BURKINA FASO

Unité-Progrès-Justice

IV^{E} REPUBLIQUE

TROISIEME LEGISLATURE DE TRANSITION

Session permanente

ASSEMBLEE LEGISLATIVE DE TRANSITION

TEXTE ISSU DE LA COMMISSION DU DEVELOPPEMENT DURABLE (CDD)

Dossier n°096

PROJET DE LOI N°_____/ALT PORTANT SECURITE DES SYSTEMES D'INFORMATION AU BURKINA FASO

Juillet 2024

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** ;[1]

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[2] ;

a délibéré en sa séance du……...

et adopté la loi dont la teneur suit :

1 Insérer « du 14 octobre 2022 et son modificatif du 25 mai 2024 » après « Transition »

2 Créer et insérer un 4e visa et lire « Vu la résolution n°003-2022/ALT du 14 novembre 2022 portant règlement de l'Assemblée législative de transition »

CHAPITRE 1[3] **: DES** DISPOSITIONS GENERALES[4]

Section 1 : De l'objet**, du but** et **du** champ d'application[5]

Article 1 nouveau :[6]

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

Article **2** :[7]

La présente loi **fixe**[8] 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[9] les conséquences des incidents de sécurité des systèmes d'information ;[10]
- de régir les acteurs intervenant dans la sécurisation des systèmes d'information.

Article **3** :[11]

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**[12] 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 ;

---

3 Remplacer « TITRE I » par « CHAPITRE 1 ». Dans tout le texte, remplacer les TITRES par des CHAPITRES et les CHAPITRES par des Sections

4: Insérer «DES » avant « DISPOSITIONS GENERALES »

5Remplacer « Objet et champ d'application » par « De l'objet, du but et du champ d'application »

6 Créer et insérer un nouvel article 1 et lire « La présente loi porte sur la sécurité des systèmes d'information au Burkina Faso »

7 Article 2 nouveau = Article 1 ancien

8 Remplacer « a pour objet de fixer » par « fixe »

9 Supprimer « au minimum » après « réduire »

10» Remplacer le point « . » après « systèmes d'information » par un point-virgule « ; »

11 Article 3 nouveau = Article 2 ancien»

12 Remplacer la virgule « , » par « et »

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

Section 2: Des[13] définitions

Article **4** **:**[14]

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**[15] **;**
- **Agrément technique :reconnaissance des capacités techniques de toute entreprise à exercer dans un domaine donné**[16] **;**
- 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**

13 Insérer « des » avant « définitions »
14 Article 4 nouveau= Article 3 ancien
15 Créer et insérer un tiret pour définir « Accréditation
16 Créer et insérer un tiret pour définir « Agrément »

ordinateurs et systèmes informatiques (attaque contre un système informatique, déni de service et logiciel malveillant par exemple)[17] ;

- 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[18], à la fois immatériel**le**[19], 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 **;**[20]
- 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 ;

---

17 Remplacer « ensemble des actes contrevenant à la législation nationale ou aux traités internationaux ratifiés, ayant pour cible les réseaux ou les systèmes d'information ou les utilisant comme moyens de la commission d'un délit ou d'un crime » par « 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) »

18 Remplacer « numériques mondial » par « numérique »»

19 Remplacer « immatériel » par « immatérielle »

20 Remplacer le point « . » par un point-virgule « ; »

- 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[21] ;**

- 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[22]** 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 ;

21 Créer et insérer un nouveau tiret pour définir « Homologation »
22Remplacer « permet » par « permettant »

- 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 **;**[23]
- 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 **;**[24]
- 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 **;**[25]
- **Traçabilité**[26] **:** garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.

[23] Remplacer le point « . » par un point-virgule « ; »
24 Remplacer le point « . » par un point-virgule « ; »
25 Remplacer le point « . » par un point-virgule « ; »
26 Ecrire « Tracabilité » avec « ç »

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

Section 1 : Des principes généraux

Article **5** **:**[27]

La sécurité des systèmes d'information[28] 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** [29]de la défense ;
- **le principe de la proportionnalité en matière de sécurité ;**[30]
- 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 regles de controle et de protection des systèmes d'information

Article **6** **:**[31]

Le contrôle et la protection des **s**ystèmes d'**i**nformation[32] 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 créé [33]par un décret pris en Conseil des ministres.

