République du Sénégal
Un Peuple - Un But - Une Foi
ASSEMBLEE NATIONALE
XVe Législature

Projet de loi n°25/2026 sur la protection des Infrastructures d'Information critiques et la sécurité numérique

COMPOSITION DU DOSSIER

1°) Décret de présentation n°2026-1256 du 02 juillet 2026 de Monsieur le Président de la République ;

2°) Exposé des motifs ;

3°) Projet de loi.

REPUBLIQUE DU SENEGAL

Un Peuple-Un But-Une Foi

Décret n° 2026-1256
ordonnant la présentation à l'Assemblée nationale du projet de loi sur la protection des Infrastructures d'Information critiques et la sécurité numérique

LE PRESIDENT DE LA REPUBLIQUE,

VU la Constitution ;

VU le décret n° 2026-1129 du 25 mai 2026 portant nomination du Premier Ministre,

DECRETE :

Article premier. - Le projet de loi dont le texte est annexé au présent décret sera présenté à l'Assemblée nationale par le Ministre des Télécommunications et du Numérique, qui sera également chargé d'en exposer les motifs et d'en soutenir la discussion.

Article 2.- Le Ministre de la Communication et des Relations avec les Institutions et le Ministre des Télécommunications et du Numérique procèdent, chacun en ce qui le concerne, à l'exécution du présent décret qui sera publié au *Journal officiel*.

Fait à Dakar, le 02 juillet 2026

Par le Président de la République **Bassirou Diomaye Diakhar FAYE**

Le Premier Ministre

Ahmadou Alhaminou Mohamed LO

REPUBLIQUE DU SENEGAL

Un Peuple – Un But – Une Foi

Projet de loi sur la protection des Infrastructures d'Information critiques et la sécurité numérique

EXPOSE DES MOTIFS

Le développement des Technologies de l'Information et de la Communication (TIC) a ouvert à notre pays un champ prometteur d'opportunités, en termes d'efficience, de compétitivité et d'inclusivité.

Cependant, il faut admettre que l'ensemble des activités administratives, économiques et sociales, rendues performantes par l'usage des TIC, sont en même temps exposées aux menaces inhérentes au cyberespace que sont notamment le terrorisme, l'espionnage, le piratage et la négligence humaine.

Pour se protéger de ces menaces, soutenir l'économie du pays, qui est en grande partie une économie de services, et garantir le respect des droits fondamentaux des citoyens, le Sénégal s'est doté d'un cadre normatif.

A cet égard, depuis plusieurs années déjà, notre pays s'est doté d'un cadre juridique couvrant les domaines de la confiance numérique, du contrôle réglementaire de la cryptographie, de la protection des informations sensibles de l'Etat, des communications électroniques, des transactions électroniques et de la cybercriminalité.

Néanmoins ce cadre juridique présente encore des limites qui doivent être comblées pour élever le niveau de sécurité numérique existant au Sénégal à la hauteur des meilleurs standards internationaux.

En effet, malgré l'existence indéniable au Sénégal, de normes et bonnes pratiques en matière de sécurité des systèmes d'information, leur application aléatoire et inégale par les acteurs concernés, empêche notre écosystème numérique d'atteindre le niveau de sécurité souhaité, faute d'un support juridique contraignant et à portée générale. Cette limite est d'autant plus notable que certaines mesures de cybersécurité concernant les infrastructures d'information critiques (IIC) ne peuvent être implémentées que grâce à des lois habilitant l'Etat à apporter des atténuations à certains droits fondamentaux comme celui du respect de la propriété privée.

Il s'y ajoute, au plan stratégique, l'Agenda national de Transformation, Sénégal 2050, qui décline les orientations politiques du Gouvernement sur le long terme, a identifié dans son Objectif stratégique 4.5 intitulé « Renforcer la sécurité nationale », la cybersécurité comme l'un des piliers de la politique sécuritaire nationale et a érigé, à ce titre, comme actions prioritaires les mesures suivantes :

- le renforcement de la surveillance des infrastructures critiques/sensibles ;

- le renforcement des infrastructures de protection du cyber (PKI, CERT national, audit et la sécurité numérique des systèmes d'informations) ;
- la modernisation des équipements et des infrastructures face aux menaces protéiformes.

C'est pour relever ces défis que le présent projet de loi s'est attelé à mettre en place un cadre juridique global dédié à la sécurité des réseaux et systèmes d'information utilisés pour fournir des services au Sénégal. Il y procède, en établissant des principes de cybersécurité de base tout en laissant aux autorités réglementaires, le soin de donner à ces principes, le degré de précision et de spécificité nécessaire à leur mise en œuvre. Pour accomplir leurs missions, les autorités réglementaires seront assistées par l'Autorité nationale de Cybersécurité.

En terme de démarche, il faut souligner que le projet de loi instaure deux régimes de régulation qui se différencient par le degré de contrainte et l'intensité de la supervision qu'ils font peser sur les exploitants de systèmes d'information. Ainsi, les réseaux et systèmes d'information identifiés comme des Infrastructures d'Information critiques et donc, comme des actifs stratégiques pour la Nation, font l'objet d'une supervision rapprochée et de règles dont l'application est plus contraignante que celle concernant les réseaux et systèmes d'information ordinaires.

Enfin, pour tenir compte des impératifs d'autonomie stratégique et de souveraineté qui sont le fondement de l'agenda national de Transformation, Sénégal 2050, et favoriser l'éclosion de « champions nationaux », le présent projet de loi confie la fourniture de certains services essentiels de cybersécurité, à des prestataires agréés. L'activité de ces structures agrées permettra d'organiser et de développer une économie de la cybersécurité autour d'acteurs de confiance exerçant leurs missions dans des conditions définies par les lois et règlements.

Telle est l'économie du présent projet de loi qui comprend quatre (4) chapitres :

- le Chapitre premier porte sur les dispositions générales
- le chapitre II concerne les dispositions applicables à tous les réseaux et systèmes d'information ;
- le chapitre III a trait aux dispositions propres aux réseaux et systèmes d'information classés IIC ;
- le chapitre IV est relatif aux sanctions administratives et pénales ;
- le chapitre V porte sur la disposition finale.

REPUBLIQUE DU SENEGAL

Un Peuple – Un But – Une Foi

Loi n°
sur la protection des Infrastructures d'Information critiques et la sécurité numérique

Chapitre premier. – Dispositions générales

Article premier.- Objet

La présente loi vise à garantir la sécurité des réseaux et systèmes d'information qui se trouvent dans son champ d'application. Elle a une finalité de préservation de la sécurité globale et des intérêts souverains du Sénégal.

A ce titre elle :

- fixe les normes et standards de sécurité applicables à l'Etat, aux particuliers et aux organisations privées ;
- prévoit des règles applicables aux exploitants d'IIC qui sont implémentées sous le suivi rapproché des autorités administratives compétentes et de l'Autorité nationale de Cybersécurité ;
- détermine les règles relatives à la fourniture des services et produits de cybersécurité ;
- prévoit des sanctions administratives et pénales destinées à renforcer l'application des normes de cybersécurité.

Article 2.- Champs d'application

La présente loi s'applique au fonctionnement des réseaux et systèmes d'information qui sont des supports pour des activités exercées au Sénégal et qui sont entièrement ou partiellement établis en territoire sénégalais.

Elle peut s'appliquer, en sus, aux services numériques fournis au Sénégal, par le biais d'équipements se trouvant à l'étranger, dans des conditions fixées par décret ou selon des modalités fixées par des accords de coopération internationale.

Elle ne s'applique aux réseaux et systèmes d'information dont le fonctionnement est régi par un accord international que dans la mesure où ces accords le prévoient.

Elle ne porte pas préjudice à l'application des règles et mesures édictées spécifiquement pour la protection physique des infrastructures critiques et points sensibles.

