**BURKINA FASO**
---
Unité - Progrès - Justice

**DÉCRET N° 2024-0842/PRES promulguant la loi n° 014-2024/ALT du 09 juillet 2024 portant sécurité des systèmes d'information au Burkina Faso**

**LE PRÉSIDENT DU FASO,**
**CHEF DE L'ÉTAT,**
**PRÉSIDENT DU CONSEIL DES MINISTRES,**

**Vu** la Constitution ;

**Vu** la Charte de la Transition du 14 octobre 2022 et son modificatif du 25 mai 2024 ;

**Vu** la lettre n°2024-069/ALT/PRES/SG/DGLCP/DSCACP du 11 juillet 2024 du Président de l'Assemblée législative de Transition transmettant pour promulgation la loi n° 014-2024/ALT du 09 juillet 2024 portant sécurité des systèmes d'information au Burkina Faso ;

**DÉCRÈTE**

**Article 1 :** Est promulguée la loi n° 014-2024/ALT du 09 juillet 2024 portant sécurité des systèmes d'information au Burkina Faso.

**Article 2 :** Le présent décret sera publié au Journal officiel du Faso.

**Ouagadougou, le** 24 juillet 2024

BURKINA FASO
LE PRESIDENT

**Capitaine Ibrahim TRAORE**

BURKINA FASO

-=-=-=-=-=-

UNITE-PROGRES-JUSTICE

-=-=-=-=-=-

ASSEMBLEE LEGISLATIVE
DE TRANSITION

IVE REPUBLIQUE

-=-=-=-=-

TROISIEME LEGISLATURE DE TRANSITION

# LOI N°014-2024/ALT

# PORTANT SECURITE DES SYSTEMES D'INFORMATION AU BURKINA FASO

# L'ASSEMBLEE LEGISLATIVE DE TRANSITION

Vu la Constitution ;

Vu la Charte de la Transition du 14 octobre 2022 et son modificatif du 25 mai 2024 ;

Vu la résolution n°001-2022/ALT du 11 novembre 2022 portant validation du mandat des députés ;

Vu la résolution n°003-2022/ALT du 14 novembre 2022 portant règlement de l'Assemblée législative de transition ;

a délibéré en sa séance du 09 juillet 2024

et adopté la loi dont la teneur suit :

## CHAPITRE 1 : DES DISPOSITIONS GENERALES

### Section 1 : De l'objet, du but et du champ d'application

**Article 1 :**

La présente loi porte sur la sécurité des systèmes d'information au Burkina Faso.

**Article 2 :**

La présente loi fixe les règles relatives à la sécurité des systèmes d'information en permettant notamment :

- de contrôler et de protéger les systèmes d'information ;
- d'identifier et de gérer les risques et incidents relatifs à la sécurité des systèmes d'information ;
- de réduire les conséquences des incidents de sécurité des systèmes d'information ;
- de régir les acteurs intervenant dans la sécurisation des systèmes d'information.

**Article 3 :**

La présente loi s'applique :

- aux systèmes d'information de l'Administration publique et des organismes à infrastructure critique y compris ceux présentant des intérêts militaires ou relevant de la cyberdéfense ;
- aux systèmes d'information des opérateurs de réseaux de communications électroniques et des prestataires de services de confiance ;
- aux systèmes d'information des personnes physiques et morales ayant un impact économique et social ou sécuritaire au Burkina Faso ;

- à toute structure assurant l'assistance et la maintenance sur les systèmes d'information de l'Administration publique ou privée.

## Section 2: Des définitions

### Article 4 :

Au sens de la présente loi, on entend par :

- Accréditation : processus d'évaluation et de reconnaissance par une autorité administrative des capacités d'une personne physique ou morale à réaliser des activités specifiques ;

- Agrément technique : reconnaissance des capacités techniques de toute entreprise à exercer dans un domaine donné ;

- Audit de sécurité d'un système d'information : 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 notamment organisationnels, techniques, humains, financiers investis au regard des risques encourus, d'optimisation, de rationalité et de performance ;

- Confidentialité : maintien du secret des informations et des transactions afin de prévenir la divulgation non autorisée d'informations aux non destinataires permettant la lecture, l'écoute, la copie illicite d'origine intentionnelle ou accidentelle durant leur stockage, traitement ou transfert ;

