Décret-loi n° 2023-17 du 11 mars 2023, relatif à la cybersécurité.

La Président de la République,

Après délibération du Conseil des ministres.

Prend le décret-loi dont la teneur suit :

Chapitre premier

Dispositions générales

Article premier - Le présent décret-loi vise à réglementer le domaine de la cybersécurité et à fixer les missions de l'Agence nationale de la cybersécurité et les mécanismes qui lui sont attribués pour assurer la sécurité de l'espace cybernétique national dans le cadre de ses attributions.

Art. 2 - Sont exclus de l'application des dispositions du présent décret-loi les systèmes d'informations et équipements électroniques par lesquels sont traitées des données relatives à la sécurité publique ou à la défense nationale et qui affectent la sécurité nationale et l'intérêt suprême de l'Etat.

La liste des structures qui exploitent les systèmes d'informations et équipements électroniques concernés par l'exception mentionnée au premier paragraphe du présent article est fixée par décret.

Art. 3 - Au sens du présent décret-loi, on entend par :

- **Espace cybernétique** : Espace numérique connectant les systèmes de traitement numérique des données aux réseaux informatiques et de télécommunications, et comprenant des composants matériels et immatériels tels que les ordinateurs, les serveurs, les systèmes d'exploitation, les logiciels, les réseaux de télécommunications, le contenu numérique, les usagers, soient opérateurs ou utilisateurs de service et toutes les opérations faites à l'aide de ces composants.

- **Réseau informatique :** Système qui interconnecte deux ou plusieurs dispositifs, afin d'échanger des informations en utilisant les technologies de communication et de partager les ressources et les données disponibles.

- **Réseau de télécommunications :** Ensemble de dispositifs interconnectés par des moyens de télécommunications filaires ou sans fil qui leur permettent d'assurer les échanges en se basant sur des protocoles conventionnels.

- **Infrastructure numérique d'importance vitale** : systèmes d'information qui abritent des actifs et des services sensibles au niveau national, dont l'arrêt ou la perturbation de leurs sécurités pourrait affecter la sûreté nationale.

- **La cybersécurité :** Ensemble des mesures et des mécanismes techniques et non techniques mises en place afin d'assurer la protection du cyber espace et de renforcer la capacité d'anticipation, de prévention contre les risques cybernétiques, de détection rapide des incidents et des attaques cybernétiques et de réponse en cas d'urgence, et ce dans le but de réduire les dommages et afin d'assurer la continuité de l'activité dans le cas des crises cybernétiques.

- **La crise cybernétique :** Un état de perturbation dû à un incident cybernétique qui endommage, de manière continue, une ou plusieurs composantes du cyberespace et qui entraîne une interruption de la continuité des services.

- **Système d'information :** Ensemble de ressources matérielles et immatérielles, logiciels, outils et dispositifs isolés ou interconnectés, permettant la gestion de l'information et assurant les opérations de collecte, de stockage, de traitement, d'envoi et de diffusion des données.

- **La vulnérabilité :** Le point faible ou le défaut au niveau d'un composant du cyberespace qui le rend vulnérable aux incidents et aux attaques cybernétiques.

- **Cyber attaque :** L'ensemble des actions techniques délibérées et non autorisées qui exploitent les vulnérabilités et causent des dommages dans le but de pénétrer, de causer un déni de service, d'affaiblir ou de perturber le fonctionnement des dispositifs, des réseaux et systèmes d'information, ou dans le but d'intercepter, de modifier ou de détruire les données.

- **Cyber incident :** Un acte ou un problème accidentel ou intentionnel qui cause des dommages matériels ou immatériels à un ou plusieurs composants du cyberespace.

- **La menace cybernétique :** L'ensemble de facteurs externes ou internes, accidentels ou intentionnels, susceptibles d'affecter ou de nuire à une ou plusieurs composantes du cyberespace.

- **Le risque cybernétique :** La possibilité qu'une cyber menace accidentelle ou intentionnelle contourne les mécanismes de cybersécurité, en exploitant les vulnérabilités présentes dans un ou plusieurs composants du cyberespace avec la possibilité de causer des dommages.

- **Label « sécurisé » :** Le résultat du processus de certification selon lequel un logiciel ou un dispositif électronique est classé après avoir été vérifié étant conforme à un ensemble de normes techniques de sécurité.

- **Nuage ou Cloud :** Un centre de données accessible par des réseaux de télécommunications.