Article 3.- Définitions

Au sens de la présente loi, on entend par :

- **CERT** : équipe chargée d'alerter sur les menaces, de prévenir les risques sur les systèmes d'information, de réagir en cas d'incident de sécurité informatique et d'aider à en atténuer les effets ;
- **cybercriminalité** : actes contrevenants aux lois nationales, utilisant les réseaux ou les systèmes d'information comme cible ou moyen de réalisation d'une infraction;
- **cybermenaces** : menaces et risques découlant du fonctionnement des systèmes d'information et réseaux de communication ou créées grâce à ce fonctionnement ;
- **cybersécurité** : l'ensemble des lois, politiques, outils, dispositifs, concepts et mécanismes de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques et technologies qui peuvent être utilisés pour protéger les personnes et les actifs informatiques connectés ou non à un réseau (avec un objectif de disponibilité, d'intégrité, de confidentialité et de non-répudiation) ;
- **fourniture d'un réseau de communications électroniques :** mise en place de l'exploitation, de la surveillance ou de la mise à disposition d'un tel réseau ;
- **fournisseur de services :** toute personne physique ou morale fournissant au public un service de communications électroniques ;
- **infrastructures d'information critiques** : systèmes et réseaux d'information interconnectés ou non, dont la perturbation ou la destruction aurait l'impact décrit à l'article 24 de la présente loi ;
- **objet connectable :** appareil doté d'une capacité de communication lui permettant d'interagir avec d'autres objets ou avec Internet et qui est capable de collecter, traiter et transmettre des données, recevoir des instructions et être contrôlé à distance via des applications ;
- **opérateur de réseaux de communication électronique** : toute personne morale exploitant un réseau de communications électroniques ouvert au public ;
- **politique de Sécurité des Systèmes d'information de l'Etat (PSSI-ES)** : document énonçant la politique de sécurité des systèmes d'information de l'Etat du Sénégal ;
- **politique de Sécurité des Systèmes d'information des Infrastructures d'Information critiques (PSSI-IIC)** : document énonçant la politique de sécurité des systèmes d'information de l'Etat du Sénégal pour les Infrastructures d'Information critiques ;
- **produit de cybersécurité :** dispositif matériel ou logiciel spécifiquement conçu pour assurer une fonction de sécurité de l'information, telle que la prévention, la détection, la protection, la surveillance ou la réponse aux menaces numériques ;
- **service de cybersécurité :** prestation, continue ou ponctuelle, visant à garantir la mise en œuvre, l'exploitation et l'amélioration des mesures de sécurité d'un système d'information ;
- **réseaux de communication électronique** : toute installation ou ensemble d'installations assurant soit la transmission et l'acheminement des signaux de

communications électroniques, ainsi que l'échange des informations de commande et de gestion qui y est associé, entre les points de terminaison de ce réseau ;

- **service de communications électroniques :** service fourni moyennant rémunération qui consiste entièrement ou principalement en la transmission ou l'acheminement de signaux ou une combinaison de ces fonctions sur des réseaux de communications électroniques, y compris les services de transmission sur les réseaux utilisés pour la radiodiffusion, mais qui exclut les services consistant à fournir des contenus à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus, notamment les services de communication au public en ligne ;
- **système d'information** : tout dispositif, isolé ou non, ou ensemble de dispositifs interconnectés assurant en tout ou partie un traitement automatisé de données en exécution d'un programme.

Chapitre II. - Dispositions applicables à tous les réseaux et systèmes d'information

Section première. - Obligations de l'Etat et des particuliers

Article 4.- Obligations de l'Etat

L'Etat et ses démembrements sont les principaux responsables de la protection des réseaux et des systèmes d'information. A cette fin, il leur appartient :

- de mettre en place, en l'actualisant régulièrement, un cadre juridique et institutionnel adapté à la cybersécurité ;
- d'assurer la protection des infrastructures d'information critiques (IIC) et des systèmes d'information de l'Etat du Sénégal, en veillant notamment à la mise en œuvre des politiques de sécurité des systémes d'information, édictées à cette fin;
- de promouvoir une culture généralisée de la cybersécurité au Sénégal ;
- de renforcer les capacités et les connaissances techniques en cybersécurité dans tous les secteurs d'activité au Sénégal ;
- de participer entièrement et activement aux efforts régionaux et internationaux de cybersécurité.
- de s'assurer que tous les acteurs concernés, développent de manière dynamique, les compétences et la capacité à protéger leurs systèmes d'information et leurs réseaux.

En vue de garantir la confidentialité, l'authenticité, l'intégrité et la non-répudiation des données circulant dans les réseaux et systèmes d'information des Administrations et du secteur privé, l'Etat du Sénégal mettra en place une Infrastructure nationale de gestion des clés publiques.

Article 5.- Obligations des particuliers

Les particuliers utilisant les technologies de l'information et de la communication, dans leur cadre professionnel ou privé, appliquent les normes et politiques de sécurité édictées

par l'Etat ou l'organisation à laquelle ils appartiennent. Ils appliquent, à cet égard, le principe de précaution, qui les conduit à éviter les comportements facilitant la réalisation des menaces cybernétiques.

Ils appliquent, dans la mesure de leurs possibilités et capacités, les guides, les recommandations ainsi que les autres documents de prévention et de sensibilisation élaborés à leur attention pour les accompagner dans leurs usages des technologies de l'information et de la communication.

Section II.- Obligations des exploitants de réseaux et systèmes d'information

Article 6.- Autorités chargées de l'élaboration de normes de cybersécurité

Les exploitants des réseaux et systèmes d'information se conforment aux règles de sécurité édictées par les autorités administratives compétentes dans le domaine de la cybersécurité. Ces règles peuvent être prises sur proposition de l'Autorité nationale de Cybersécurité.

Les exploitants des réseaux et systèmes d'information veillent également à appliquer les normes élaborées par l'Autorité nationale de Cybersécurité sous forme de guides, directives, référentiels ou sous d'autres dénominations et qui ont valeur de recommandation.

L'Autorité nationale de Cybersécurité du Sénégal est une entité dotée de la personnalité juridique et possédant un statut spécial, dérogatoire à la loi d'orientation sur le secteur parapublic. Son organisation et son fonctionnement sont fixés par décret.

Les missions de l'Autorité nationale de Cybersécurité sont exercées par toute structure désignée par décret.

Article 7.- Mesures techniques et organisationnelles de cybersécurité

Sans préjudice des alinéas 1 et 2 de l'article 6, les exploitants de réseaux et de systèmes d'information, sont tenus d'identifier les risques qui menacent la sécurité de leurs systèmes d'information et de prendre des mesures techniques et organisationnelles nécessaires pour gérer ces risques ainsi que pour en réduire au minimum l'impact lorsque ces risques se réalisent.

Ils doivent notamment :

- formuler des politiques de gestion de la sécurité interne et procéder systématiquement à la désignation d'un responsable de la sécurité des systèmes d'information chargé de veiller à l'application des règles de cybersécurité ;
- élaborer des Plans de continuité d'activités (PCA) et des Plans de reprise d'activité (PRA) pour la gestion des crises ;
- procéder à la classification des actifs ;
- faire des audits réguliers de leurs systèmes d'information ;

- mettre en place, lorsque cela s'avère nécessaire, de moyens de supervision et détection des événements susceptibles d'affecter la sécurité des systèmes d'information ;
- enregistrer le fonctionnement du réseau et des événements liés à la sécurité du réseau, et conserver les journaux pendant au moins six mois.
- assurer la sauvegarde et le chiffrement des données sensibles ;
- effectuer régulièrement des tests de résilience et des scans de vulnérabilité.

