériel écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance, de l'origine nationale ou ethnique ou de la religion ;

79) Services essentiels : tout service essentiel pour la sûreté publique, la défense nationale, la stabilité économique, la sécurité nationale, la stabilité internationale et pour la pérennité et la restauration du cyberespace critique ;

80) Sécurité : situation dans laquelle quelqu'un, quelque chose n'est exposé à aucun danger. Mécanisme destiné à prévenir un événement dommageable ou à en limiter les effets ;

81) Signature électronique : une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de procédé d'identification ;

82) Sous-traitant : toute personne physique ou morale, publique ou privée, tout autre organisme ou association qui traite des données pour le compte du responsable du traitement ;

83) 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 ;

84) 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 ;

85) Système 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 informatiques, ainsi que les données informatiques traitées, stockées, récupérées ou transmises par ce dispositif ou cet ensemble de dispositifs en vue du fonctionnement, de l'utilisation, de la protection ou de la maintenance de celui-ci ;

86) Vulnérabilité : défaut de sécurité 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.

TITRE II - PROMOTION DE LA CYBERSECURITE

CHAPITRE I^er^ - CADRE POLITIQUE ET STRATEGIQUE DE LA CYBERSECURITE

Article 3 : Politique nationale de cybersécurité

Le gouvernement, en collaboration avec toutes les parties prenantes et par le biais des ministères chargés de l'économie numérique et de la sécurité, définit la politique nationale de cybersécurité.

La politique nationale de cybersécurité identifie et reconnait l'importance des infrastructures essentielles pour la nation. Elle identifie en outre les risques auxquels les infrastructures essentielles sont confrontées. Enfin, la politique nationale de cybersécurité définit, dans les grandes lignes, les objectifs de l'Etat en matière de cybersécurité ainsi que les modalités selon lesquelles de tels objectifs sont mis en œuvre.

Les opérateurs de services essentiels sont soumis à des règles de sécurité destinées à assurer la protection de leurs infrastructures essentielles.

Un décret fixe les conditions et modalités selon lesquelles les opérateurs de services essentiels sont désignés et selon lesquelles les infrastructures essentielles sont déterminées.

Les règles de cybersécurité, au respect desquelles les opérateurs de services essentiels sont tenus, sont définies par décret en conseil des ministres.

Article 4 : Stratégies nationales de cybersécurité

Pour assurer la mise en œuvre de la politique nationale de cybersécurité, les ministères chargés de la sécurité et de l'économie numérique définissent et mettent en œuvre les stratégies appropriées et suffisantes, en tenant compte de l'évolution technologique et des priorités du gouvernement dans ce domaine.

Les stratégies nationales de cybersécurité peuvent notamment être constituées autour des axes suivants :

1) les réformes du dispositif juridique et institutionnel indispensables à l'amélioration et au développement du cadre de la cybersécurité ;
2) la promotion d'un leadership national pour le développement de la culture de la sécurité ;
3) la promotion d'une culture de la cybersécurité chez toutes les parties prenantes ;
4) la sensibilisation et le développement des capacités des acteurs clés ;
5) les mécanismes de renforcement de la souveraineté numérique ;
6) le partenariat public-privé et la coopération internationale.

Les stratégies nationales de cybersécurité établissent des structures organisationnelles et fixent des objectifs ainsi que des délais pour mener à bien tous les aspects de la politique de cybersécurité, tout en posant les bases d'une gestion effective des volets prévention, protection, détection et riposte relatifs aux incidents de cybersécurité.

CHAPITRE II - CADRE DE GOUVERNANCE DE LA CYBERSECURITE

Article 5 : Autorités gouvernementales de gouvernance de la cybersécurité

Le ministère chargé de la sécurité est l'autorité gouvernementale en matière de cybersécurité. Il assure en collaboration avec le ministère chargé de l'économie numérique, la gouvernance stratégique de la cybersécurité en République togolaise.

Article 6 : Agence nationale de la cybersécurité

Il est créé une personne morale de droit public dotée de la personnalité juridique et de l'autonomie financière, assurant une mission d'utilité publique dénommée « Agence nationale de la cybersécurité », en abrégé « ANCy ». L'Agence nationale de la cybersécurité est placée sous la tutelle du ministère chargé de la sécurité et du ministère chargé de l'économie numérique.

