Loi | Générale | modern

Loi n° 195/AN/25/9ème L portant création de l’Autorité Nationale de Cybersécurité.

n° 195/AN/25/9ème L

Ministère
ASSEMBLÉE NATIONALE

Date de publication
8 janvier 2026

Numéro JO
n° 23 du 15/12/2025

Date du numéro
15 décembre 2025

INTRODUCTION

L'ASSEMBLÉE NATIONALE A ADOPTÉLE PRÉSIDENT DE LA RÉPUBLIQUE PROMULGUELA LOI DONT LA TENEUR SUIT :

VISAS

L’ASSEMBLEE NATIONALE A ADOPTE LE PRESIDENT DE LA REPUBLIQUE PROMULGUE LA LOI DONT LA TENEUR SUITVU La Constitution du 15 septembre 1992

VU La Loi Constitutionnelle n°92/AN/10/6ème L du 21 avril 2010 portant révision de la Constitution

VU La Loi n°100/AN/15/7ème L du 11 juillet 2015 portant création de l’Agence Nationale des Systèmes d’Information de l’État

VU La Loi n°56/AN/19/8ème L du 17 juillet 2019 portant régime juridique des établissements publics

VU La Loi n°18/AN/23/9ème L du 21 janvier 2024 portant ratification de la Convention de l’Union Africaine sur la cybersécurité et la protection des données à caractère personnel (Convention de Malabo)

VU La Loi n°19/AN/23/9ème L du 18 septembre 2025 portant Code Numérique de la République de Djibouti

VU Le Décret n°2006-0106/PRE du 13 avril 2006 portant création d’une Unité de Coordination du projet e-gouvernement

VU Le Décret n°2012-215/PRE du 30 septembre 2012 portant création du Comité National de Coordination du Projet e-gouvernement

VU Le Décret n°2021-105/PRE du 24 mai 2021 portant nomination du Premier Ministre

VU Le Décret n°2021-106/PRE du 24 mai 2021 portant nomination des membres du Gouvernement

VU Le Décret n°2021-114/PRE du 31 mai 2021 fixant les attributions des Ministères

VU Le Décret n°2022-001/PRE du 02 janvier 2022 portant remaniement Ministériel

VU Le Décret n°2025-082/PRE du 01 avril 2025 portant nomination d’un nouveau membre du Gouvernement

VU La Circulaire n°178/PAN/AI du 10/11/2025 portant convocation de l’Assemblée Nationale en séance publique. Le Conseil des Ministres entendu en sa séance du 04 Novembre 2025. A ADOPTÉ, EN SA DEUXIEME SEANCE PUBLIQUE DU 12/11/2025, LA LOI DONT LA TENEUR SUIT :

TEXTE INTÉGRAL

TITRE I : DISPOSITIONS GÉNÉRALES

Article 1er

Il est créé une Autorité Nationale de Cybersécurité (ANC), établissement public à caractère administratif doté de la personnalité juridique et de l'autonomie financière et administrative.Le siège de l'Autorité Nationale de Cybersécurité (ANC) est fixé à Djibouti.

Article 2

L'Autorité Nationale de Cybersécurité dénommée ANC est rattachée à la Présidence de la République sous la supervision de la Direction Générale de la Sécurité Nationale de la République.