Article 8.- Responsabilité civile découlant d'un incident informatique

En cas de dommage causé à un tiers par le mauvais fonctionnement d'un système d'information, alors qu'il est avéré que l'exploitant de ce système d'information a omis, sans motif justifié, de prendre les mesures de sécurité visées dans la présente section, ce dernier est présumé civilement responsable du préjudice en découlant.

Article 9.- Notification d'incidents

Les exploitants de réseaux et de systèmes d'information, qu'ils soient organismes public ou privé, notifient immédiatement les intrusions, attaques et autres perturbations ayant un impact significatif sur la continuité des services qu'ils fournissent, afin que les mesures nécessaires pour y faire face soient prises.

La notification est faite auprès de prestataires de services de cybersécurité, agréés dans les conditions fixées par l'article 15 de la présente loi et des textes pris pour son application.

Lorsqu'il estime qu'il est dans l'intérêt public de notifier la survenance de l'incident à l'Autorité nationale de Cybersécurité, l'exploitant peut, en même temps qu'il saisit un prestataire agréé de service de cybersécurité, déclarer ledit incident à l'Autorité nationale de Cybersécurité.

Cette dernière apprécie alors, en fonction de l'impact potentiel de l'incident, de l'utilité ou non d'intervenir en substitution du prestataire agréé. Lorsque l'Autorité nationale de Cybersécurité, décide de se substituer à un prestataire agréé, et l'en informe, ce dernier se dessaisit sans délai de sa mission, en lui communiquant toutes les informations à sa disposition et en lui faisant le rapport des diligences effectuées.

Lorsqu'à la suite d'une notification volontaire d'incident, l'Autorité nationale de Cybersécurité décide de prendre en charge la réponse à l'incident, il agit conformément aux dispositions des articles 31 et suivants de la présente loi.

Article 10.- Audit

Les réseaux et systèmes d'information relevant des services étatiques sont soumis à un régime d'audit obligatoire et périodique de sécurité informatique.

En outre, une liste des réseaux et systèmes d'information des organismes privés établis sur le territoire national qui peuvent, pour des raisons de sécurité publique, périodiquement faire l'objet d'audits de sécurité informatique, sera établi par voie

réglementaire sur proposition de l'Autorité nationale de Cybersécurité. Ces audits peuvent être faits par les services internes compétents.

Les critères relatifs à la nature, la périodicité, les procédures et le suivi des recommandations de l'audit, seront également fixés par voie réglementaire.

Dans le cas où les organismes publics ou privés visés dans le présent article ne procèdent pas à l'audit obligatoire périodique, l'Autorité nationale de Cybersécurité avertit l'organisme concerné qui devra effectuer l'audit dans un délai ne dépassant pas trois (03) mois à partir de la date de l'avertissement.

A l'expiration de ce délai sans résultat, l'Autorité nationale de Cybersécurité est tenue de désigner, aux frais de l'organisme contrevenant, un prestataire qui sera chargé de l'audit sus-indiquée. Cet audit est effectué par des prestataires agréés dans les conditions fixées par l'article 15 de la présente loi et de ses textes d'application.

Article 11.- Classification des actifs

Les exploitants de réseaux et systèmes d'information veillent à la classification des actifs informationnels et systèmes d'information selon leur niveau de sensibilité en termes de confidentialité, d'intégrité et de disponibilité. Les mesures de protection des actifs informationnels et systèmes d'information doivent être proportionnées au niveau de classification attribué.

Chaque exploitant de réseaux et systèmes d'information arrête des procédures d'habilitation des personnes pouvant accéder aux informations classifiées et aux conditions d'échange, de conservation ou de transport de ces informations.

Le référentiel de classification des actifs informationnels et des systèmes d'information est établi par l'Autorité nationale de Cybersécurité.

Article 12.- Stockage des données

Les données produites, collectées ou détenues à un quelconque titre, par les services de l'État ou par des partenaires privés de l'État exécutant une mission de service public, sont hébergées et traitées sur le territoire national.

Toutefois, lorsque des raisons impérieuses rendent nécessaires le stockage temporaire de ces données hors du territoire national, un acte réglementaire pourra autoriser la prise de mesures dérogatoires à l'alinéa 1er du présent article en précisant la durée pour laquelle cette dérogation est permise.

Le stockage et le traitement des données autres que celles du secteur public, liées à l'activité des réseaux et systèmes d'information régis par la présente loi, se fait dans des conditions de nature à en assurer la disponibilité, l'inviolabilité et l'intégrité, en application des lois et règlements édictés, en la matière, par l'État sénégalais.

Dans tous les cas, l'Autorité nationale de Cybersécurité établit des normes de sécurité relatives aux conditions de stockage des données sur le territoire et hors du territoire national, en rapport avec les engagements internationaux du Sénégal.

L'hébergement des données qui ont un caractère personnel respecte, en outre, les règles spécifiques à cette matière.

Article 13.- Divulgation de données consécutive à une cyberattaque

Lorsqu'une violation de données personnelles est consécutive à un incident informatique, et en particulier à une cyberattaque, le responsable du traitement, en plus de la notification faite auprès de la Commission des Données à caractère Personnel (CDP), est tenu d'en informer les personnes dont les données ont été compromises dans les mêmes délais que ceux prévus par la réglementation des données à caractère personnel.

Cependant, lorsqu'en raison du nombre important de personnes concernées, il y a lieu de craindre qu'une information portée à grande échelle ne compromette les chances de traiter efficacement l'incident ou l'attaque informatique, le délai de notification de soixante-douze (72) heures peut être allongé pour une durée appropriée, par l'Autorité nationale de Cybersécurité qui informe alors par écrit le responsable du traitement concerné du nouveau délai qu'elle a fixé.

Article 14.- Assurance pour risques de cybersécurité

Tout exploitant de réseau et système d'information peut souscrire, conformément au Traité instituant la Conférence Interafricaine des Marchés d'Assurances (CIMA), un contrat d'assurance destiné à couvrir les préjudices consécutifs à un incident informatique ou à une cyberattaque dont son système d'information pourrait être l'objet.

Le préjudice garanti couvre notamment :

- les dommages causés à l'exploitant lui-même ou aux tiers du fait de l'indisponibilité du système d'information ;
- les frais consécutifs à gestion de la cybercrise née de l'incident ou de l'attaque informatique ;
- les frais liés au règlement des procédures contentieuses auxquelles l'exploitant pourrait être partie prenante ;
- les sanctions financières éventuellement prononcées contre l'exploitant du système d'information pour diverses situations de non-conformité.

Les parties au contrat d'assurance ne sont pas autorisées à inclure dans le préjudice garanti, les paiements de rançons consécutives à des cyberattaques.

Dans tous les cas, l'indemnisation de l'assuré est subordonnée au dépôt d'une plainte par la victime auprès des autorités judiciaires sénégalaises compétentes.

Article 15.- Prestataires de services de cybersécurité

Afin d'assister les particuliers, les entreprises et les autres organismes de droit privé, ainsi que les exploitants d'Infrastructures d'Information critiques, contre les menaces

cybernétiques de tous ordres, l'Autorité nationale de Cybersécurité agréera des prestataires de cybersécurité qui interviendront notamment dans les domaines suivants :

- audit de sécurité ;
- prévention, détection et réactions aux incidents et risques de cybersécurité ;
- hébergement sécurisé des données ;
- certification et homologation de produits et services de cybersécurité ;
- conseils et maintenance sécurisée des systèmes d'information ;

Les conditions dans lesquelles les prestataires de service de cybersécurité seront autorisés à exercer leurs activités au Sénégal ou à y fournir d'une quelconque manière leurs services, ainsi que les contrôles et inspections dont ils seront l'objet de la part de l'Autorité nationale de Cybersécurité, seront fixées par voie réglementaire.