- **Informatique en nuage ou Cloud computing :** Le modèle de transfert des ressources, de transfert du traitement et de transfert du stockage des données vers le Cloud, et les modalités d'accès de l'usager à ces éléments à travers le réseau de télécommunications.

- **Fournisseur de services Cloud gouvernemental « G-Cloud » :** Une personne morale publique ou privée spécialisée dans l'hébergement des systèmes, des plateformes électroniques et infrastructures numériques gouvernementaux. Il doit être impérativement relié au réseau national intégré de l'administration et à la plateforme nationale d'interopérabilité.

- **Réseau National Intégré de l'Administration :** Un réseau informatique privé qui fournit des services intégrés et qui se compose d'un groupe de sites administratifs qui permettent l'échange de données entre les serveurs et les ordinateurs qui leur sont connectés via des protocoles unifiés et un adressage privé.

- **Fournisseur de services Cloud national « N-Cloud » :** Une personne morale publique ou privée spécialisée dans l'hébergement des systèmes, des plateformes électroniques et d'infrastructures numériques nationaux.

Chapitre II

De l'Agence nationale de la cybersécurité

Art. 4 - Il est créé un établissement public à caractère non administratif doté de la personnalité morale et de l'autonomie financière dénommé « Agence nationale de la cybersécurité », soumis dans ses rapports avec les tiers à la législation commerciale. Son siège est situé à Tunis, et ci-après désignée « l'Agence ».

L'Agence est placée sous la tutelle du ministère chargé des technologies de la communication.

L'organisation administrative et financière et les modalités de fonctionnement de l'Agence sont fixées par décret.

Art. 5 - L'Agence est chargée, en coordination avec les différentes structures impliquées dans le domaine, de la supervision de la sécurité des systèmes d'information et de communication des structures publiques et privées de l'espace cybernétique national et exerce principalement les missions suivantes :

- Elaborer et mettre à jour les politiques et mécanismes de gouvernance et de la sécurité de l'espace cybernétique national et les mettre à la disposition des secteurs et organismes concernés.
- Suivre la mise en œuvre des plans d'actions pour la sécurité de l'espace cybernétique national concernant :
- Les mesures proactives pour éviter les menaces délibérées et accidentelles sur l'espace cybernétique national.
- Les mesures préventives pour se protéger contre les risques cybernétiques.
- Les mécanismes de détection et de signalement instantanés des incidents et des attaques cybernétiques.
- La réponse urgente en cas d'urgences pour faire face aux attaques cybernétiques et atténuer leurs impacts.
- La reprise rapide suite à effets des incidents et des attaques cybernétiques pour assurer la continuité de l'activité.
- L'enquête et l'investigation numérique pour diagnostiquer les incidents et déterminer les responsabilités en relation avec la cyber sécurité.
- Elaborer et suivre la mise en œuvre des programmes de développement des compétences dans le domaine de la cybersécurité à travers :
- La participation à l'élaboration des programmes académiques et professionnels spécialisés dans le domaine de la cyber sécurité.
- La validation des programmes de formation dans le domaine de la cyber sécurité et leur publication sur le site officiel de l'Agence.
- L'organisation des sessions de formations spécialisées dans le domaine de la cybersécurité.
- Élaborer et publier les référentiels, les modèles et les guides liés à la cybersécurité dont les organismes publics et privés doivent adopter.
- Elaborer les indicateurs de mesure du niveau national de cybersécurité et publier les tableaux de bord de façon périodique.
- Mener des campagnes périodiques de communication et de sensibilisation dans le domaine de la cybersécurité, notamment lors des crises cybernétiques.
- Assurer la veille technologique et suivre les évolutions dans le domaine de la cybersécurité,
- La coopération internationale et la coordination avec les structures étrangères officielles compétentes conformément aux accords conclus à cet effet à l'échelle bilatérale, régionale et internationale.

Et d'une manière générale, toute autre activité qui lui est confiée par l'autorité de tutelle et en rapport avec son domaine d'intervention.