Article 3

Au sens de la présente loi, on entend par

- Cybersécurité : Ensemble des mesures visant à garantir la résilience, l'intégrité, la confidentialité et la disponibilité des systèmes d'information
- Cybercriminalité : Toute infraction pénale commise au moyen d'un système informatique ou contre un système d'information, y compris les accès non autorisés, les atteintes aux données, les fraudes électroniques, et les infractions facilitées par les technologies numériques
- Infrastructure d'importance vitale : Installation, système ou service dont l'indisponibilité compromettrait gravement la sécurité nationale, l'économie ou la santé publique
- Opérateur d'importance vitale : Personne publique ou privée gestionnaire d'une infrastructure d'importance vitale
- Incident de sécurité : Événement compromettant ou susceptible de compromettre la sécurité d'un système d'information
- Souveraineté numérique : Capacité de l'État à exercer son autorité et à protéger ses intérêts dans le cyberespace
- Technologies émergentes stratégiques : Technologies innovantes présentant un potentiel stratégique majeur pour la souveraineté numérique et la sécurité nationale, notamment l'intelligence artificielle, l'informatique quantique, la cryptographie post quantique, la 5G/6G, la blockchain et l'internet des objets
- Manipulation de l'information : Diffusion intentionnelle et massive de nouvelles fausses ou trompeuses dans le but d'influencer l'opinion publique ou de déstabiliser les institutions
- Cyberattaque : Action malveillante visant à compromettre la sécurité d'un système d'information
- Crise cybernétique majeure : Situation résultant d'une ou plusieurs cyberattaques affectant gravement les infrastructures d'importance vitale ou le fonctionnement normal de l'État
- Résilience numérique : Capacité des systèmes d'information à résister et à se rétablir après une cyberattaque
- Identité numérique : Ensemble des attributs liés à une entité qui permet de l'identifier dans l'environnement numérique
- Incident de sécurité significatif : Incident susceptible d'affecter la continuité de service d'une infrastructure d'importance vitale pendant plus de quatre heures consécutives ou compromettant l'intégrité de données sensibles
- Urgence cybernétique caractérisée : Situation présentant un risque imminent et documenté de compromission grave d'une infrastructure d'importance vitale
- Mesure technique proportionnée : Mesure strictement nécessaire à la neutralisation de la menace, d'impact minimal sur le fonctionnement normal des systèmes
- Attribution technique établie : Identification de l'origine d'une cyberattaque fondée sur des preuves techniques documentées selon des critères objectifs. TITRE II : MISSIONS

Article 4

L'Autorité Nationale de Cybersécurité est chargée de définir, coordonner et mettre en œuvre la politique nationale de cybersécurité.À ce titre, l'ANC exerce les missions suivantes :1. Élaborer et mettre en œuvre la stratégie nationale de cybersécurité

2. Assurer la protection des systèmes d'information de l'État et des opérateurs d'importance vitale
3. Gérer et sécuriser les infrastructures de communication électronique dédiées aux besoins souverains de l'État
4. Assurer les fonctions de Computer Emergency Response Team (CERT) national
5. Promouvoir et accompagner la création des CERT/SOCs sectoriels
6. Prévenir, détecter et contrer les opérations d'ingérence numérique, de manipulation de l'information et de désinformation susceptibles de porter atteinte aux intérêts fondamentaux de la Nation
7. Développer l'écosystème national de cybersécurité et promouvoir la souveraineté numérique
8. Coopérer avec les partenaires nationaux et internationaux dans le respect des intérêts fondamentaux de la Nation
9. Évaluer l'impact des technologies émergentes stratégiques sur la cybersécurité nationale et contribuer à l'élaboration de cadres normatifs adaptés
10. Contribuer au développement de solutions souveraines fondées sur des technologies émergentes stratégiques
11. Contribuer à la protection des données personnelles des citoyens face aux menaces cybernétiques, en coordination avec la commission nationale de protection des données
12. Coordonner les initiatives de protection des enfants en ligne, en collaboration avec les autorités compétentes, afin de prévenir les contenus illicites, les abus et les risques liés à l'usage du numérique par les mineurs
13. Veiller à la prise en compte des besoins spécifiques des personnes handicapées dans l'élaboration et la sécurisation des services numériques, en promouvant l'accessibilité, l'inclusion et la protection contre les menaces cybernétiques
14. Assurer la gestion des aspects techniques de l'identité numérique et veiller à la sécurité des systèmes d'authentification électronique nationaux
15. Évaluer et approuver préalablement les services et solutions numériques destinés aux institutions publiques et aux opérateurs d'importance vitale, afin d'en mesurer l'impact sur la souveraineté numérique et la sécurité nationale
16. Collaborer étroitement avec les autorités compétentes, notamment les ministères chargés de la justice, de l'intérieur et de la défense, les autorités judiciaires et les forces de sécurité intérieure, dans la prévention, la détection, l'enquête et la pour suite des infractions commises au moyen des technologies de l'information et de la communication
17. Organiser, en coordination avec les autorités compétentes, des sessions de formation continue destinées aux magistrats, enquêteurs et officiers de police judiciaire en matière de cybercriminalité.