La délivrance des autorisations d'exercice, sera assujettie au respect de critères qui seront fixés en fonction des impératifs de sécurité nationale et qui porteront notamment sur :

- la nationalité des personnes physiques ou morale détenant l'actionnariat ou assurant la direction de l'activité au sein de la structure concernée, à travers les droits de vote, la participation au capital ou tout autre moyen ;
- la nationalité des professionnels et employés intervenant dans les missions confiées aux prestataires ;
- la localisation d'infrastructures et d'équipements utilisés pour remplir les missions confiées au prestataire.
- les moyens techniques et technologiques utilisés pour fournir les services proposés.

Les contrats relatifs à la commande publique portant sur des services réglementés de cybersécurité ne pourront être assurés que par des prestataires et des professionnels détenteurs d'une autorisation d'exercice dûment accordée par l'Autorité nationale de cybersécurité.

Section III.- Obligations des fabricants, fournisseurs et distributeurs

Article 16.- Sécurité des objets connectables

Les objets connectables, mis en circulation, à quelque titre que ce soit, sur le marché sénégalais, doivent être conformes aux meilleurs standards de sécurité et aux normes nationales de sécurité, s'il en existe.

Ces standards incluent notamment :

- l'existence d'une documentation technique intelligible et complète faisant apparaitre toute information pertinente, y compris les vulnérabilités connues des objets connectables mis en circulation ;
- la non-installation de programmes malveillants sur l'objet connectable ;
- l'information portée expressément à l'utilisateur sur toute information que l'objet connectable pourrait collecter sur lui ;

- la définition éventuelle d'une période d'assistance qui corresponde à la durée de vie de l'objet connectable ;
- la mise à jour régulière des objets connectables suivant les référentiels du constructeur.

Lorsque les fabricants, distributeurs ou fournisseurs d'un produit connectable commercialisé sur le marché sénégalais, acquièrent la connaissance de vulnérabilités ou de défauts de conformité avec les exigences nationales de sécurité, après sa mise en circulation sur le marché sénégalais, celles-ci doivent être signalées, par toutes les voies appropriées, à leurs utilisateurs et à l'Autorité nationale de Cybersécurité. Le signalement doit s'accompagner d'une information pertinente sur les politiques et procédures pour traiter et corriger les vulnérabilités et défauts de conformité.

Le défaut de communication de ces informations engage la responsabilité civile et pénale des fabricants, fournisseurs ou distributeurs, s'il apparait au vu des circonstances, que ces derniers ne pouvaient raisonnablement ignorer l'existence des vulnérabilités et défauts de conformité qui seraient décelés sur ces produits.

Un importateur ou un distributeur établi au Sénégal est considéré comme un fabricant aux fins de la présente loi et est soumis aux obligations incombant au fabricant lorsque cet importateur ou ce distributeur met un produit connectable sous son propre nom ou sa propre marque, ou lorsqu'il apporte une modification substantielle à un produit connectable mis sur le marché.

L'Autorité nationale de Cybersécurité met en place une base de données nationales des vulnérabilités dont le contenu est communicable à ceux qui ont besoin d'en connaitre.

Article 17.- Exception à la sécurité des objets connectables

Les équipements, logiciels et produits informatiques utilisés pour les besoins de tests, d'expérimentations, et d'études ne sont pas concernés par les dispositions de l'article 16 de la présente loi.

Article 18.- Certification de cybersécurité

L'Autorité nationale de Cybersécurité met en place un système de certification des produits de cybersécurité qui lui permet d'assujettir la circulation sur le marché sénégalais de certains produits de cybersécurité, à l'évaluation de leur conformité technique et réglementaire.

Des normes internationales jugées équivalentes peuvent être substituées aux certificats de cybersécurité visés à l'alinéa précédent, sur décision réglementaire prise par les autorités sénégalaises.

Lorsqu'un produit est jugé non conforme à l'issue de son évaluation, les personnes physiques ou morales responsables de sa mise en circulation sur le marché sénégalais sont invitées, sans tarder, par l'Autorité nationale de Cybersécurité, à prendre toutes les

mesures correctives appropriées pour le mettre en conformité avec les exigences nécessaires, le retirer du marché ou le rappeler dans un délai raisonnable. Lesdites mesures doivent être proportionnées à la nature des risques encourus.

La certification des produits de cybersécurité est faite par l'Autorité nationale de Cybersécurité, au besoin, avec le concours d'organismes privés agréés par cette dernière.

Chapitre III.- Dispositions propres aux réseaux et systèmes d'information classés Infrastructure d'Information critiques

Section première. - Considérations générales sur les IIC

Article 19.- Finalité des mesures applicables aux IIC

Les dispositions du présent chapitre s'appliquent spécifiquement aux Infrastructures d'Information critiques, en abrégé « IIC ». Elles visent à préserver la continuité des services et systèmes d'information vitaux pour la Nation sénégalaise en veillant à ce qu'ils ne soient pas compromis et, dans la mesure où ils le sont, à ce que la compromission soit détectée et son impact minimisé ou effacé.

Ces mesures sont prises et appliquées avec l'aide de l'Autorité nationale de Cybersécurité qui a, conformément à l'article 26 de la présente loi, une mission de recommandation, de suivi, de supervision et d'élaboration de normes de cybersécurité concernant les entités classées IIC.

Article 20.- IIC spécifiques

Les réseaux et systèmes d'information relevant de la Défense nationale, de la sécurité publique, des cours et tribunaux, de l'Administration pénitentiaire ainsi que de l'Administration des Douanes, sont classés d'office IIC.

Les obligations de la présente loi leur sont applicables. Cependant les modalités de suivi, de supervision et de contrôle du respect desdites obligations seront fixées par décret.

Section II.- Identification et désignation des IIC

Article 21.- Autorités chargées de la désignation des IIC

L'Ensemble des IIC, partiellement ou entièrement établis sur le territoire national, sont classées selon les secteurs d'activités auxquels ils appartiennent, la liste desdits secteurs d'activités étant fixée par voie réglementaire. Chaque secteur d'activité est placé sous la responsabilité d'une autorité sectorielle.

Chaque autorité sectorielle procède à l'identification et au recensement des IIC de son secteur dont il transmet ensuite la liste à l'Autorité nationale de Cybersécurité par un moyen de nature à en assurer la confidentialité la plus totale.

L'autorité administrative dont relève l'Autorité nationale de Cybersécurité, établit alors, par arrêté, le répertoire national des IIC, sur proposition de l'Autorité nationale de Cybersécurité.

En cas d'urgence ou lorsque des raisons techniques, économiques ou d'une autre nature le rendent nécessaire, l'Autorité nationale de Cybersécurité peut également, à la demande de l'autorité administrative dont elle relève, faire à cette dernière, une proposition de répertoire national des IIC.

Le répertoire national des IIC est actualisé par l'autorité administrative dont relève l'Autorité nationale de Cybersécurité, chaque fois que de besoin, par insertion ou retrait, et au moins, tous les trois (3) ans.

La notification aux exploitants d'IIC de leur classement dans le répertoire national des IIC déclenche, pour ces derniers, l'obligation d'appliquer les mesures prévues dans la présente section.

Seuls les délais prévus aux articles 27 alinéa 1, 30 alinéa 1 et 39 alinéa 1 de la présente loi, font exception à la règle édictée à l'alinéa précédent.

Le répertoire national des IIC est tenu secret et n'est communiqué qu'aux personnes habilitées à cet effet et ayant besoin d'en connaitre.

Article 22.- Avis requis pour l'identification des IIC

Afin d'identifier les IIC relevant de sa compétence, chaque Autorité sectorielle prend, au préalable, l'avis de l'Autorité nationale de Cybersécurité, celui des potentiels exploitants d'IIC de son secteur, ainsi que de toute entité publique ou privée dont l'appréciation est de nature à l'éclairer. Il peut recourir à l'office d'experts qui remplissent leurs missions dans les conditions de confidentialité.