L'Agence nationale de la cybersécurité est l'autorité nationale en matière de sécurité des infrastructures essentielles et des systèmes d'information des autorités publiques. Elle concourt de manière significative à la définition et à la mise en œuvre de la politique et des orientations stratégiques en matière de cybersécurité. Elle apporte son concours aux services de la République togolaise en matière de défense et de sécurité nationale.

A ce titre, l'Agence nationale de la cybersécurité :

1) assure la fonction d'autorité nationale de défense des infrastructures essentielles et des systèmes d'information des autorités publiques. En cette qualité, elle :

   a) propose aux autorités gouvernementales compétentes les mesures destinées à répondre aux crises affectant ou menaçant la sécurité des infrastructures essentielles ou des systèmes d'information des autorités publiques ;

   b) coordonne, dans le cadre des orientations fixées par les autorités gouvernementales compétentes, l'action gouvernementale en matière de défense des systèmes d'information ;

2) conçoit, fait réaliser et met en œuvre les moyens interministériels sécurisés de communications électroniques nécessaires au Président de la République et au gouvernement ;

3) anime et coordonne les travaux interministériels en matière de sécurité des systèmes d'information ;

4) désigne les opérateurs de services essentiels ;

5) vérifie la pertinence et l'exhaustivité des listes d'infrastructures essentielles ;

6) fixe les règles relatives aux mesures de protection à mettre en œuvre par les opérateurs de services essentiels pour assurer la cybersécurité de leurs infrastructures essentielles et veille par des contrôles au respect desdites règles par les opérateurs de services essentiels ;

7) octroie des accréditations aux opérateurs de services essentiels qui respectent les règles qui leur incombent en matière de cybersécurité ;

8) fixe les conditions financières de réalisation des contrôles et de délivrance des accréditations ;

9) prononce des astreintes et sanctions, y compris pécuniaires, à l'encontre des opérateurs de services essentiels qui ne respectent pas leurs obligations en termes de cybersécurité ;

10) mène des inspections et audits des systèmes d'information des services de l'Etat et des infrastructures essentielles des opérateurs de services essentiels ;

11) met en œuvre un système de détection et d'évaluation des menaces ou des évènements susceptibles d'affecter la sécurité des systèmes d'information de l'Etat et coordonne la réaction à ces évènements ; elle apporte son concours pour répondre à ces incidents ;

12) recueille les informations techniques relatives aux incidents affectant les infrastructures essentielles des opérateurs de services essentiels et les systèmes d'information de l'Etat ;

13) délivre des agréments aux dispositifs et aux mécanismes de sécurité destinés à protéger, dans les systèmes d'information, les informations couvertes par le secret de la défense nationale ;

14) certifie les dispositifs matériels ou logiciels et les services informatiques au regard de leur capacité à assurer des fonctions de cybersécurité ;

15) participe aux négociations internationales et assure la liaison avec ses homologues étrangers ;

16) assure la sensibilisation du public et la formation des personnels qualifiés dans le domaine de la sécurité des systèmes d'information ;

17) assure la création d'une structure d'alerte et d'assistance sur l'Internet placée auprès de l'ANCy, chargée d'une mission de veille et de réponse aux attaques informatiques des systèmes d'information.

18) effectue des contrôles destinés à vérifier le respect par les opérateurs de services essentiels des obligations qui leur incombent et à les sanctionner en cas de non-respect ;

Les modalités de contrôle et les sanctions applicables en cas de non-respect sont définies par décret en conseil des ministres.

Les attributions et missions ainsi que les modalités d'organisation et de fonctionnement de l'Agence nationale de la cybersécurité sont précisées par décret en conseil des ministres.

Article 7 : Fonds de souveraineté numérique

Il est créé un Fonds de souveraineté numérique dont l'ordonnateur est le ministre chargé de l'économie numérique. Le Fonds de souveraineté numérique participe, entre autres, au financement des stratégies nationales de cybersécurité et appuie les actions de l'Agence nationale de la cybersécurité. Un décret en conseil des ministres définit les modalités de son fonctionnement et de son financement.