Article 5

Dans l'exercice de ses missions, l'ANC agit dans le respect des lois et des règlements en vigueur, notamment ceux relatifs à la protection des données à caractère personnel et aux libertés fondamentales. Son action est guidée par les principes de nécessité, de proportionnalité, d'impartialité et de transparence. TITRE III : ORGANISATION

Article 6

Il est institué un Conseil National de Cybersécurité, présidé par le Directeur Général de la Sécurité Nationale

- Il définit les orientations stratégiques nationales en matière de cybersécurité etassure la coordination interministérielle en cas de crise majeure
- Il exerce les fonctions de Conseil d'Administration de l'ANC.Un décret pris en Conseil des Ministres précise la composition et les modalités de fonctionnement du Conseil National de Cybersécurité.

Article 7

L'Autorité Nationale de la Cybersécurité (ANC) est dirigée par un Directeur Général nommé par décret pris en Conseil des Ministres. Elle est structurée en unités spécialisées chargées de la mise en œuvre opérationnelle de ses missions.Ces unités spécialisées ayant rang de direction dans la hiérarchie administrative. Placées sous l'autorité du Directeur Général, les unités spécialisées initiales de l'ANC sont les suivantes

- L'Unité de détection, de réponse et de coordination aux incidents de cybersécurité (DJ-CERT)
- L'Unité de la gouvernance, du risque et de la résilience
- L'Unité des technologies émergentes et de la sécurité de l'identité numérique
- L'Unité des services support.Ces unités initiales peuvent être modifiées, réorganisées ou complétées, en fonction des besoins opérationnels ou stratégiques, par décision du Directeur Général, après approbation du Conseil National de Cybersécurité. Les différents organes de fonctionnement de l'autorité seront précisés par acte règlementaire.

Article 8

L'ANC est dotée d'un agent comptable. La gestion financière et comptable s'exerce dans les conditions prévues par les dispositions relatives aux établissements publics administratifs. TITRE IV : POUVOIRS

Article 9

Dans l'exercice de ses missions, l'ANC dispose des prérogatives suivantes

- Édicter des règles de sécurité applicables aux systèmes d'information de l'État et des opérateurs d'importance vitale, après consultation des entités concernées
- Contrôler le respect de ces règles et procéder aux audits nécessaires
- Enjoindre la mise en œuvre de mesures correctives en cas de vulnérabilité critique
- Certifier la conformité des produits et des systèmes de sécurité
- Identifier et proposer au Gouvernement la liste initiale des opérateurs d'importance vitale (OIV)
- Alerter les autorités et le public des menaces majeures
- Sanctionner les manquements dans les conditions prévues par la présente loi
- Qualifier les campagnes de manipulation de l'information d'origine étrangère et en informer les autorités compétentes et les opérateurs concernés
- Définir les normes techniques relatives à l'identité numérique et certifier les solutions d'authentification électronique.Ces prérogatives s'exercent dans le respect du principe de subsidiarité, privilégiant l'accompagnement et l'autorégulation avant les mesures contraignantes.