Article 23.- Critères d'identification des IIC

Pour l'identification des IIC les critères cumulatifs suivants sont appliqués :

- l'IIC est constitutive de réseaux ou systèmes d'information utilisés pour la fourniture de services essentiels au fonctionnement de la société et de l'économie, services dont la liste sera fixée par voie réglementaire ;
- un incident affectant ces réseaux et systèmes d'information doit être susceptible d'entraîner une perturbation grave des services essentiels qu'il fournit, la gravité étant déterminée en tenant compte des critères et des niveaux d'incidence ou seuils visés à l'article 24 de la présente loi.

Article 24.- Critères de détermination de la gravité d'un incident de cybersécurité

Pour déterminer la gravité d'une perturbation des réseaux et systèmes d'information, tel qu'évoqué à l'article 23 de la présente loi, il est tenu compte, de manière non cumulative, des données suivantes :

a) le nombre d'utilisateurs tributaires du service fourni par l'entité concernée ;
b) la dépendance d'autres secteurs essentiels à l'égard du service fourni par cette entité ;
c) les conséquences que des incidents pourraient avoir, en termes de degré et de durée, sur les fonctions économiques ou sociétales ou sur la sécurité publique ;
d) l'importance économique de cette entité ;
e) l'ampleur de la zone géographique susceptible d'être touchée par un incident ;
f) l'importance que revêt l'entité pour garantir un niveau de service suffisant, compte tenu de la disponibilité de solutions de rechange pour la fourniture de ce service.

Eu égard aux caractéristiques particulières de son secteur, toute autorité responsable peut établir, en concertation avec l'Autorité nationale de cybersécurité, des critères additionnels lui permettant d'identifier les IIC de son secteur.

Section III. - Obligations de cybersécurité

Article 25.- Obligations générales pesant sur les exploitants d'IIC

Les exploitants d'IIC prennent les mesures nécessaires pour identifier les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent. Ils ont recours, pour ce faire, à des procédés techniques et organisationnels, à la fois nécessaires et proportionnés.

Ils mettent notamment en œuvre les mesures prévues à l'article 7 de la présente loi.

Les règles et recommandations de sécurité fixées par les autorités administratives compétentes sont appliquées aux frais des exploitants d'IIC.

Article 26.- Missions normatives de l'Autorité nationale de Cybersécurité

L'Autorité nationale de Cybersécurité peut :

- élaborer des normes qui ont valeur de recommandation à l'endroit des exploitants d'IIC ;
- proposer aux autorités administratives compétentes des normes de sécurité dont l'application pourrait être rendue obligatoire par ces dernières, dans les conditions fixées par décret et dont le non-respect est sanctionné par les amendes administratives et financières prévues au chapitre IV de la présente loi.

Article 27.- Programmes de cybersécurité des exploitants d'IIC

Chaque exploitant d'IIC, dans les six (6) mois qui suivent la notification de son classement dans le répertoire national des IIC, élabore un programme de cybersécurité de ses systèmes et réseaux d'information reprenant au moins les objectifs et les mesures de sécurité concrètes, de la Politique de Sécurité des Systèmes d'Information des Infrastructures d'Information critiques (PSSI-IIC) élaboré par l'Autorité nationale de cybersécurité à l'attention des exploitants d'IIC.

Le programme de cybersécurité, visé ci-dessus, devra comprendre des mesures de sécurité raisonnables permettant :

- d'identifier et de gérer les risques de cybersécurité, y compris ceux liés à la chaîne d'approvisionnement de l'exploitant d'IIC et à l'utilisation de produits et services tiers ;
- de protéger les systèmes critiques contre toute compromission ;
- de détecter les incidents de sécurité affectant les systèmes ;
- de minimiser l'impact de tout incident de sécurité.

Les programmes de cybersécurité sont transmis à l'Autorité nationale de Cybersécurité et mis à jour par l'exploitant selon des modalités fixées par voie réglementaire.

Article 28.- Sécurité des produits, services et solutions utilisés dans le fonctionnement des IIC

Les services, produits ou solutions utilisés par les exploitants d'IIC doivent respecter des standards élevés en matière de cybersécurité.

Lorsqu'ils contractualisent en vue d'acquérir des produits, services et solutions, les exploitants d'IIC signent des accords avec leurs fournisseurs dans lesquels les obligations de sécurité et de confidentialité qui pèsent sur eux sont précisées.

L'Autorité nationale de Cybersécurité peut décider de soumettre à une certification préalable à leur utilisation, certains des dispositifs matériels ou logiciels ou services informatiques utilisés dans le fonctionnement des IIC.

La certification porte sur l'aptitude de ces services, dispositifs matériels ou logiciels à assurer la disponibilité, l'intégrité ou la confidentialité de l'information traitée par les IIC face aux menaces en la matière.

La certification est faite par l'Autorité nationale de Cybersécurité avec le concours de structures agrées à cette fin.

Article 29.- Assurance obligatoire de cybersécurité

En fonction de la nature du risque qui pèse sur certaines de leurs activités, et par dérogation au principe de l'assurance facultative prévue à l'article 14 de la présente loi, les exploitants d'IIC peuvent être assujettis, par voie réglementaire, à souscrire à des contrats d'assurance en vue de couvrir les dommages provenant d'incidents de cybersécurité.

Les réserves établies par les alinéas 3 et 4 de l'article 14 de la présente loi, s'appliquent lorsque l'assurance revêt un caractère obligatoire.

Article 30.- Externalisation de la gestion des systèmes d'information des IIC

Dans les cinq (5) mois qui suivent la notification de son classement dans le répertoire national des IIC, tout exploitant d'IIC doit communiquer à l'Autorité nationale de Cybersécurité, selon un canevas qui sera fixée par cette dernière, ceux de ses systèmes d'information dont la gestion a été entièrement ou totalement externalisée.

L'Autorité nationale de Cybersécurité informe alors l'exploitant d'IIC, des règles et référentiels techniques qu'elle a élaboré en matière d'externalisation des systèmes d'information et lui demande de lui fournir toutes les indications nécessaires sur le respect desdites mesures.

En cas de non-respect des exigences en matière d'externalisation de systèmes d'information, l'Autorité nationale de Cybersécurité impartit un délai raisonnable à l'exploitant pour y pourvoir.

Les exigences stipulées par l'Autorité nationale de Cybersécurité en matière d'externalisation des systèmes d'information doivent comprendre des engagements de protection de l'information, d'auditabilité et de réversibilité, ainsi que d'autres obligations de sécurité et de niveaux de service.

Section IV.- Prévention, signalement et traitement des incidents de cybersécurité

Article 31.- Missions du CERT national

En sa qualité de service de l'Autorité nationale de Cybersécurité en charge du suivi et de la gestion des incidents de cybersécurité, le CERT national a pour missions :

- le suivi et l'analyse des incidents au niveau national et international, y compris le traitement de données liés à ces activités ;
- la surveillance, au besoin, en temps réel ou quasi réel des réseaux et systèmes d'information des exploitants d'IIC ;
- l'activation du mécanisme d'alerte précoce, la diffusion de messages d'alerte, les annonces ainsi que la diffusion d'informations sur les cybermenaces, les vulnérabilités et incidents auprès des entités concernées ;
- l'intervention en cas d'incident ;
- la détection, l'observation et l'analyse des problèmes de sécurité informatique ;
- la collecte et l'analyse des données de police scientifique, et l'analyse dynamique des risques et incidents et une appréciation de la situation en matière de cybersécurité ;
- la promotion de l'adoption et de l'utilisation de pratiques communes ou normalisées pour les procédures de gestion des risques et incidents, ainsi que des systèmes de classification des incidents, risques et informations ;
- l'établissement de relations de coopération avec le secteur privé, d'autres services administratifs ou autorités publiques ;

- la participation aux réseaux de CERT nationaux ou organismes assimilés ;
- la mise en œuvre de services de veille, de détection, d'alerte, d'analyse et de gestion en continu des risques et des menaces, ainsi que de réactions aux attaques des systèmes d'information du public et du privé, en relation avec tout organisme national et international intervenant dans ce domaine ;
- la coordination nationale de la réaction à ces événements, en liaison avec les structures spécialisées ;
- le déploiement de services de SOC et de CERT sectoriels pour certaines entités de l'Administration publique.

