PRESIDENCE DE LA REPUBLIQUE

REPUBLIQUE TOGOLAISE
Travail-Liberté-Patrie

LOI N° 2022-009

PORTANT MODIFICATION DE LA LOI N° 2018-026 DU 07 DECEMBRE 2018 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 :

Article premier : Les dispositions des articles 2, 3 et 6 de la loi n° 2018-026 du 7 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité sont modifiées ainsi qu'il suit :

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 : tout dispositif isolé ou non ou tout ensemble de dispositifs interconnectés assurant, en tout ou en partie, un traitement automatisé de données en exécution d'un programme. Il comprend également l'ensemble des moyens électroniques destinés à élaborer, à traiter, à stocker, à transmettre ou à sécuriser des 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.

Article 3 nouveau : 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 de désignation des opérateurs de services essentiels et de détermination des infrastructures essentielles.

Les règles de cybersécurité, au respect desquelles les opérateurs de services essentiels sont tenus, sont définies par voie règlementaire.

Article 6 nouveau : Agence nationale de la cybersécurité

Il est créé une personne morale de droit public dotée de l'autonomie de gestion administrative et financière, assurant une mission d'utilité publique dénommée « Agence nationale de la cybersécurité », en abrégé « ANCy ».

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.

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

1) assure la fonction d'autorité nationale de protection et 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) qualifie les dispositifs, matériels et logiciels qui contribuent à la sécurité des systèmes d'information des administrations et des opérateurs de services essentiels et les matériels, logiciels et systèmes d'information destinés à traiter les informations couvertes par le secret de la défense nationale ;

14) qualifie les prestataires fournissant des services qui contribuent à la sécurité (i) des systèmes d'information des administrations ou des opérateurs de services essentiels et (ii) de tout matériel, logiciel ou système d'information destiné à traiter des informations couvertes par le secret de la défense nationale ;

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 2 : La présente loi sera exécutée comme loi de l'Etat.

Fait à Lomé, le 24 JUIN 2022

Le Président de la République

SIGNE

Faure Essozimna GNASSINGBE

Le Premier ministre

SIGNE

Victoire Sidémého TOMEGAH-DOGBE

Pour ampliation
le Secrétaire général
de la Présidence de la République

Ablamba Ahoéfavi JOHNSON