- Contenu : ensemble d'informations relatives aux données appartenant à des personnes physiques ou morales, transmises ou reçues à travers les réseaux de communications électroniques et les systèmes d'information ;

- Cybercriminalité : activités criminelles dont les ordinateurs et systèmes informatiques constituent soit l'arme soit la cible principale. La cybercriminalité recouvre les délits habituels

(fraude, contrefaçon et usurpation d'identité par exemple), les délits liés au contenu (distribution en ligne de matériel pédopornographique ou incitation à la haine raciale par exemple) et les délits spécifiques aux ordinateurs et systèmes informatiques (attaque contre un système informatique, déni de service et logiciel malveillant par exemple) ;

- Cyberdéfense : ensemble des mesures permettant à l'Etat de défendre, dans le cyberespace, les systèmes d'information jugés essentiels ;

- Cyberespace : espace artificiel constitué par l'interconnexion de l'ensemble des équipements de traitement de l'information numérique, à la fois immatérielle, technologique et informationnelle ;

- Cybersécurité : ensemble de mesures de prévention, de protection et de dissuasion d'ordre technique, organisationnel, juridique, financier, humain, procédural et autres actions permettant d'atteindre les objectifs de sécurité fixés à travers les réseaux de communications électroniques, les systèmes d'information et pour la protection de la vie privée des personnes ou état recherché par un système d'information lui permettant de résister à des événements issus du cyberespace susceptible de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles ;

- Disponibilité : critère de sécurité permettant l'accessibilité et l'utilisation selon les besoins des ressources de communications électroniques, des systèmes d'information ou des équipements terminaux ;

- Données : représentation de faits, d'informations ou de notions sous une forme susceptible d'être traitée par un équipement terminal, y compris un programme permettant à ce dernier d'exécuter une fonction ;

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

- Exploitant du système d'information : toute personne physique ou morale qui exploite un réseau de communications électroniques ouvert au public ou à toute personne physique ou morale qui fournit un service de communications électroniques ;

- Fiabilité : aptitude d'un système d'information ou d'un réseau de télécommunications à fonctionner sans incident pendant un temps d'observation prédéfini ;

- Fournisseur d'accès à Internet : toute personne physique ou morale fournissant au public un accès à Internet ;

- Homologation : processus permettant d'une part de donner une assurance des propriétés de sécurité d'une solution de sécurité (matériel ou logiciel) ou d'un système d'information et d'autre part de renseigner d'une manière rationnelle sur les risques résiduels qui correspondent à l'utilisation ;

- Infrastructures critiques : installations, ouvrages et systèmes qui sont indispensables au maintien des fonctions vitales de la société et qui contribuent fortement à la santé, à la sûreté, à la sécurité et au bien-être économique ou social, et dont le dommage, l'indisponibilité ou la destruction aurait un impact induisant la défaillance de ces fonctions ;

- 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 permettant 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 ;

- Logiciel : ensemble des programmes, procédés et règles, et éventuellement de la documentation, relatifs au fonctionnement d'un ensemble de traitement de données ;

- Logiciel espion : type particulier de logiciel trompeur collectant tout type d'informations sur un terminal ou un système d'information sans autorisation ;

- Logiciel potentiellement indésirable : logiciel présentant des caractéristiques d'un logiciel trompeur ou d'un logiciel espion ;

- 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 le 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 ;

- Métadonnée : donnée synthétisant des informations élémentaires sur d'autres données ;

- Organisme à infrastructures critiques : organisme abritant une ou plusieurs infrastructure(s) critique(s) ;

- Prestataire de service de confiance : entité qui fournit des services de certification électronique et de signature électronique. Le prestataire de service de confiance est responsable de la création, de la distribution et de la gestion des certificats électroniques qui sont utilisés pour authentifier les signataires et garantir l'intégrité des documents signés électroniquement ;

- Sécurité des systèmes d'information : ensemble des mesures de protection et de répression numériques impliquant la cybersécurité, la cyberdéfense et la cybercriminalité ;

- Système d'information : ensemble organisé de ressources humaines, matérielles, organisationnelles, procédurales, technologiques, informatiques permettant de collecter, stocker, traiter et distribuer de l'information ;

- Système informatique : 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 ;

- Traçabilité : garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.