Article **7** **:**[34]

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

27 Article 5 nouveau = article 4 ancien
28 Supprimer le « s » à « informations »
29 remplacer « des droits »par « du droit », supprimer « et » après « défense »
30 Détacher le membre de phrase « le principe de la proportionnalité en matière de sécurité » du 1er tiret pour en faire un 2e tiret nouveau
31 Article 6 nouveau = Article 5 ancien
32 Ecrire « Systèmes d'Information » avec « s » et « i » minuscules
33 Supprimer « ou identifié » après « est créé »
34 Article 7 nouveau = Article 6 ancien

agrément **technique**[35] délivré par l'organe national de contrôle et de la protection prévu à l'article **6**[36] 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.**[37]

Article **8** **:**[38]

Tout auditeur de sécurité des systèmes d'information des **o**rganismes à **i**nfrastructures **c**ritiques[39] **dispose**[40] 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.[41]

Article **9** **:**[42]

Le matériel ou logiciel destiné à la sécurité des systèmes d'information des **o**rganismes à **i**nfrastructures **c**ritiques[43] **est**[44] homologué par l'organe national en charge du contrôle et de la protection du cyberespace national.

[45]Nonobstant les dispositions **de l'alinéa 1 ci-dessus,** [46], tout autre organisme **concepteur ou promoteur**[47] peut soumettre tout matériel et logiciel destiné à la sécurité des systèmes d'information à homologation suivant les conditions prévues **par voie règlementaire.**[48]

35 Insérer « technique » après « agrément »
36 Remplacer « l'articel 5 » par « l'article 6 »
37 Remplacer « décret en Conseil des ministres » par « voie règlementaire »
38 Article 8 nouveau = Article 7 ancien
39 Ecrire« Organismes à Infrastructures Critiques » avec « o », « i » et « c » minuscules
40 Remplacer « doit disposer » par « dispose »
41 Créer et insérer un nouvel alinéa et lire « Les conditions et modalités d'octroi, de renouvellement et de retrait d'une accréditation sont précisées par voie règlementaire »
42 Article 9 nouveau = Article 8 ancien
43 Ecrire« Organismes à Infrastructures Critiques » avec « o », « i » et « c » minuscules
44 Remplacer « doit être » par « est »
45 Détacher la première phrase du 2e alinéa pour en faire un 3e alinéa nouveau

46 Remplacer « les présentes dispositions » par « les dispositions de l'alinéa 1 ci-dessus »
47 Insérer « concepteur ou promoteur » après « organisme »
48 Remplacer « aux articles 11 et 12 de la présente loi » par « par voie règlementaire »

La liste des matériels et logiciels concernés ainsi que les organismes soumis sont déterminés par voie règlementaire[49].

Article **10** **:[50]**

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[51].

Article **11[52]** **:**

Le secret professionnel et le secret des affaires ne peuvent être opposés[53] à l'organe national en charge du contrôle et de la protection du cyberespace ainsi que 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.

49 Détacher la première phrase du 2e alinéa pour en faire un 3e alinéa nouveau et lire « La liste des matériels et logiciels concernés ainsi que les organismes soumis sont déterminés par voie règlementaire »

50 Article 10 nouveau = Article 9 ancien.

51 Remplacer le contenu de l'article 9 ancien par « Toute personne commise à des opérations d'audit, d'homologation, d'accréditation et de délivrance d'agrément 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. »

52 Article 11 nouveau = Article 10 ancien

53 Enlever le gras à « et le secret des affaires ne peuvent être opposés »

CHAPITRE 3 ancien : **Supprimé**

Article **12**[54] **:**

La délivrance, la modification et le retrait d'une accréditation, d'un agrément **ou**[55] 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.

Article 12 ancien : Supprimé

CHAPITRE 3 : DES OBLIGATIONS **ET DES** SANCTIONS[56]

Section 1 : Des obligations des exploitants des systemes 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[57] 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 de 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 ;
- [58]

54 Article 12 nouveau = Article 11 ancien
55 Remplacer « et » par « ou »
56 Remplacer «OBLIGATIONS ET SANCTIONS » par «DES OBLIGATIONS ET DES SANCTIONS »
57 Supprimer « (03) » après « trois »
58 Supprimer le 4e tiret

- de garantir la sécurité des systèmes d'information[59], 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[60] 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** :[61]

- **prennent**[62] toutes les mesures techniques et administratives afin de garantir la sécurité des services offerts ;
- **se dotent**[63] de systèmes normalisés leur permettant d'identifier, d'évaluer, de traiter et de gérer de façon continue les risques liés à la

59 Supprimer « et des données » après « information »
60 Supprimer « (48) » après « quarante-huit »
61 Remplacer « desdits systèmes doivent » par « des systèmes d'information »
62 Remplacer « prendre » par « prennent »
63 Remplacer « se doter » par « se dotent »

sécurité des systèmes d'information dans le cadre des services offerts directement ou indirectement ;

- **mettent**[64] 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**[65] les plates-formes des systèmes d'information contre d'éventuelles intrusions qui peuvent compromettre l'intégrité des données transmises et contre toute cyberattaque ;
- **informent**[66] 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, espion**s**[67], potentiellement indésirables ou tout autre outil conduisant à un comportement frauduleux dans le but de perpétrer des actions malveillantes ;
- **assurent**[68] la confidentialité, l'accessibilité, la disponibilité et l'intégrité des systèmes d'information de leurs clients ;
- **assurent** [69] 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[70]**.**

Article 16 :

Les rapports issus des audits périodiques[71] sont confidentiels et ampliation est faite à l'organe national en charge du contrôle et de la protection du cyberespace national.