Le CERT national peut, dans le cadre de ses missions, procéder à des scans proactifs sur les réseaux et systèmes d'information accessibles au public, des entités du secteur critique et de toute autre entité, en cas de besoin.

Ces scans sont effectués dans le but de détecter les réseaux et systèmes d'information vulnérables ou configurés de façon peu sûre et d'informer les entités concernées. Il ne doit pas avoir d'effet négatif sur le fonctionnement des services desdites entités.

Lorsque cela s'avère nécessaire, le CERT national peut communiquer aux responsables des réseaux et systèmes d'information les adresses IP utilisées pour effectuer le scan, afin que celles-ci ne fassent pas l'objet d'un blocage. Les responsables de réseaux et systèmes d'information prennent alors les dispositions nécessaires pour éviter le bocage des adresses IP concernées durant la période au cours de laquelle doit se dérouler le scan.

Article 32.- Principes d'intervention du CERT national

Les mesures prises par le CERT national dans le cadre de ses missions doivent être proportionnelles à ses objectifs, et respecter les principes d'objectivité et de transparence.

Par ailleurs, il veille toujours en priorité, à ce que son action ne perturbe pas le fonctionnement des systèmes informatiques sur lesquels il intervient et en prenant toutes précautions raisonnables afin qu'aucun dommage matériel ne leur soit causé.

Le CERT national veille, par l'adoption de procédures internes, au respect des exigences du présent article.

Article 33.- Habilitation et assermentation des agents du CERT national

Les agents du CERT national exerçant les prérogatives qui leur sont dévolues par la présente loi, doivent être habilités dans des conditions fixées par voie réglementaire. Ils prêtent ensuite serment devant le tribunal de grande instance de Dakar. La formule de ce serment est fixée par décret.

Les agents assermentés du CERT national peuvent accéder aux locaux, terrains, sites ou moyens de transport à usage professionnel, demander la communication de tout document professionnel et en prendre copie, recueillir, sur convocation ou sur place, les renseignements et justifications qu'ils jugent nécessaires.

Les agents assermentés du CERT national bénéficient de la protection de la loi et du concours des forces de l'ordre dans l'exercice de leur mission.

Article 34.- Objectifs du CERT national

Lorsque l'Autorité nationale de Cybersécurité reçoit des informations concernant une menace ou un incident de cybersécurité présentant les caractéristiques prévues par l'article 35 de la présente loi, elle peut, par le biais du CERT national, prendre les mesures nécessaires afin :

- d'évaluer l'impact réel ou potentiel de la menace ou de l'incident de cybersécurité ;
- d'éliminer la menace pour la cybersécurité ou prévenir de toute autre manière tout préjudice ou tout autre dommage résultant de l'incident de cybersécurité ;
- de prévenir tout autre incident de cybersécurité.

Article 35.- Signalement des incidents

Les personnes en charge de l'exploitation d'une IIC, déclarent, sans délai, tout incident dont l'impact est de nature à :

- causer une perturbation opérationnelle grave des services ou des pertes financières pour l'entité concernée ;
- affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.

La déclaration est faite simultanément à l'Autorité nationale de Cybersécurité et à l'Autorité sectorielle.

La déclaration d'incident contient toute information disponible, permettant d'évaluer l'ampleur éventuel de l'incident au plan national et international.

Elle contient notamment :

- une description détaillée de l'incident, y compris de sa gravité et de son impact;
- le type de menace ou la cause profonde qui a probablement déclenché l'incident;
- les mesures d'atténuation appliquées et en cours ;
- le cas échéant, l'impact transfrontière de l'incident.

A défaut de pouvoir transmettre l'ensemble de ces informations à l'Autorité nationale de Cybersécurité, dans les vingt-quatre (24) heures qui suivent le constat de l'existence de l'incident, le responsable désigné de l'IIC porte à sa connaissance celles qui sont à sa disposition, dans ce délai.

Il transmet ensuite selon une périodicité établie par voie réglementaire, un rapport contenant autant que possible l'ensemble des éléments visés à l'alinéa 4 du présent article.

Lorsque l'incident a potentiellement un impact international, les autorités compétentes des États concernés peuvent être informées conformément aux accords les liant à celui du Sénégal.

Article 36.- Mesures correctives pouvant être prises par le CERT national

Dans le cadre de ses missions, le CERT national peut ordonner, par notification écrite, à toute personne de prendre les mesures correctives ou de cesser d'exercer les activités qui peuvent lui être spécifiées, en relation avec un ordinateur ou un système informatique dont le CERT national a de bonnes raisons de soupçonner qu'il est ou a été affecté par l'incident de cybersécurité, afin de réduire au minimum les vulnérabilités de l'ordinateur ou du système informatique sur le plan de la cybersécurité.

Elle peut également demander à toute personne de lui fournir des informations relatives à la conception, à la configuration ou au fonctionnement d'un ordinateur, d'un programme informatique ou d'un système informatique, dès lors que ces informations sont en lien avec une menace ou un incident informatique sur lequel il intervient.

Lorsque les réseaux et les systèmes d'information liés à l'activité d'une IIC sont situés en dehors du territoire sénégalais, il peut être sollicité, par les voies appropriées, la coopération et l'assistance des autorités compétentes des États concernés. Cette assistance et cette coopération peuvent aussi porter sur des échanges d'informations et sur des demandes de prise de mesures de contrôle.

Article 37.- Mise en place de CERT sectoriels

Dans le cadre de la gestion des incidents de cybersécurité, chacune des autorités sectorielles visées à l'article 21 de la présente loi, peut faire superviser les IIC dont il a la charge par un CERT sectoriel qui a pour missions :

- le suivi et l'analyse des incidents sectoriels ;
- l'intervention en cas d'incident sectoriel ;
- le report des incidents au CERT national et, de manière générale, les interactions avec le CERT national ;
- l'analyse dynamique des risques et incidents sectoriels et conscience situationnelle ;
- l'activation du mécanisme d'alerte précoce, la diffusion de messages d'alerte, les annonces et la diffusion d'informations sur les risques et les incidents auprès des parties intéressées du secteur ;
- l'établissement de relations de coopération avec les acteurs de son secteur ;
- l'établissement de relations de coopération avec les opérateurs de son secteur ;
- la participation aux réunions, relatives à son secteur, du réseau des CSIRT.

Article 38.- Gestion et exploitation des CERT sectoriels

La gestion et l'exploitation d'un CERT sectoriel peuvent être assurées par les services compétents de l'Autorité sectorielle compétente. Dans ce cas la structure mise en place par l'Autorité sectorielle doit bénéficier d'un agrément délivré par l'Autorité nationale de Cybersécurité.

Cependant, deux ou plusieurs autorités sectorielles peuvent mutualiser leurs ressources pour mettre en place un CERT sectoriel commun.

La gestion et l'exploitation d'un CERT sectoriel peuvent également être confiées aux prestataires agréés de cybersécurité visés à l'article 15 de la présente loi.