## CHAPITRE 2 : DES REGLES DE SECURISATION DES SYSTEMES D'INFORMATION

### Section 1 : Des principes généraux

### Article 5 :

La sécurité des systèmes d'information est régie par les principes suivants :

- le principe de sécurité et de sauvegarde de la souveraineté nationale dans le respect des droits et libertés fondamentaux notamment le principe du droit de la défense ;

- le principe de la proportionnalité en matière de sécurité ;

- le principe d'égalité de traitement dans la protection de tous les systèmes d'information dans les circonstances analogues ;

- le principe de neutralité technologique en matière de sécurité des systèmes d'information, sur l'ensemble du territoire national ;

- le principe d'appropriation des normes de sécurité des systèmes d'information par les acteurs.

## Section 2 : Des règles de contrôle et de protection des systèmes d'information

### Article 6 :

Le contrôle et la protection des systèmes d'information sont assurés par l'organe national en charge du contrôle et de la protection du cyberespace national.

L'organe national en charge du contrôle et de la protection du cyberespace national est habilité à installer, sur les réseaux publics de télécommunications, ceux des fournisseurs d'accès à internet ainsi que ceux des organismes à infrastructures critiques, des dispositifs techniques aux seules fins de détecter les évènements susceptibles d'affecter la sécurité des systèmes d'information nationaux.

Ces dispositifs sont installés pour la duré et dans la mesure strictement necessaire à la caractérisation de la menace.

L'organe national en charge du contrôle et de la protection du cyberespace national est créé par un décret pris en Conseil des ministres.

### Article 7 :

Toute activité d'importation, de vente de matériels ou de logiciels destinée à la sécurité des systèmes d'information est conditionnée par la possession d'un agrément technique délivré par l'organe national de contrôle et de la protection prévu à l'article 6 ci-dessus.

Les conditions et modalités d'octroi, de renouvellement et de retrait des agréments techniques en matière de sécurité des systèmes d'information sont précisées par voie règlementaire.

### Article 8 :

Tout auditeur de sécurité des systèmes d'information des organismes à infrastructures critiques dispose d'une accréditation de l'organe national en charge du contrôle et de la protection du cyberespace national.

Les conditions et modalités d'octroi, de renouvellement et de retrait d'une accréditation sont précisées par voie règlementaire.

**Article 9 :**

Le matériel ou logiciel destiné à la sécurité des systèmes d'information des organismes à infrastructures critiques est homologué par l'organe national en charge du contrôle et de la protection du cyberespace national.

Nonobstant les dispositions de l'alinéa 1 ci-dessus, tout autre organisme concepteur ou promoteur peut soumettre tout matériel et logiciel destiné à la sécurité des systèmes d'information à homologation suivant les conditions prévues par voie règlementaire.

La liste des matériels et logiciels concernés ainsi que les organismes soumis sont déterminés par voie règlementaire.

**Article 10 :**

Toute personne commise à des opérations d'audit, d'homologation, d'accréditation et de délivrance d'agrément technique est soumise à l'obligation du secret professionnel sur les renseignements et documents recueillis ou portés à sa connaissance à l'occasion de l'exercice de sa mission.

L'obligation de secret professionnel pèse sur cette personne pendant et après la durée de sa mission.

Les sanctions prévues par le code pénal en matière de secret professionnel s'appliquent aux alinéas précédents.

**Article 11 :**

Le secret professionnel et le secret des affaires ne peuvent être opposés à l'organe national en charge du contrôle et de la protection du cyberespace ainsi qu'à toute personne régulièrement commise pour l'assister ou le conseiller dans le cadre de la présente loi.

Toute personne appelée à fournir des informations audit organe en charge du contrôle et de la protection est déliée de son obligation professionnelle de discrétion.

**Article 12 :**

La délivrance, la modification et le retrait d'une accréditation, d'un agrément ou d'une homologation sont faits par l'organe national en charge du contrôle et de la protection du cyberespace national.

Il est annexé à l'acte d'accréditation ou l'agrément un cahier des charges fixant les droits et les obligations du titulaire.