64 Remplacer « mettre » par « mettent »
65 Remplacer « protéger » par « protègent »
66 Remplacer « informer » par « informent »
67 Ecrire « espion » avec un « s » à la fin
68 Remplacer « assurer » par « assurent »
69Remplacer « assurer » par « assurent »
70 Remplacer le contenu du 2e alinéa par : « Un décret en Conseil des ministres fixe les types d'audits, leurs modalités et conditions de rélisation »
71 Remplacer « les rapports d'audit » par « Les rapports issus des audits périodiques »

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**[72], 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**.[73]

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**[74], aux frais de la structure contrevenante, un expert qui sera chargé de l'audit **de sécurité**[75].

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**[76] à l'encontre de l'organisme une amende 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[77] à cinq **pour cent**[78] du chiffre d'affaires du dernier exercice clos de l'organisme. **Dans tous les cas, l'amende prononcée est supérieure à la précédente**.[79]

72 Insérer « à leurs obligations » après « d'information »
73 Remplacer « lui » par « voie règlementaire »
74 Remplacer « est tenu de désigner » par « désigne »
75 Remplacer « sus-indiqué » par « de sécurité »
76 Remplacer « peut prononcer » par « prononce »
77 Supprimer « (1) » après « un »
78 Supprimer « (5%) » après « pourcent » puis écrire « pour cent » au lieu de « pourcent »
79 Remplacer « En tout état de cause, elle doit être supérieure à la première amende. » par « 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**[80] dans un délai fixé par **voie règlementaire**[81].

Si à l'expiration **du délai prescrit**[82], l'organisme mis en demeure ne se conforme pas, l'organe national en charge du contrôle et de la protection du cyberespace national **prononce**[83] à son encontre une amende **d'un**[84] million (1 000 000) à cent millions (100.000.000) de francs CFA sans préjudice de toute poursuite judiciaire.

[85]**En cas de récidive, l'organe national en charge du contrôle et de la protection du cyberespace national prononce**[86] **une nouvelle amende à son encontre**.

Dans tous les cas[87], l'amende prononcée pour la récidive **est**[88] 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**[89].

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.

80Remplacer « devra s'exécuter » par « s'exécute »
81 Remplacer « lui » par « voie règlementaire » et supprimer « Ce délai ne saurait excéder 12 mois »
82 Remplacer « de ce délai » par « du délai prescrit »
83 Remplacer « peut prononcer » par « prononce »
84 Remplacer « de un » par « d'un »
85 Détacher la dernière phrase de l'alinéa 2 pour en faire un alinéa 3 nouveau
86 Remplacer « peut prononcer » par « prononce »
87 Remplacer « En tout état de cause » par « Dans tous les cas »
88 Remplacer « doit être » par « est »
89 Remplacer « l'organe nationale en charge du contrôle et de la protection du cyberespace nationale » par « voie règlementaire »

La mise en demeure du titulaire est assortie d'un délai qui lui est notifiée par l'organe de contrôle après information des griefs qui lui sont reprochés.[90]

Article 21 **:**

Lorsque le mis en cause remédie au manquement dans le délai **prescrit**[91], l'organe national en charge du contrôle et de la protection du cyberespace national lui en donne **quitus**[92], au plus tard dans les quinze[93] jours suivant[94] 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**[95], l'organe national en charge du contrôle et de la protection**,**[96] en fonction de la gravité du manquement, **prononce**[97] à son encontre une amende allant de 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**[98] au contrevenant pour qu'il remédie à son manquement.

90 Remplacer le contenu de l'article 20 par « 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 notifiée par l'organe de contrôle après information des griefs qui lui sont reprochés. »
91 Remplacer « fixé » par « prescrit »
92 Remplacer « acte » par « quitus »
93 Supprimer « (15) » après « quinze »
94 Supprimer « s » à « suivants »
95 Remplacé « fixé » par « prescrit »»
96 Insérer une virgule « , » après « protection »
97 Remplacer « peut prononcer » par « prononce »
98 Remplacer « fixé » par « prescrit »

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**[99] l'une des sanctions suivantes :

- la suspension de l'accréditation, de l'agrément **technique**[100] ou de l'homologation pour une durée de deux ans au maximum ;
- la réduction de la durée de l'accréditation, de l'agrément **technique**[101] ou de l'homologation ;
- le non renouvellement de l'accréditation, de l'agrément **technique**[102] ou de l'homologation ;
- le retrait de l'accréditation, de l'agrément **technique**[103] 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**[104] 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**[105] 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**[106] qui n'excède pas **douze**[107] mois.