Chapitre III

De l'audit obligatoire de la sécurité des systèmes d'information

Art. 6 - Sont soumis à un système d'audit obligatoire et périodique les systèmes d'information et les réseaux relevant des organismes publics et privés suivants :

- Les opérateurs de réseaux publics de télécommunications et les fournisseurs des services de télécommunications et d'internet,
- Les entreprises dont les réseaux informatiques sont interconnectés à travers des réseaux de télécommunications,
- Les fournisseurs des services d'hébergement et d'informatique en nuages.
- Les entreprises qui procèdent au traitement automatisé des données personnelles de leurs usagers dans le cadre de la fourniture de leurs services à travers les réseaux de télécommunications.
- Les infrastructures numériques d'importance vitale

Les critères techniques d'audit et les modalités de suivi de la mise en œuvre des recommandations contenues dans le rapport d'audit sont fixés par arrêté du ministre chargé des technologies de la communication.

Art. 7 - L'opération d'audit obligatoire de sécurité des systèmes d'information est effectuée par des experts exerçant leurs activités conformément à la législation en vigueur de manière périodique une fois au moins tous les douze (12) mois.

L'Agence publie et met à jour la liste des experts et des organismes autorisés à exercer l'activité d'audit dans le domaine de la sécurité cybernétique.

Art. 8 - Les organismes soumis à l'audit de sécurité des systèmes d'information remettent à l'Agence une copie électronique protégée du rapport d'audit dans un délai ne dépassant pas dix (10) jours après la fin des opérations d'audit.

Les organismes visés au premier paragraphe du présent article doivent mettre en œuvre toutes les recommandations de sécurité contenues dans le rapport.

Art. 9 - Il est interdit aux agents de l'Agence et aux experts chargés des opérations d'audit de divulguer toutes informations dont ils ont eu connaissance lors de l'exercice de leurs missions.

Sont passibles des sanctions prévues à l'article 254 du code pénal, quiconque divulgue, participe ou incite à la divulgation de ces informations.

Chapitres IV

De la sécurité des logiciels et équipements électroniques

Art. 10 - L'Agence, sur demande du développeur ou de l'importateur, attribue le label « sécurisé » à chaque logiciel ou équipement électronique

La demande du label est facultative et basée sur un rapport d'audit de sécurité détaillé présenté par les experts-auditeurs exerçant leurs activités conformément à la législation en vigueur.

Art. 11 - Le label « Sécurisé » délivré au logiciel ou équipement électronique est renouvelé tous les trois (3) ans, et il peut être retiré avant l'expiration de la durée de la validité en cas de modification des caractéristiques techniques ou survenance de changement technologique qui introduit des failles au logiciel ou équipement électronique.

Les procédures et conditions d'octroi du label « sécurisé » et de son retrait seront fixées par arrêté du ministre chargé des technologies de la communication.

L'Agence est chargée de tenir et publier un registre national des logiciels et équipements électroniques ayant obtenu le label « sécurisé », qui sera mis à jour périodiquement

Chapitre V

Du classement des fournisseurs des services de l'informatique en nuage et de l'hébergement

Art. 12 - L'Agence attribue, renouvelle et retire le label « Fournisseur de services informatique en nuage gouvernemental (G-cloud) » et le label « Fournisseur de services informatique en nuage national (N-cloud) » aux fournisseurs des services d'hébergement après avis des ministres de la défense nationale et de l'intérieur.

Les procédures et les conditions d'octroi, de renouvellement et de retrait du label « Fournisseur de services informatique en nuage gouvernemental (G-cloud) » et du label « Fournisseur de services informatique en nuage national (N-cloud) » seront fixées par arrêté du ministre chargé des technologies de la communication.

L'Agence publie et met à jour la liste des fournisseurs de services informatique en nuage qui ont obtenu le label.

Art. 13 - Le label « Fournisseur de services informatique en nuage gouvernemental (G-cloud) » et le label « Fournisseur de services informatique en nuage national (N-cloud) » sont renouvelés annuellement.

Le label octroyé peut retirer avant l'expiration de la durée de la validité en cas de manquement à l'une des conditions techniques fixées par l'arrêté mentionné à l'article 12 du présent décret-loi.

Art. 14 - Les organismes visés à l'article 6 du présent décret-loi sont tenus d'héberger les systèmes et services électroniques gouvernementaux auprès des fournisseurs de services informatique en nuage ayant obtenu le label conformément aux conditions techniques mentionnées à l'arrêté cité à l'article 12 du présent décret-loi.

Chapitre VI

De la classification selon le degré de sécurité

Art. 15 - Les organismes cités à l'article 6 du présent décret-loi sont soumis à un système de classification obligatoire et périodique.