TITRE III - LUTTE CONTRE LA CYBERCRIMINALITE

CHAPITRE I^er^ - INFRACTIONS ET PEINES EN MATIERE DE CYBERCRIMINALITE

Section 1^ere^ : Atteintes aux systèmes informatiques

Article 8 : Accès et maintien frauduleux *à* un système informatique

Est punie d'une peine d'emprisonnement de six (6) mois à deux (2) ans et d'une amende cinq millions (5 000 000) à vingt millions (20 000 000) de francs CFA ou de l'une de ces deux (2) peines, toute personne qui, sans droit, accède ou tente d'accéder, se maintient ou tente de se maintenir dans tout ou partie d'un système informatique.

Les peines prévues à l'alinéa précédent sont portées au double lorsqu'il en est résulté une perturbation grave ou interruption de ce système informatique.

Lorsque l'infraction au présent article est commise au préjudice de l'Etat togolais, les peines encourues sont portées à cinq (5) ans d'emprisonnement et à une amende de quinze millions (15 000 000) à soixante millions (60 000 000) de francs CFA.

Article 9 : Entrave au fonctionnement d'un système informatique

Est punie d'une peine d'emprisonnement de trois (3) à cinq (5) ans et d'une amende de vingt-cinq millions (25 000 000) à cent millions (100 000 000) de francs CFA, toute personne qui, avec ou

sans droit détruit, entrave, fausse, perturbe, interrompt le fonctionnement d'un système informatique.

Article 10 : Atteinte aux données informatisées

Est punie d'une peine d'emprisonnement de trois (3) à cinq (5) ans et d'une amende de vingt-cinq millions (25 000 000) à cent millions (100 000 000) de francs CFA, toute personne qui, avec ou sans droit :

1) introduit, supprime ou modifie les données informatiques d'un système informatique ;
2) détruit, détériore, altère, rend inaccessibles ou endommage ces données ;
3) soustrait ces données pour son usage personnel ou pour les céder à un tiers, à titre onéreux ou gratuit ;
4) détruit, entrave, fausse, perturbe, interrompt le fonctionnement d'un système informatique.

Est punie des mêmes peines, toute personne qui intercepte frauduleusement par des moyens techniques des données informatisées lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système informatique.

Lorsque l'infraction définie au présent article est commise au préjudice de l'Etat togolais, son auteur est puni d'une peine de vingt (20) à trente (30) ans de réclusion criminelle et d'une amende de cinquante millions (50 000 000) à cent cinquante millions (150 000 000) de francs CFA.

Section 2 : Infractions se rapportant au contenu

Article 11 : Production d'une image ou d'une représentation à caractère pornographique infantile

Est punie d'une peine de cinq (5) à dix (10) ans de réclusion criminelle et d'une amende de dix millions (10 000 000) à vingt cinq (25 000 000) de francs CFA ou de l'une de ces deux (2) peines, toute personne qui produit ou enregistre, offre, met à disposition, diffuse, transmet une image ou une représentation présentant un caractère de pornographie mettant en scène un ou plusieurs enfants âgés de moins de quinze (15) ans par le biais d'un système informatique ou par tout autre procédé technique quelconque.

Article 12 : Importation ou exportation d'une image ou d'une représentation à caractère pornographique infantile

Est punie de cinq (5) à dix (10) ans de réclusion criminelle et d'une amende de vingt cinq millions (25 000 000) à cinquante millions (50 000 000) de francs CFA ou de l'une de ces deux (2) peines, toute personne qui se procure ou procure à autrui, importe ou fait importer, exporte ou fait exporter une image ou une représentation présentant un caractère pornographique mettant en scène un ou plusieurs enfants âgés de moins de quinze (15) ans par le biais d'un système informatique ou par tout autre procédé technique quelconque.

Article 13 : Possession d'une image ou d'une représentation à caractère pornographique infantile

Est punie d'une peine d'emprisonnement de six (6) mois à trois (3) ans 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 (2) peines, toute personne qui sciemment, possède des images ou représentations présentant un

caractère pornographique mettant en scène un ou plusieurs enfants âgés de moins de quinze (15) ans dans un système informatique ou dans un moyen quelconque de stockage de données informatisées.