## CHAPITRE 3 : DES OBLIGATIONS ET DES SANCTIONS

### Section 1 : Des obligations des exploitants des systèmes d'information

**Article 13 :**

Les exploitants des systèmes d'information ont l'obligation :

- de conserver au Burkina Faso les métadonnées de connexion et de trafic de leurs systèmes d'information pendant une période de trois ans minimum, de nature à pouvoir obtenir une traçabilité complète des données et des utilisateurs, dans le respect des textes en vigueur. Les données conservées doivent être accessibles lors des investigations conformément aux textes en vigueur ;

- d'installer à leurs frais des mécanismes de surveillance, de contrôle d'accès aux données de leurs systèmes d'information conformément aux normes édictées par l'organe national en charge du contrôle et de la protection du cyberespace national ;

- d'évaluer, de réviser leurs systèmes de sécurité et d'introduire en cas de nécessité les modifications appropriées dans leurs pratiques, mesures et techniques de sécurité en fonction de l'évolution des technologies et des menaces du moment ;

- de garantir la sécurité des systèmes d'information, leur intégrité et d'empêcher leur accès par des tiers non autorisés ;

- de garantir la pérennité et la mutation des systèmes d'information et des données par rapport à l'évolution technologique ;

- de sécuriser les transactions électroniques par tout moyen approuvé par l'autorité compétente conformément aux textes en vigueur ;

- de déclarer à l'organe national en charge du contrôle et de la protection du cyberespace tout incident de sécurité à impact critique survenu sur son système d'information conformément aux modalités fixées par ledit organe ;

- de réaliser la cartographie des risques et incidents et de la tenir périodiquement à jour ;

- de respecter, en cas d'externalisation des systèmes d'information sensibles, les exigences en matière de sécurité des systèmes d'information préalablement fixées par l'organe national en charge du contrôle et de la protection du cyberespace national et celles relatives à la protection des organismes à infrastructures critiques, notamment par la conclusion d'un contrat de droit burkinabè intégrant des engagements de protection de l'information, d'auditabilité, de réversibilité et des exigences de sécurité et des niveaux de service voulus ;

- de mettre en place des moyens nécessaires pour la supervision et la détection des cyberattaques et de transmettre dans les quarante-huit heures, après constat d'un incident, les données techniques générées à l'organe national en charge du contrôle et de la protection du cyberespace national.

**Article 14 :**

Pour assurer la sécurité des systèmes d'information, les exploitants des systèmes d'information :

- prennent toutes les mesures techniques et administratives afin de garantir la sécurité des services offerts ;

- se dotent de systèmes normalisés leur permettant d'identifier, d'évaluer, de traiter et de gérer de façon continue les risques liés à la sécurité des systèmes d'information dans le cadre des services offerts directement ou indirectement ;

- mettent en place des mécanismes techniques conformément aux normes et aux règles nationales en vigueur pour faire face aux atteintes préjudiciables à la sécurité des systèmes d'information ;

- protègent les plates-formes des systèmes d'information contre d'éventuelles intrusions qui peuvent compromettre l'intégrité des données transmises et contre toute cyberattaque ;

- informent les utilisateurs de l'interdiction faite d'utiliser le réseau de communication pour éditer, consulter ou diffuser des contenus illicites ou toute autre action pouvant compromettre la sécurité des réseaux ou des systèmes d'information, de l'interdiction de concevoir des logiciels trompeurs, espions, potentiellement indésirables ou tout autre outil conduisant à un comportement frauduleux dans le but de perpétrer des actions malveillantes ;

- assurent la confidentialité, l'accessibilité, la disponibilité et l'intégrité des systèmes d'information de leurs clients ;

- assurent l'intégrité des données pendant leur transfert.

**Article 15 :**

Les systèmes d'information des organismes publics et privés sont soumis à un régime d'audit de sécurité périodique.

Un décret en Conseil des ministres fixe les types d'audits, leurs modalités et conditions de réalisation.

**Article 16 :**

Les rapports issus des audits périodiques sont confidentiels et ampliation est faite à l'organe national en charge du contrôle et de la protection du cyberespace national.

**Section 2 : Des sanctions**

**Article 17 :**

L'organe national en charge du contrôle et de la protection du cyberespace national constate et sanctionne les manquements des exploitants des systèmes d'information à leurs obligations, conformément aux dispositions de la présente loi.