Article 39.- Mise en place de Services des Opérations de Cybersécurité (SOC)

Chaque exploitant d'IIC met en place, au plus tard, un (1) an après la notification de son inscription sur le répertoire national des IIC, un Service des Opérations de Cybersécurité (SOC), dont la mission est de surveiller, d'analyser et de protéger son infrastructure numérique.

Les Services des Opérations de Cybersécurité sont notamment chargés :

- de la surveillance en temps réel des réseaux, systèmes et applications de l'IIC ;
- de la protection des données de l'IIC ;
- du suivi des vulnérabilités (de la détection à la correction) ;
- de la veille en sécurité informatique ;
- du pilotage de la mise en œuvre des correctifs de sécurité ;
- de la sensibilisation des utilisateurs ;
- de la fourniture d'expertise et de conseil auprès des équipes informatiques
- du suivi des obligations réglementaires de cybersécurité.

Article 40.- Gestion et exploitation des SOC

La gestion d'un SOC peut être assurée par l'exploitant de l'IIC lui-même, dans des conditions fixées par voie réglementaire ou être confiée à un prestataire agréé par l'Autorité nationale de Cybersécurité.

Les prestataires fournissant des services de SOC doivent respecter les exigences fixées par l'article 15 de la présente loi ainsi que par les textes pris pour son application.

Article 41.- Relations entre SOC, CERT sectoriels et CERT national

Les modalités de partage d'information entre les Services des Opérations de Cybersécurité, les CERT sectoriels et le CERT national, avec précisions des notifications facultatives et des notifications automatiques, seront fixées par voie réglementaire.

Article 42.- Cadre national de collaboration dans la gestion des incidents de cybersécurité

Les autorités administratives et judiciaires, ainsi que les entités du secteur non étatique, coopèrent pleinement à l'effet de remplir leurs missions en matière de protection des IIC. A cet effet, elles établissent un Cadre national de Coordination des Activités de Détection, d'Alerte et de Réponse aux Incidents informatiques et autres cyberattaques (CADARCA).

Les informations échangées au sein de ce Cadre se limitent à ce qui est pertinent et sont proportionnées à l'objectif de cet échange, notamment dans le respect des dispositions législatives et réglementaires relatives à la protection du secret administratif.

Section V.- Modalités de partage d'information et de renseignement

Article 43.- Protection du secret en rapport avec la protection des IIC

Les dispositions de la présente section ne portent pas préjudice à l'application des règles législatives et réglementaires relatives à la protection du secret de l'information administrative ainsi qu'aux obligations de discrétion et de confidentialité pesant sur les agents de l'administration.

Dans ce cadre, les informations en relation avec le travail de protection des IIC peuvent être classifiées par les Administrations intervenant dans ce domaine, en fonction de leur degré de sensibilité.

Par ailleurs, les personnes n'ayant pas la qualité d'agent de l'administration, et qui par un biais quelconque, ont accès à une information en lien avec la protection des IIC, sont soumises aux mêmes règles de confidentialité et de discrétion professionnelle que les agents publics et les services de l'Etat. En cas de non-respect de cette obligation de confidentialité, ces personnes encourent les sanctions pénales prévues par la présente loi.

Article 44.- Communication en rapport avec la protection des IIC

Toutefois, nonobstant les dispositions de l'article précédent, les autorités étatiques compétentes ainsi que l'Autorité nationale de Cybersécurité peuvent informer le public d'incidents particuliers ou imposer aux exploitants d'IIC de le faire, lorsque cette information peut s'avérer nécessaire, soit pour prévenir ou gérer un incident en cours, soit pour d'autres raisons d'intérêt public.

Le choix des informations à porter à l'attention du public doit être guidé par des considérations de proportionnalité, de prudence et de pertinence.

Article 45.- Collaboration avec les autorités étrangères

Les informations en lien avec la protection des IIC peuvent également être partagées avec des autorités étrangères chargées de la cybersécurité lorsque les modalités de ce partage auront été fixées par des accords liant l'État du Sénégal à l'État dont dépendent ces autorités.

Le partage d'information peut également avoir lieu avec des Institutions communautaires investies de missions de cybersécurité, lorsque ce partage aura été organisé par les textes communautaires.

Le partage d'information visé aux alinéas précédents se fait sans préjudice de la préservation des buts de sécurité nationale et des intérêts essentiels de la Nation. Il se

fait également dans le respect du secret des procédures judiciaires, et en particulier celles pénales.

Article 46.-Collaboration avec les autorités judiciaires

Lorsqu'une enquête judiciaire est ouverte, les autorités administratives en charge de la cybersécurité collaborent avec les autorités judiciaires dans le respect des règles du Code de procédure pénale et des autres textes applicables aux enquêtes en matière pénale. L'Autorité nationale de Cybersécurité ainsi que les prestataires agréés de services de cybersécurité peut être requis en leurs capacités techniques pour apporter leur concours aux enquêtes pénales.

Section VI. - Audits et contrôles

Article 47.- Audits réalisés par les exploitants d'IIC

Tout exploitant d'IIC réalise, chaque année et à ses frais, un audit interne de ses réseaux et systèmes d'information qui doit lui permettre de s'assurer que les règles et normes de sécurité élaborées par l'Etat ainsi que les processus définis dans son programme de cybersécurité sont respectés.

Les rapports de l'audit, sont transmis, dans les quinze (15) jours qui suivent leur élaboration à l'Autorité responsable du secteur auquel est rattaché l'IIC et à l'Autorité nationale de Cybersécurité.

Un audit externe est réalisé tous les trois (3) ans, par l'exploitant d'IIC. Le rapport de cet audit est également, respectivement transmis à l'Autorité sectorielle et à l'Autorité nationale de Cybersécurité dans les mêmes conditions que celles précisées à l'alinéa précédent.

Article 48.- Audits et contrôles réalisés par l'Autorité nationale de Cybersécurité

Nonobstant les audits réalisés par l'exploitant d'IIC lui-même, l'Autorité nationale de Cybersécurité conduit un programme d'audit relatif aux IIC. Ces audits, réalisés sur pièce et sur place, sont destinés à vérifier le respect des obligations et normes s'appliquant aux IIC et à connaitre le niveau de sécurité de leurs réseaux et systèmes d'information.

Les audits portent notamment sur les domaines suivants :

- réseaux et systèmes d'information ;
- infrastructure physique ;
- infrastructure logique
- projets et marchés ;
- conformité ;
- communication.

L'Autorité nationale de Cybersécurité peut recourir à des prestataires agréés pour réaliser son programme d'audit.

En dehors de son programme d'audit, l'Autorité nationale de Cybersécurité peut réaliser des audits et contrôles ponctuels toutes les fois que cela s'avère nécessaire.

Article 49.- Conduite des opérations d'audit

Les exploitants d'IIC sont tenus de communiquer aux agents de l'Autorité nationale de Cybersécurité ou à ceux des prestataires travaillant au nom de cette dernière, toutes informations qu'ils jugent pertinentes dans l'accomplissement de leurs missions.

Les agents de l'Autorité nationale de Cybersécurité et ceux des prestataires travaillant pour cette dernière, accèdent sans entrave ni refus, à tout lieu situé sur le territoire national dans lequel se trouverait tout ou une partie d'un système d'information ou d'un équipement dont les auditeurs estiment l'examen nécessaire à l'accomplissement de leur mission.

Les agents de l'Autorité nationale Cybersécurité intervenant dans la conduite des audits prêtent serment dans les conditions prévues par l'article 33 de la présente loi pour les agents du CERT national.

Chapitre IV.- Sanctions administratives et pénales

Section première. - Sanctions administratives

Article 50.- procédure de constatation et de prononcé des sanctions administratives

Lorsqu'un ou plusieurs manquements aux exigences pesant sur un exploitant d'IIC sont constatés, l'Autorité nationale de Cybersécurité met en demeure l'exploitant d'IIC concerné de se conformer, dans un délai qu'elle fixe, aux obligations qui lui incombent.