Article 14 : Facilitation d'accès à des images, des documents, du son ou une représentation présentant un caractère de pornographie à un mineur

Toute personne qui sciemment, facilite l'accès à des images, des documents, du son ou une représentation présentant un caractère de pornographie à un mineur, est punie de d'un (1) à trois (3) ans d'emprisonnement et d'une amende d'un million (1 000 000) à quinze millions (15 000 000) de francs CFA ou de l'une de ces deux (2) peines.

Article 15 : Disposition d'écrits ou d'images de nature raciste ou xénophobe par le biais d'un système informatique

Quiconque crée, télécharge, diffuse ou met à disposition sous quelque forme que ce soit des écrits, messages, photos, dessins ou toute autre représentation d'idées ou de théories, de nature raciste ou xénophobe, par le biais d'un système informatique, est puni de six (6) mois à deux (2) ans et d'une amende de cinq cent mille (500 000) à deux millions (2 000 000) de francs CFA ou de l'une de ces deux peines.

Toute personne qui, par tout moyen de communication, incite à la discrimination, est punie d'une peine d'emprisonnement de six (6) mois à deux (2) an(s) et d'une amende d'un million (1 000 000) à trois millions (3 000 000) de francs CFA ou de l'une de ces deux (2) peines.

Article 16 : Menace par le biais d'un système informatique

La menace effectuée par le biais d'un système informatique visant à commettre une infraction pénale envers une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, 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 punie de six (6) mois à deux (2) ans d'emprisonnement et d'une amende de cent mille (100 000) à cinq cent mille (500 000) francs CFA ou de l'une de ces deux (2) peines.

Lorsqu'il s'agit d'une menace de mort, la peine est de trois (3) à cinq (5) ans d'emprisonnement et de cent mille (100 000) à cinq cent mille (500 000) francs CFA d'amende ou de l'une de ces deux (2) peines.

Lorsque la menace est faite avec ordre ou sous condition d'accomplir ou laisser accomplir un acte illicite ou préjudiciable à autrui, la peine est d'un (1) an à trois (3) an(s) d'emprisonnement et de cent mille (100 000) à cinq cent mille (500 000) francs CFA d'amende ou de l'une de ces deux (2) peines.

Article 17 : Injure commise par le biais d'un système informatique

L'injure commise par le biais d'un système informatique envers une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, 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 punie de six (6) mois à deux (2) ans d'emprisonnement et d'une amende de

cinq cent mille (500 000) à deux millions (2 000 000) de francs CFA ou de l'une de ces deux (2) peines.

Article 18 : Négationnisme

Quiconque nie, approuve ou justifie intentionnellement des actes constitutifs de génocide ou de crimes contre l'humanité par le biais d'un système informatique, est puni de cinq (5) à dix (10) ans de réclusion criminelle et d'une amende de vingt-cinq millions (25 000 000) à cent millions (100 000 000) de francs CFA.

Section 3 : Adaptation des infractions classiques aux technologies de l'information et de la communication

Article 19 : Vol d'information ou de données

La soustraction frauduleuse d'information ou de données au préjudice d'autrui est assimilée au vol et est punie conformément aux peines prévues par le code pénal.

Article 20 : Circonstances aggravantes

Le fait d'utiliser les technologies de l'information et de la communication ou d'agir en bande organisée en vue de commettre des infractions de droit commun comme le vol, l'escroquerie, le recel, l'abus de confiance, constitue une circonstance aggravante de ces infractions au sens de la présente loi.

Lorsque les infractions visées au premier alinéa du présent article ont été commises par le biais d'un système informatique, les peines prévues dans le code pénal ou autre texte législatif en vigueur pour les sanctionner peuvent être portées au double.

Lorsque les infractions ont été commises par le biais d'un système informatique, il ne peut être prononcé le sursis à l'exécution

Article 21 : Acte de terrorisme au moyen des TIC

Quiconque utilise ou tente d'utiliser les technologies de l'information et de la communication en vue de commettre un ou des actes de terrorisme, est puni de dix (10) à vingt (20) ans de réclusion criminelle et d'une amende de cinq millions (5 000 000) à dix millions (10 000 000) de francs CFA.