99 Remplacer « peut prononcer » par « prononce »
100 Insérer « technique » après « agrément »
101 Insérer « technique » après « agrément »
102 Insérer « technique » après « agrément »
103 Insérer « technique » après « agrément »
104 Remplacer « peut prononcer » par « prononce »
105 Remplacer « peut prononcer » par « prononce »
106 Remplacer « l'organe national en charge du contrôle et de la protection qui n'excède pas 12 mois » par « voie règlementaire »
107 Remplacer « 12 » par « douze »

Article 25 :

En cas de manquements d'un organisme relatifs à l'utilisation d'un matériel ou 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**[108].

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**[109] à son encontre une amende allant de deux millions (2 000 000) à cent millions (100 000 000) francs CFA.

En cas de récidive, l'organe en charge du contrôle et de la protection du cyberespace national **prononce**[110] une nouvelle amende à l'encontre de cet organisme.

Dans tous les cas,[111] l'amende prononcée pour la récidive **est**[112] 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[113] **technique**[114] 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**[115].

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**[116] à son encontre une amende de deux millions (2.000.000) à cent millions (100.000.000) de francs CFA.

108 Remplacer « lui » par « voie règlementaire »
109 Remplacer « peut prononcer » par « prononce »
110 Remplacer « peut prononcer » par « prononce »
111 Remplacer « En tout état de cause » par « Dans tous les cas »
112 Remplacer « doit être » par « est »
113 Supprimer le « s » à « agréments »
114 Insérer « technique » après « agrément »
115 Remplacer « lui » par « voie règlementaire » et supprimer « Ce délai ne saurait excéder 24 mois »
116 Remplacer « peut prononcer » par « prononce »

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 inopinées ou non **au niveau**[117] de tout exploitant de système d'information ou tout détenteur d'une accréditation, d'un agrément **technique**[118] 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**[119] à son encontre, une amende **d'un**[120] 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 mésures conservatoires sont fixées par voie reglementaire.[121]

Article 29 : **Supprimé**

CHAPITRE 4 : DES DISPOSITIONS DIVERSES, TRANSITOIRES ET FINALES

Article **29 :**[122]

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**.[123]

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.[124]

117 Remplacer « à l'égard » par « au niveau »
118 Insérer « technique » après « agrément »
119 Remplacer « peut prononcer » par « prononce »
120 Remplacer « de un » par « d'un »
121 Créer et insérer un alinéa 2 nouveau et lire «Les cas d'urgence et la durée des mésures conservatoires sont fixées par voie reglementaire »
122 Article 29 nouveau = Article 30 ancien
123 Remplacer « sont confiées à une structure du Ministère de la defense nationale » par « relèvent de la compétence du Ministère en charge de la defense nationale. »
124 Supprimer la deuxième phrase, puis créer un 2e alinéa nouveau et lire : « Les modalités d'exercice des missions de protection et de contrôle des organismes à infrastructures critiqques présentant un intérêt militaire sont déterminées par voie règlementaire. »

Article **30** :[125]

Les agréments **techniques**[126]**,** accréditations, homologations, autorisations et déclarations **en cours de validité**[127] doivent **se conformer à**[128] la présente loi au plus tard un[129] an après son entrée en vigueur.

Article **31** :[130]

Une procédure commune et un cadre de concertation[131] sont mis en place par **voie règlementaire**[132].

[133]

Article **32** :[134]

Les modalités de recouvrement des amendes et leur répartition sont fixées par voie règlementaire.[135]

Article **33** :[136]

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

Le Président

Le Secrétaire de s**éance**[137]

125 Article 30 nouveau = Article 31 ancien
126 Insérer « techniques » après « agréments »
127 Remplacer « existants » par « en cours de validité »
128 Remplacer « être mis en conformité avec » par « se conformer à »
129 Supprimer « (01) » après « un »
130Article 31 nouveau = Article 32 ancien
131 Supprimer « régulière » après « concertation »
132 Remplacer « arrêté du Ministre en charge des Communications électroniques sur proposition de l'organe de contrôle » par « voie règlementaire »
133 Supprimer le 2e alinéa
134Article 32 nouveau = Article 33 ancien
135 Remplacer le contenu de l'article par « Les modalités de recouvrement des amendes et leur répartition sont fixées par voie règlementaire »
136 Article 33 nouveau = Article 34 ancien
137 Remplacer « séanc » par « séance »