Le délai est déterminé en tenant compte des conditions de fonctionnement de l'exploitant d'IIC et des mesures à mettre en œuvre.

Au préalable, l'Autorité nationale de Cybersécurité informe, de manière motivée, le contrevenant de son intention de lui adresser une mise en demeure et lui fait part de son droit, dans les quinze (15) jours de la réception de cette information, de formuler par écrit ses moyens de défense ou de solliciter d'être d'entendu.

Lorsque les mesures dont l'Autorité nationale de Cybersécurité demandent l'accomplissement ne sont pas prises dans le délai indiqué, l'Autorité nationale de Cybersécurité transmet le dossier de ses constatations ainsi que les réponses de l'exploitant d'IIC en faisant une proposition de sanction appropriée à l'autorité administrative compétente pour prononcer la sanction.

L'exploitant d'IIC concerné peut se faire assister ou représenter par une personne de son choix auprès de l'autorité chargée du prononcé de la sanction. À l'issue d'une procédure contradictoire, l'autorité compétente peut prononcer à l'encontre de l'exploitant de l'IIC concerné une ou plusieurs des sanctions visées à l'article 51 de la présente loi.

Les sanctions administratives prises à l'issue de cette procédure contradictoire peuvent faire l'objet de recours devant les juridictions administratives compétentes.

Article 51.- Types de sanctions administratives

Un décret désignera l'autorité ou les autorités chargées de prononcer des sanctions administratives contre les personnes morales exploitant les IIC.

Lesdites sanctions sont les suivantes :

1) l'avertissement ;
2) le blâme ;
3) l'amende administrative dont le montant proportionné à la gravité du manquement reproché à l'exploitant de l'IIC, est comprise entre 1.000.000 de francs CFA et 800.000.000 frs CFA.
4) l'amende administrative portée à un montant compris entre 1 à 5% du chiffre d'affaires de l'entité concernée lorsque la gravité des faits reprochés à cette dernière est telle que l'autorité administrative estime que le montant de 800.000.000 frs CFA doit être dépassé.

L'amende administrative ne peut être prononcée que pour autant que les manquements visés n'ont pas déjà fait l'objet de condamnations pénales.

Lorsqu'une condamnation pénale définitive advient à la suite d'une sanction administrative définitive, l'exploitant n'est astreint par les juridictions pénales compétentes, qu'au paiement du surplus résultant de la différence entre les deux amendes.

Lorsque le montant de l'amende pénale est inférieur ou égal à celui de l'amende administrative, le paiement des deux sommes se cumulera.

Section II.- Sanctions pénales

Article 52.- Procédure de constatation des infractions pénales

Outre les officiers de police judiciaire, les agents de l'Autorité nationale de Cybersécurité, assermentés dans les conditions fixées par voie réglementaire, sont habilités à rechercher et à constater, par procès-verbaux, les infractions aux dispositions de la présente loi et des textes pris pour son application.

Ces agents assermentés exercent, en dehors de ceux prévus aux articles 55 à 55 ter du Code de procédure pénale, les pouvoirs dévolus aux autorités de police judiciaire dans le Code de procédure pénale. Lesdits pouvoirs sont exercés dans les conditions prévues à l'article 21 du Code de procédure pénale.

Article 53.- Infractions visant les personnes morales

Est sanctionné conformément aux dispositions du Code pénal relatives à la responsabilité pénale des personnes morales :

1) tout exploitant d'IIC qui aura omis de prendre les mesures prescrites à l'article 27 alinéa 2 de la présente loi ou aux textes pris pour son application ;
2) tout exploitant d'IIC ayant utilisé des produits ou services non certifiés en violation de l'article 28 de la présente loi ;
3) tout exploitant d'IIC ayant confié des services de cybersécurité à un prestataire non agréé, en violation des dispositions de l'article 15 de la présente loi et des textes pris pour son application ;
4) toute personne morale ayant fourni l'une des prestations de cybersécurité, visées à l'article 15 sans être agréée par l'Autorité nationale de Cybersécurité ou ayant continué à fournir ces prestations malgré le retrait de son agrément par ladite autorité ;
5) tout exploitant d'IIC dont les agents ou personnes agissant sous la responsabilité ou autorité, auront refusé, empêché ou entravé d'une quelconque manière, l'exercice par les agents du CERT national, des missions qui leur sont dévolues par la présente loi ;
6) tout exploitant d'IIC dont les agents ou personnes agissant sous la responsabilité ou autorité auront refusé, empêché ou entravé d'une quelconque manière la conduite des opérations d'audit prévues aux articles 10, 48 et 49 de la présente loi ;
7) tout exploitant de système d'information qui aura procédé à l'hébergement de ses données en dehors du territoire national, en violation des dispositions de l'article 12 alinéa 1 de la présente loi ;
8) tout exploitant dont le système d'information a été utilisé à son insu pour propager des programmes malveillants ou pour accomplir des actes illicites et qui sera abstenu d'exécuter les directives de l'Autorité nationale de cybersécurité, après en avoir été informé ;
9) tout exploitant d'un système d'information critique qui n'aura pas procédé à la déclaration d'un incident dans les conditions fixées par la présente loi et les textes réglementaires pris pour son application ;
10) tout opérateur de télécommunications ou exploitant de système d'information, qui n'aura pas informé ses clients de l'existence d'une attaque ayant entraîné la violation de leurs données sauf lorsqu'Autorité nationale de Cybersécurité aura décidé de surseoir à cette communication.

Article 54.- Infractions visant les personnes physiques

Sans préjudice de l'application de l'article précédent, est puni d'une peine d'emprisonnement de 06 mois à 05 ans et d'une peine d'amende de 500.000 frs CFA à 10.000.000 frs CFA :

1) quiconque, par quelque moyen que ce soit, fait obstacle, empêche ou entrave d'une quelconque manière :

- le déroulement des audits de sécurité des systèmes d'information prévus par la présente loi ;
- l'exercice par les agents du CERT, des fonctions qui leur sont dévolues par la présente loi ;

2) toute personne dont le système d'information a été utilisé à son insu pour propager des programmes malveillants ou pour accomplir des actes illicites, qui s'abstient d'exécuter les directives de l'autorité nationale, après en avoir été requis ;
3) toute personne physique ou professionnel de la cybersécurité ayant fourni, ou participé d'une quelconque manière, à la fourniture des services réservés aux prestataires agréés de cybersécurité, en violation de l'article 15 de la présente loi et des textes pris pour son application ;
4) toute personne qui, après en avoir été requis par les agents du CERT national en application de l'article 36 de la présente loi, aura omis d'effectuer les diligences demandées alors qu'il avait la capacité de le faire ;
5) Toute personne n'ayant pas la qualité d'agent de l'Etat qui, étant dépositaire par ses fonctions ou par tout autre moyen, d'informations classifiées en relation avec la protection des IIC, les aura divulguées ;
6) Toute personne qui :
   - étant préposé par ses fonctions ou ses attributions au sein d'une entité, à informer les personnes appropriées de cette entité, de l'existence d'un incident de cybersécurité au sens de l'article 35 de la présente loi, aura omis de le faire ;
   - étant préposé par ses fonctions ou ses attributions, à déclarer au CERT national ou à un CERT sectoriel, l'existence d'un incident de cybersécurité au sens de l'article 35 de la présente loi, aura omis de le faire, alors que les systèmes d'information affectés par l'incident de cybersécurité ont été déclarés critiques.

Chapitre V.- Disposition finale

Article 55.- Texte d'application

Les autres modalités d'application de la présente loi sont fixées, en tant que de besoin, par décret.