Toute personne complice de la commission de l'infraction prévue au premier alinéa du présent article ou transmet des informations et données à un groupe terroriste est punie des mêmes peines.

Article 22 : Acte de terrorisme visant les logiciels et programmes informatiques

Quiconque commet ou tente de commettre un ou des actes de terrorisme visant des logiciels et/ou programmes informatiques, est puni de dix (10) à vingt (20) ans de réclusion criminelle et d'une amende de cinq millions (5 000 000) à dix millions (10 000 000) de francs CFA.

Toute personne complice de la commission de l'infraction prévue au premier alinéa du présent article est punie des mêmes peines.

Article 23 : Diffusion de procédés ou de moyens de destruction à des fins de terrorisme

Est punie de cinq (5) à dix (10) ans de réclusion criminelle et de trois millions (3.000.000) à cinq millions (5.000.000) de francs CFA d'amende, toute personne qui diffuse ou met à la disposition d'autrui par le biais d'un système informatique, sauf à destination des personnes autorisées, un mode d'emploi ou un procédé, permettant la fabrication des armes à feu, de leurs pièces, éléments et munitions de nature à porter atteinte à la vie humaine, aux biens ou à l'environnement.

Est punie des mêmes peines, toute personne qui diffuse ou met à la disposition d'autrui par le biais d'un système informatique, sauf à destination des personnes autorisées, un mode d'emploi ou un procédé, permettant l'emploi, la fabrication et le stockage des armes non conventionnelles de nature à porter atteinte à la vie humaine, aux biens ou à l'environnement.

Article 24 : Incitation au suicide

Quiconque diffuse ou met à la disposition d'autrui par le biais d'un système informatique, un mode d'emploi, des informations ou procédés d'incitation au suicide, est puni d'un (1) à trois (3) an(s) d'emprisonnement et d'une amende d'un million (1 000 000) à cinq millions (5 000 000) de francs CFA ou de l'une de ces deux peines. Toute personne complice de la commission de l'infraction prévue au premier alinéa du présent article est punie des mêmes peines.

Article 25 : Diffusion de fausses nouvelles tendant à faire croire à une situation d'urgence

Quiconque communique ou divulgue par le biais d'un système informatique, une fausse information tendant à faire croire qu'une destruction, une dégradation ou une détérioration de biens ou une atteinte aux personnes a été commise ou va être commise ou toute autre situation d'urgence, est puni d'un (1) à trois (3) an (s) d'emprisonnement et d'un million (1 000 000) à trois millions (3 000 000) de francs CFA d'amende ou de l'une de ces deux (2) peines.

Toute personne complice de la commission de l'infraction prévue au premier alinéa du présent article est punie des mêmes peines.

Article 26 : Menace de commettre un acte terroriste

Quiconque menace de commettre par le biais d'un système informatique, une destruction, une dégradation ou une détérioration de biens ou une atteinte aux personnes, lorsqu'une telle menace est matérialisée par un écrit, une image, une vidéo, un son ou toute autre donnée, est coupable de menace terroriste et est puni de trois (3) à cinq (5) ans d'emprisonnement et d'une amende de cent mille (100 000) à cinq cent mille (500 000) francs CFA ou de l'une de ces deux (2) peines.

Toute personne complice de la commission de l'infraction prévue au premier alinéa du présent article est punie des mêmes peines.

Section 4 : Infractions commises par tous moyens de diffusion publique

Article 27 : Atteinte aux bonnes mœurs par des moyens de diffusion publique

Quiconque :

1) fabrique ou détient aux fins de commerce, distribution, location, affichage ou exposition ;

2) importe ou fait importer, exporte ou fait exporter, transporte ou fait transporter sciemment aux mêmes fins ;

3) affiche, expose ou projette aux regards du public ;

4) vend, loue, met en vente ou en location, même non publiquement ;

5) offre, même à titre gratuit, même non publiquement sous quelque forme que ce soit, directement ou par moyen détourné ;

6) 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 mœurs, est puni d'une peine d'emprisonnement de six (6) mois à deux (2) ans et d'une amende de cinq cent mille (500 000) à deux millions (2 000 000) de francs CFA ou de l'une de ces deux (2) peines.