Article 10

Les agents habilités de l'ANC peuvent accéder aux systèmes d'information dans le cadre de leurs missions, en présence du responsable du système ou de son représentant, sauf cas d'urgence cybernétique caractérisée.Un préavis de quarante-huit heures est notifié au responsable du système, sauf urgence caractérisée dûment motivée.L'accès est limité aux données strictement nécessaires à l'accomplissement de la mission.Un procès-verbal contradictoire est établi à l'issue de chaque intervention.Le secret des affaires ne peut pas être opposé à l'ANC dans l'exercice de ses missions.

Article 11

L'ANC est habilitée à qualifier le niveau de menace cybernétique nationale et à déclencher les mesures correspondantes.La qualification du niveau de menace s'appuie sur des critères techniques objectifs, notamment la gravité, l'ampleur et l'origine de la menace, conformément aux standards internationaux reconnus. Les modalités d'application du présent alinéa sont fixées par décret pris en Conseil des Ministres.

Article 12

En cas de crise cybernétique majeure constituant une menace grave et imminente pour la sécurité nationale, l'ANC peut, sur décision du Conseil National de Cybersécurité et pour une durée strictement limitée à la résolution de la crise

- Imposer aux opérateurs d'importance vitale des mesures techniques proportionnées nécessaires pour faire face à la menace
- Ordonner l'isolement temporaire de certains systèmes d'information des réseaux publics pour une durée maximale de quarante-huit heures, non renouvelable sauf autorisation du juge administratif
- Ordonner la mise hors service des systèmes compromis jusqu'à leur remise en sécurité, dans la limite de sept jours, sauf autorisation judiciaire pour une durée supérieure.Ces mesures exceptionnelles sont prises par décision motivée notifiée. Elles sont strictement proportionnées à la gravité de la menace. Un compte rendu des mesures prises est adressé dans les quarante-huit heures au président de la République. TITRE V : OBLIGATIONS ET SANCTIONS

Article 13

Les opérateurs d'importance vitale (OIV) sont tenus de

- Mettre en œuvre les mesures de sécurité prescrites par l'ANC
- Notifier sans délai tout incident de sécurité significatif
- Coopérer aux investigations en cas d'incident majeur.

Article 14

Le non-respect des obligations prévues par la présente loi est passible de sanctions administratives prononcées par l'ANC après procédure contradictoire.Les sanctions administratives peuvent comprendre

- Une mise en demeure de se conformer aux obligations dans un délai déterminé
- Une amende administrative dont le montant ne peut pas excéder 2% du chiffre d'affaires annuel mondial total de l'exercice précédent pour les entreprises privées ou 1% du budget annuel pour les entités publiques
- À titre exceptionnel et en cas de risque grave et imminent pour la sécurité nationale, une interdiction temporaire d'exploiter certains systèmes d'information pour une durée maximale d'un mois, renouvelable une fois sur décision motivée.Les sanctions sont motivées, proportionnées et tiennent compte de la capacité financière de l'entité sanctionnée.

Article 15

Les décisions prises en application des articles 11 et 13 font l'objet d'un recours suspensif devant le juge administratif dans un délai de quarante-huit heures pour les mesures d'urgence et de trente jours pour les sanctions administratives.Le juge administratif statue en référé dans un délai de soixante douze heures pour les recours contre les mesures d'urgence.

Article 16

Les décisions de sanction de l'ANC sont susceptibles de recours devant la juridiction administrative compétente. TITRE VI : COOPÉRATION ET TRANSPARENCE

Article 17

L'ANC anime l'écosystème national de cybersécurité et peut conclure des conventions de partenariat avec les acteurs publics et privés.

Article 18

L'ANC coopère avec ses homologues étrangers et les organisations internationales compétentes dans le respect des intérêts fondamentaux de la Nation.Cette coopération peut notamment prendre la forme

- D'échanges d'informations sur les menaces et vulnérabilités
- De participation à des exercices internationaux de gestion de crise
- De contribution aux initiatives de renforcement des capacités régionales
- D'assistance technique aux pays partenaires.L'échange d'informations avec les partenaires étrangers respecte la législation nationale sur la protection des données. Aucune donnée personnelle de citoyens djiboutiens n'est transmise sans garanties équivalentes de protection dans le pays destinataire.L'ANC représente la République de Djibouti dans les instances internationales spécialisées en matière de cybersécurité.