L'organe national en charge du contrôle et de la protection du cyberespace national prend les mesures appropriées ou saisit l'autorité compétente, lorsqu'il a connaissance de faits constitutifs de violation des lois et règlements.

**Article 18 :**

En cas de non-respect de l'obligation contenue à l'article 15 de la présente loi, l'organe national en charge du contrôle et de la protection du cyberespace national met en demeure la structure concernée de s'exécuter dans un délai fixé par voie règlementaire.

Si à l'expiration de ce délai, la structure mise en demeure ne se conforme pas, l'organe national en charge du contrôle et de la protection du cyberespace national désigne, aux frais de la structure contrevenante, un expert qui sera chargé de l'audit de sécurité.

En fonction de la complexité du système d'information, de son étendue géographique et de sa criticité, l'organe national en charge du contrôle et de la protection du cyberespace national prononce à l'encontre de l'organisme une amende allant de cinq millions (5 000 000) à cent millions (100 000 000) de francs CFA.

En cas de récidive, l'amende encourue est de un à cinq pour cent du chiffre d'affaires du dernier exercice clos de l'organisme. Dans tous les cas, l'amende prononcée est supérieure à la précédente.

**Article 19 :**

En cas de non-respect des dispositions prévues aux articles 13 et 14 de la présente loi, exception faite de l'obligation de déclaration des incidents de sécurité à impact critique, l'organe national en charge du contrôle et de la protection du cyberespace national met en demeure l'organisme concerné qui s'exécute dans un délai fixé par voie règlementaire.

Si à l'expiration du délai prescrit, l'organisme mis en demeure ne se conforme pas, l'organe national en charge du contrôle et de la protection du cyberespace national prononce à son encontre une amende allant d'un million (1 000 000) à cent millions (100 000 000) de francs CFA sans préjudice de toute poursuite judiciaire.

En cas de récidive, l'organe national en charge du contrôle et de la protection du cyberespace national prononce une nouvelle amende à son encontre.

Dans tous les cas, l'amende prononcée pour la récidive est au moins égale au double de la précédente.

L'organisme peut, en outre, être contraint de déconnecter son système d'information du réseau national et international ou être interdit d'exercer son activité pendant une durée fixée par voie règlementaire.

**Article 20 :**

Le titulaire d'une accréditation, d'une homologation ou d'un agrément technique en matière de sécurité des systèmes d'information ou l'organisme à infrastructure critique est mis en demeure de conformité par l'organe national en charge du contrôle et de la protection du cyberespace national en cas de manquement constaté.

La mise en demeure du titulaire est assortie d'un délai qui lui est notifié par l'organe de contrôle après information des griefs qui lui sont reprochés.

**Article 21 :**

Lorsque le mis en cause remédie au manquement dans le délai prescrit, l'organe national en charge du contrôle et de la protection du cyberespace national lui en donne quitus, au plus tard dans les quinze jours suivant la constatation de la réparation du manquement.

**Article 22 :**

Lorsque le mis en cause ne se conforme pas à la mise en demeure conformément à l'article 20 de la présente loi dans le délai prescrit, l'organe national en charge du contrôle et de la protection, en fonction de la gravité du manquement, prononce à son encontre une amende allant d'un million (1 000 000) à cinquante millions (50 000 000) de francs CFA sans préjudice de toute poursuite judiciaire.

La décision visée à l'alinéa ci-dessus est assortie d'un nouveau délai prescrit au contrevenant pour qu'il remédie à son manquement.

**Article 23 :**

Lorsque le manquement est grave ou répété et que les mesures prises en vertu de l'article 22 ci-dessus de la loi n'ont pas permis d'y remédier, l'organe national en charge du contrôle et de la protection du cyberespace national prononce l'une des sanctions suivantes :

- la suspension de l'accréditation, de l'agrément technique ou de l'homologation pour une durée de deux ans au maximum ;
- la réduction de la durée de l'accréditation, de l'agrément technique ou de l'homologation ;
- le non renouvellement de l'accréditation, de l'agrément technique ou de l'homologation ;
- le retrait de l'accréditation, de l'agrément technique ou de l'homologation.