Le maximum de la peine est prononcé lorsque les faits visés à l'alinéa premier du présent article ont un caractère pornographique.

Le condamné peut en outre faire l'objet, pour une durée ne dépassant pas six (6) 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 périodique.

Quiconque contrevient à l'interdiction visée à l'alinéa 3 du présent article est puni des peines prévues au présent article.

Article 28 : Atteinte à la dignité humaine

Quiconque produit, diffuse ou met à la disposition d'autrui des données de nature à troubler l'ordre ou la sécurité publique ou à porter atteinte à la dignité humaine ou à l'intimité et à la vie privée d'une personne par le biais d'un système informatique, d'un mode d'emploi, des informations ou procédés d'incitation au suicide, est puni de six (6) mois à deux (2) ans d'emprisonnement et d'une amende de deux millions (2 000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux (2) peines .

Toute personne complice de la commission de l'infraction prévue au premier alinéa du présent article est punie des mêmes peines.

Section 5 : Atteintes à la sécurité publique et à la défense nationale

Article 29 : Trahison

Est puni du maximum de la réclusion criminelle à temps pour trahison tout togolais, qui :

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

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

3) détruit ou laisse détruire un tel renseignement, objet, document, procédé, donnée numérisée ou fichier informatisé en vue de favoriser une puissance étrangère.

Article 30 : Atteinte au secret de défense nationale

Est puni d'une peine d'emprisonnement de trois (3) à cinq (5) ans et d'un million (1 000 000) à cinq millions (5 000 000) de francs CFA d'amende, tout togolais ou tout étranger qui, dans l'intention de les livrer à tout pays tiers, rassemble des renseignements, objets, documents, procédés, données, logiciels, programmes ou fichiers informatisés dont la réunion et l'exploitation sont de nature à nuire à la défense nationale.

Est puni de cinq (5) à dix (10) ans de réclusion criminelle et d'un million (1 000 000) à cinq millions (5 000 000) de francs CFA d'amende, tout gardien, tout dépositaire, par fonction ou par qualité, d'un renseignement, objet, document, procédé, donnée, logiciel, programme ou fichier informatisé qui doit être tenu secret dans l'intérêt de la défense nationale ou dont la connaissance pourrait conduire à la découverte d'un secret de défense nationale, qui sans intention de trahison ou d'espionnage, l'a :

3) détruit, soustrait, laissé détruire ou soustraire, reproduit ou fait reproduire ;
4) porté ou laissé porter à la connaissance d'une personne non qualifiée ou du public.

Lorsque le gardien ou le dépositaire a agi par maladresse, imprudence, inattention, négligence ou inobservation des règlements, l'infraction est punie d'une peine d'un (1) à cinq (5) an(s) d'emprisonnement et de cinq cent mille (500 000) à un million (1 000 000) de francs CFA d'amende.

Article 31 : Espionnage

Est puni du maximum de la réclusion criminelle à temps tout étranger qui, à tout moment, initie ou entretient des intelligences avec un togolais pour favoriser l'un des actes de trahison visés à l'article 29 de la présente loi.

Article 32 : Atteinte aux infrastructures essentielles

Quiconque commet l'une des infractions définies aux articles 8 à 10 de la présente loi en atteinte à un ou des systèmes informatiques protégés, considérés comme infrastructure essentielles et/ou en raison des données critiques de sécurité nationale qu'ils contiennent, est puni du maximum de la réclusion criminelle à temps.
L'infraction d'atteinte à une infrastructure essentielle visée à l'alinéa premier du présent article inclut le fait de dépasser un accès autorisé.

Article 33 : Entrave à l'action des autorités nationales en charge de la cybersécurité

Est puni d'une peine d'emprisonnement de six (6) mois à trois (3) ans et d'une amende de cinq cent mille (500 000) francs CFA à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines, quiconque entrave l'action des autorités nationales en charge de la cybersécurité ou de leur mandataire, soit :

- en s'opposant à l'exercice des missions confiées à leurs membres ou agents habilités ;
- en refusant de communiquer à leurs membres ou agents habilités, les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître ;

- 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.