L'Agence classe les organismes concernés selon le degré de confiance numérique en trois (03) niveaux comme suit :

- Premier niveau : organisme classifié premier degré.
- Deuxième niveau : organisme classifié deuxième degré.
- Troisième niveau : organisme non classifié.

Les niveaux de classifications sont déterminés en fonction des critères suivants :

- L'engagement de l'organisme de l'audit obligatoire de sécurité des systèmes d'information et le degré de son application des recommandations qui en découlent.
- L'utilisation de l'organisme d'équipements et solutions homologués selon la législation en vigueur.
- L'hébergement de l'organisme de ses systèmes auprès d'un fournisseur de service d'hébergement classé conformément aux dispositions de l'article 8 du présent décret-loi.

Les procédures et mécanismes de classification des organismes indiqués à l'article 6 du présent décret-loi et sa publication sont fixés par arrêté du ministre chargé des technologies de la communication.

Art. 16 - Le ministre chargé des technologies de la communication, sur proposition de l'Agence, met en demeure les organismes classés au troisième niveau pour se conformer aux normes appliquées dans le classement dans un délai ne dépassant pas une année.

Art. 17 - En cas d'incident ou d'attaque cybernétique aux organismes mentionnés à l'article 6 du présent décret-loi, ayant entravé l'exploitation d'un système d'information ou d'un réseau de communication ou ayant constitué un danger pour la sécurité de l'espace cybernétique national, l'Agence met en garde l'organisme concerné pour lever les défaillances dans un délai ne dépassant pas trente (30) jours.

Le ministre chargé des technologies de la communication, dans le cas prévu au premier paragraphe du présent article, peut prendre une décision pour isoler temporairement les systèmes d'information et les réseaux afin de protéger le cyberespace, et ce en vertu d'une décision sur rapport motivé de l'Agence.

Chapitre VII

De la réponse aux urgences cybernétiques

Art. 18 - Dans le cadre de réponse aux urgences cybernétiques, l'Agence assure les missions suivantes :

- Elaborer et appliquer le plan national de réponse aux urgences cybernétiques en collaboration avec les centres de réponse aux urgences cybernétiques sectoriels publics et privés.
- Mettre en place les modalités techniques nécessaires à la détection précoce des incidents et attaques cybernétiques qui menacent l'espace cybernétique national.
- Mettre en place et exploiter les canaux de signalement des incidents et attaques cybernétiques.
- Réduire les répercussions des incidents et attaques cybernétiques et garantir la continuité de l'activité et la récupération rapide de leurs effets.
- Alerter les institutions, les administrations et les individus, renforcer les systèmes d'information, gérer les incidents, organiser et coordonner les efforts pour remédier aux faiblesses, les étudier, les analyser et prévoir les solutions appropriées.
- Désigner un point de contact national pour la réponse aux urgences cybernétiques, qui coordonne avec les centres de réponse aux urgences cybernétiques publics ou sectoriels ou privés mentionnés à l'article 19 du présent décret-loi.

Art. 19 - Les organismes mentionnées à l'article 6 du présent décret-loi sont tenues de créer leurs propres centres de réponse aux urgences ou d'adhérer à des centres de réponse aux urgences cybernétiques publics ou sectoriels ou privés.

Les centres de réponse aux urgences cybernétiques doivent obligatoirement coordonner avec le point de contact national mentionné au dernier alinéa de l'article 18 du présent décret-loi.

Art. 20 - Les organismes mentionnés à l'article 6 du présent décret-loi informent immédiatement le point de contact national pour la réponse aux urgences cybernétiques ou le centre de réponse aux urgences cybernétiques des incidents et des attaques cybernétiques et doivent se conformer aux mesures urgentes arrêtées par ces derniers.

Chapitre VIII

Des dispositions spécifiques aux infrastructures numériques d'importance vitale

Art. 21 - La liste des structures qui gèrent les infrastructures numériques d'importance vitale est fixée par décret.

Art. 22 - Les structures qui gèrent des infrastructures numériques d'importance vitale sont tenues de prendre les mesures de sécurité suivantes :

- Utiliser des logiciels et équipements ayant le label « sécurisé ».
- Avoir son propre centre d'hébergement principal et un centre de backup auprès d'un fournisseur de services informatique en nuage ayant obtenu le label.
- Respecter les mesures et les procédures nécessaires pour assurer la continuité d'activité et protéger les bases de données sensibles dont l'atteinte à l'intégrité pourrait affecter à la sécurité nationale en cas de crise cybernétique, et ce selon un manuel de procédure approuvé par décret sur proposition du ministre chargé des technologies de la communication.