Nonobstant le retrait de l'accréditation, de l'agrément technique ou de l'homologation, l'organe national en charge du contrôle et de la protection du cyberespace national prononce à l'encontre du contrevenant une interdiction définitive d'exercice de l'activité.

**Article 24 :**

En cas de manquement aux dispositions de la présente loi par des experts commis d'office conformément à l'article 18 de la présente loi, l'organe national en charge du contrôle et de la protection du cyberespace national prononce l'une des sanctions suivantes :

- la suspension de l'accréditation ;
- le retrait de l'accréditation ;
- l'interdiction d'exercer sur tout le territoire national pendant une durée déterminée par voie règlementaire qui n'excède pas douze mois.

**Article 25 :**

En cas de manquements d'un organisme relatifs à l'utilisation d'un matériel ou d'un logiciel non homologué destiné à la sécurité des systèmes d'information dans le réseau de l'Administration publique, de ses démembrements ou d'un organisme à infrastructure critique, l'organe national en charge du contrôle et de la protection du cyberespace national met en demeure l'organisme concerné qui doit s'exécuter dans un délai fixé par voie règlementaire.

Si à l'expiration de ce délai, l'organisme mis en demeure ne se conforme pas, l'organe national en charge du contrôle et de la protection du cyberespace national prononce à son encontre une amende allant de deux millions (2 000 000) à cent millions (100 000 000) de francs CFA.

En cas de récidive, l'organe en charge du contrôle et de la protection du cyberespace national prononce une nouvelle amende à l'encontre de cet organisme.

Dans tous les cas, l'amende prononcée pour la récidive est au moins égale au double de la première amende.

**Article 26 :**

Pour les manquements d'un organisme relatifs à des activités d'importation et de vente sans agrément technique de matériels ou de logiciels liés à la sécurité des systèmes d'information, l'organe national en charge du contrôle et de la protection du cyberespace national met en demeure l'organisme concerné qui devra s'exécuter dans un délai fixé par voie règlementaire.

Si à l'expiration de ce délai, l'organisme interpellé ne se conforme pas, l'organe en charge du contrôle et de la protection du cyberespace national prononce à son encontre une amende allant de deux millions (2 000 000) à cent millions (100 000 000) de francs CFA.

**Article 27 :**

L'organe national en charge du contrôle et de la protection du cyberespace national procède à des missions de vérifications et de contrôles inopinés ou non au niveau de tout exploitant de système d'information ou tout détenteur d'une accréditation, d'un agrément technique ou d'une homologation.

En cas de rétention d'information ou d'entrave à son action lors du contrôle d'une structure, l'organe en charge du contrôle et de la protection du cyberespace national prononce à son encontre, une amende allant d'un million (1 000 000) à vingt millions (20 000 000) de francs CFA.

**Article 28 :**

En cas d'urgence, l'organe national en charge du contrôle et de la protection du cyberespace national prend toutes les mesures conservatoires qu'il juge nécessaires.

Les cas d'urgence et la durée des mesures conservatoires sont fixés par voie règlementaire.

## CHAPITRE 4 : DES DISPOSITIONS DIVERSES, TRANSITOIRES ET FINALES

**Article 29 :**

Les missions de protection et de contrôle des organismes à infrastructures critiques présentant un interêt militaire relèvent de la compétence du Ministère en charge de la défense nationale.

Les modalités d'exercice des missions de protection et de contrôle des organismes à infrastructures critiques présentant un intérêt militaire sont déterminées par voie règlementaire.

**Article 30 :**

Les agréments techniques, accréditations, homologations, autorisations et déclarations en cours de validité doivent se conformer à la présente loi au plus tard un an après son entrée en vigueur.

**Article 31 :**

Une procédure commune et un cadre de concertation sont mis en place par voie règlementaire.

**Article 32 :**

Les modalités de recouvrement des amendes et leur répartition sont fixées par voie règlementaire.

**Article 33 :**

La présente loi qui abroge toutes dispositions antérieures contraires sera exécutée comme loi de l'Etat.

Ainsi fait et délibéré en séance publique

à Ouagadougou, le 09 juillet 2024

Le Président

ASSEMBLEE LEGISLATIVE DE TRANSITION
Le Président

**Dr Ousmane BOUGOUMA**

La Secrétaire de séance

**Linda Gwladys KANDOLO**