Section 6 : Autres infractions en matière de cybercriminalité

Article 34 : Disposition d'un équipement pour commettre des infractions

La production, la commercialisation, la fourniture ou la maintenance d'outils, d'équipements, de programmes informatiques, de dispositifs, de données, de mots de passe, codes d'accès ou données informatisées similaires, conçus ou destinés à commettre les délits et les crimes visés au présent chapitre, lorsqu'on ne peut méconnaître l'usage délictueux ou criminel qui peut en être fait par nature ou par destination, est punie d'une peine d'emprisonnement d'un (1) à cinq (5) an(s) et d'une amende de cinq millions (5 000 000) à cinquante millions (50 000.000) de francs CFA.

Lorsque l'infraction définie au présent article a été commise au préjudice de l'Etat togolais, les peines encourues sont portées à dix (10) ans de réclusion criminelle et à une amende de deux cent millions (200 000 000) de francs CFA.

Article 35 : Participation à une association formée ou à une entente en vue de commettre des infractions informatiques

La commission en bande organisée des délits visés dans la présente loi est punie du doublement du maximum des peines encourues pour ces infractions.

Lorsque l'Etat togolais a été victime de ces infractions commises en bande organisée, la peine de réclusion criminelle est portée à trente (30) ans et les amendes au quintuple du maximum encouru.

Section 7 : Adaptation du régime de responsabilité pénale et de certaines sanctions à l'environnement numérique

Article 36 : Responsabilité des personnes morales

Les personnes morales, autres que l'Etat, les collectivités décentralisées et les établissements publics, sont pénalement responsables des infractions prévues par la présente loi, commises pour leur compte par leurs organes ou représentants.
La responsabilité des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits.

Les peines encourues par les personnes morales sont :

1) l'amende qui peut être portée au quintuple de celle encourue par les personnes physiques ou à trois cent millions (300 000 000) de francs CFA si aucune amende n'est prévue ;
2) la dissolution, lorsque la personne morale a été créée ou détournée de son objet pour commettre les faits incriminés ;
3) l'interdiction à titre définitif ou temporaire d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ;
4) la fermeture définitive ou temporaire d'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

5) l'exclusion des marchés publics à titre définitif ou temporaire ;

6) l'interdiction à titre définitif ou temporaire de faire appel public à l'épargne ;

7) l'interdiction temporaire 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 ;

8) la confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit ;

9) 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.

Article 37 : Confiscation des matériels ayant servi à commettre les infractions

En cas de condamnation, le tribunal pourra prononcer la confiscation des matériels, équipements, instruments, programmes informatiques ou tous dispositifs ou données appartenant au condamné et ayant servi à commettre les infractions.

Article 38 : Interdictions à titre de peines complémentaires

En cas de condamnation pour une infraction commise par le biais d'un support de communication numérique, la juridiction peut prononcer à titre de peines complémentaires, outre les interdictions et confiscations prévues par la présente loi, 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, la coupure de l'accès par tous moyens techniques disponibles ou l'interdiction de l'hébergement.

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

La durée de l'interdiction est fixée par la juridiction saisie. Elle ne peut excéder cinq (5) ans.

La violation des interdictions prononcées par la juridiction compétente expose son auteur à une amende de cent mille (100 000) à un million (1 000 000) de francs CFA. En cas de récidive, l'auteur est puni d'un emprisonnement de deux (2) mois à un (1) an et du double de la peine d'amende

Article 39 : Publication de la décision de justice à titre de peines complémentaires

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

La juridiction saisie peut en outre, si elle l'estime opportun, ordonner la publication de la condamnation au journal officiel ou par affichage en caractères très apparents dans les lieux publics pour une durée ne pouvant excéder deux (2) mois.

Toute personne qui a fait l'objet d'une ordonnance de non-lieu, d'une décision de relaxe ou d'acquittement a le droit de demander la publication de cette décision par les médias. Cette publication doit être requise auprès du juge de la décision qui en apprécie l'intérêt et l'opportunité eu égard au traitement médiatique réservé préalablement au demandeur.

Son refus doit être spécialement motivé.