Chapitre IX

Des infractions et des sanctions

Section première - De la constatation des infractions

Art. 23 - Les infractions aux dispositions du présent décret-loi sont constatées, sur la base d'un rapport de l'Agence adressé au ministre chargé des technologies de la communication, par des procès-verbaux dressés par deux des agents suivants :

- Les officiers de police judiciaire visés aux numéros 3 et 4 de l'article 10 du code de procédure pénale.
- Les agents assermentés du ministère chargé des technologies de la communication.
- Les Agents assermentés du ministère de l'intérieur.

Les procès-verbaux sont transmis au ministre chargé des technologies de la communication qui les transmet, pour poursuite, au procureur de la République territorialement compétent.

Section 2 - Des sanctions administratives

Art. 24 - Le ministre chargé des technologies de la communication peut, sur rapport motivé de l'Agence, dégrader les organismes mentionnés à l'article 6 du présent décret-loi, et classés aux premier et deuxième niveaux, et ce dans les cas suivants :

- La non-réalisation de l'audit obligatoire et périodique de sécurité des systèmes d'information.
- Le défaut de remise à l'Agence d'une copie électronique protégée du rapport d'audit dans le délai mentionné à l'article 8 du présent décret-loi.
- La non-exécution des recommandations du rapport d'audit ou leur exécution partielle dans un délai n'excédant pas une année.
- Le non-respect des mesures d'urgence prescrites par le point de contact national pour la réponse aux urgences cybernétiques ou les centres de réponse aux urgences cybernétiques suite à la survenance d'un incident ou d'une attaque cybernétique.
- Le non-relève des défaillances dans le délai mentionné à l'article 17 du présent décret-loi.
- La non-création d'un centre de réponse aux urgences cybernétiques ou la non-adhésion aux centres de réponse aux urgences cybernétiques.
- Le non-respect du référentiel mentionné à l'article 14 du présent décret-loi.

Section 3 - Des sanctions financières

Art. 25 - Est puni d'une amende de cinquante mille (50 000) dinar à cent mille (100 000) dinar les organismes mentionnés à l'article 6 du présent décret-loi, et classés au troisième niveau, et ce dans les cas suivants :

- La non-réalisation de l'audit obligatoire et périodique de sécurité des systèmes d'information.
- La non-exécution des recommandations du rapport d'audit ou leur exécution partielle dans un délai n'excédant pas une année.
- Le non-respect des mesures d'urgence prescrites par le point de contact national pour la réponse aux urgences cybernétiques ou les centres de réponse aux urgences cybernétiques suite à la survenance d'un incident ou d'une attaque cybernétique.
- Le non-relève des défaillances dans le délai mentionné à l'article 17 du présent décret-loi.
- La non-création d'un centre de réponse aux urgences cybernétiques ou la non adhésion aux centres de réponse aux urgences cybernétiques.

Chapitre X

Dispositions finales

Art. 26 - Les règles de conclusion, d'exécution et de contrôle des marchés et consultations liées à la spécificité des attributions de l'Agence sont fixées par décret.

Art. 27 - L'Agence créée par l'article 4 du présent décret-loi se substitue à l'Agence nationale de sécurité informatique créée par l'article 2 de la loi n° 2004-5 du 3 février 2004 relative à la sécurité informatique. Tous ses biens, droits et obligations lui sont transférés.

En cas de dissolution de l'Agence, ses biens feront retour à l'Etat qui exécutera ses obligations et ses engagements conformément à la législation en vigueur.

Art. 28 - Sont abrogées, à compter de la date d'entrée en vigueur du présent décret-loi, toutes les dispositions qui lui sont contraires, notamment celles de la loi n° 2004-05 du 3 février 2004 relative à la sécurité informatique.

Art. 29 - L'expression « Agence nationale de la sécurité informatique » est remplacée là où elle figure dans les textes législatifs et réglementaires par L'expression « Agence nationale de la cybersécurité ».

Art. 30 - Les dispositions du présent décret-loi entrent en vigueur six (6) mois après la date de sa publication au Journal officiel de la République tunisienne.

Art. 31 - Le présent décret-loi sera publié au Journal officiel de la République tunisienne.

Tunis, le 11 mars 2023.

Le Président de la République

Kaïs Saïed