Article 19

L'ANC établit un rapport annuel d'activité soumis au président de la République et présenté à l'Assemblée nationale.Elle publie semestriellement des statistiques anonymisées sur les incidents traités et les mesures prises.

Article 20

Les agents de l'ANC sont astreints au secret professionnel et au secret de la défense nationale dans les conditions prévues par le Code pénal.

Article 21

L'ANC peut créer en son sein une unité de recherche et d'innovation dédié en cybersécurité et aux technologies émergentes stratégiques. Cette unité peut conclure des partenariats avec les institutions académiques et les acteurs industriels nationaux et internationaux. TITRE VII : RESSOURCES

Article 22

Les ressources de l'ANC comprennent :- Les crédits inscrits au budget de l'État ;- Le produit des redevances pour services rendus ;- Le produit des sanctions pécuniaires ;- Les dons et legs autorisés ;- Toute autre ressource prévue par la loi.

Article 23

L'ANC est soumise au contrôle financier de l'État dans les conditions applicables aux établissements publics. TITRE VIII :

DISPOSITIONS TRANSITOIRES ET FINALES

Article 24

La Direction de la Sécurité des Systèmes d'Information (DSSI) de l'Agence Nationale des Systèmes d'Information de l'État (ANSIE) constitue le noyau initial de l'ANC. Les missions, moyens et personnels de cette direction sont transférés à l'ANC.Les attributions, les moyens matériels et financiers ainsi que le personnel relevant de ladite direction sont transférés de plein droit à l'ANC.La loi n°100/AN/15/7ème L portant création de l'Agence Nationale des Systèmes d'Information de l'État (ANSIE) est ainsi modifiée :1- Les dispositions relatives à la Direction de la Sécurité des Systèmes d'information sont abrogées ;2- Les missions relatives à la sécurité des systèmes d'information de l'Etat précédemment exercées par l'ANSIE, sont transférées

à l'ANC ;3- Sont abrogées toutes dispositions de la loi N°100/AN/15/7ème L portant création de l'Agence Nationale des Systèmes d'Information de l'État (ANSIE), contraires aux présentes dispositions.

Article 25

Le personnel de la direction mentionnée à l'article précédent, transféré à l'ANC, est intégré de plein droit à celle-ci.Il conserve le bénéfice de son statut ainsi que l'ensemble de ses droits acquis.

Article 26

Pour renforcer ses capacités, l'ANC peut recruter :- Des agents de la fonction publique par voie de détachement ou de mise à disposition ;- Un personnel contractuel.

Article 27

Le recrutement des agents de la fonction publique s'effectue par voie de concours ouverts aux agents publics justifiants des qualifications requises.Ces concours comportent des épreuves techniques spécifiques aux métiers de la cybersécurité et des technologies émergentes.Ils sont organisés selon des principes garantissant l'égalité des chances et la sélection des candidats selon leurs compétences et aptitudes.Les modalités d'organisation de ces concours, la composition des jurys et les conditions d'aptitude requises des candidats sont fixées par arrêté.

Article 28

L'ANC contribue à la valorisation des expertises techniques au sein de l'État et peut proposer des programmes de formation au bénéfice des agents publics.

Article 29

Les modalités d'application de la présente loi sont fixées par décret en Conseil des Ministres.

Article 30

Les dispositions de la présente loi font l'objet d'une révision quinquennale pour tenir compte de l'évolution technologique et des retours d'expérience.

Article 31

La présente Loi sera enregistrée et publiée au Journal Officiel de la République de Djibouti, dès sa promulgation.

Fait à Djibouti, le 14 Décembre 2025

Le Président de la République
Chef du Gouvernement

ISMAÏL OMAR GUELLEH