CHAPITRE II - REGLES DE PROCEDURE PENALE EN MATIERE DE CYBERCRIMINALITE

Article 40 : Prescription en matière d'infractions commises par le biais de réseaux informatiques

Les crimes, délits et contraventions, lorsqu'ils sont commis par le biais de réseaux informatiques se prescrivent dans les délais de droit commun à compter de la cessation de l'activité délictueuse en ligne.

Article 41 : Preuve électronique en matière pénale

L'écrit électronique en matière pénale est admis comme mode de preuve au même titre que l'écrit sur support papier à condition que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.

Article 42 : Perquisition ou accès à un système informatique

Lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données informatisées sur le territoire togolais, sont utiles à la manifestation de la vérité, l'officier de police judiciaire peut opérer une perquisition, sous le contrôle du procureur de la République, ou accéder à un système informatique ou à une partie de celui-ci ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.

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

Article 43 : Placement sous scellé de supports électroniques

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

L'officier de police judiciaire désigne, sous le contrôle du procureur de la République, toute personne qualifiée pour utiliser les moyens techniques appropriés afin d'empêcher l'accès aux données visées à l'article 42 de la présente loi dans le système informatique ou aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique et de garantir leur intégrité.

Si les données qui sont liées à l'infraction, soit qu'elles en constituent l'objet, soit qu'elles en ont été le produit, sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, l'officier de police judiciaire ordonne, sous le contrôle du procureur de la République, les mesures conservatoires nécessaires, notamment en désignant toute personne qualifiée avec pour mission d'utiliser tous les moyens techniques appropriés pour rendre ces données inaccessibles.

Lorsque la mesure prévue à l'alinéa 2 du présent article n'est pas possible, pour des raisons techniques ou en raison du volume des données, l'officier de police judiciaire, sous le contrôle

du procureur de la République, utilise les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.

L'Officier de police judiciaire, sous le contrôle du procureur de la République, informe le responsable du système informatique de la recherche effectuée dans le système informatique et lui communique une copie des données qui ont été copiées, rendues inaccessibles ou retirées.

Article 44 : Interception des données informatisées

Lorsque les nécessités de l'information l'exigent, l'Officier de police judiciaire, sous le contrôle du procureur de la République, peut utiliser les moyens techniques appropriés pour collecter ou enregistrer en temps réel, les données relatives au contenu de communications spécifiques, transmises au moyen d'un système informatique ou obliger un fournisseur de services, dans le cadre de ses capacités techniques à collecter ou à enregistrer, en application de moyens techniques existants, ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer lesdites données informatisées.

Le fournisseur d'accès est tenu de garder le secret.

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

Article 45 : Interceptions de sécurité

Dans les conditions prévues par décret, peuvent être autorisées les interceptions de correspondances émises par voie des communications électroniques et susceptibles de révéler des renseignements relatifs aux finalités prévues par décret.

Les coûts supportés par les opérateurs de communications électroniques, les personnes qui fournissent au public des services de communications électroniques et les personnes qui offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès réseau, occasionnés par l'acquisition des équipements d'interception et la mise en œuvre des interceptions de sécurité restent à leur charge.

Un décret définit les conditions réglementaires d'exécution et de contrôle des présentes dispositions.

Article 46 : Pouvoirs des agents assermentés des structures nationales de cybersécurité et de lutte contre la cybercriminalité

Les agents assermentés des structures nationales de cybersécurité et de lutte contre la cybercriminalité, assistés au besoin par les forces de sécurité, peuvent, pour les nécessités de l'enquête ou de l'exécution d'une délégation judiciaire, procéder aux opérations prévues aux articles 42 à 44 de la présente loi.

TITRE IV - DISPOSITIONS TRANSITOIRES ET FINALES

Article 47 : Dispositions transitoires

Le ministère chargé de l'économie numérique assure les missions de l'ANCy en attendant son opérationnalisation effective.

Article 48 : Dispositions finales

Des décrets d'application fixent, en tant que de besoin, les modalités d'application de la présente loi.

Fait à Lomé, le 07 DEC 2018

Le Président de la République

SIGNE

Faure Essozimna GNASSINGBE

Le Premier ministre

SIGNE

Selom Komi KLASSOU

Pour ampliation
le Secrétaire général
de la Présidence de la République

SIGNE

Daté Patrick TEVI-BENISSAN