RÉPUBLIQUE DE VANUATU

PROJET DE
LOI N° DE 2026 SUR LA CYBERSÉCURITÉ

Exposé des motifs

En novembre 2022, une attaque par rançongiciel a frappé le réseau à haut débit du gouvernement de Vanuatu. Simultanément, les systèmes de messagerie gouvernementaux, les disques partagés et les services vocaux sont tombés en panne. Les infrastructures d'information critiques (IIC) au sein de l'État, notamment les systèmes soutenant les hôpitaux, les services financiers publics et d'autres services publics, ont été gravement touchées, bloquant l'accès aux outils opérationnels essentiels. En conséquence, le recouvrement des recettes, les procédures d'octroi de licences, les fonctions administratives des tribunaux et de nombreuses autres activités ont été paralysés. Le processus de rétablissement a pris plusieurs mois et a nécessité le soutien des partenaires de développement. Par la suite, une organisation criminelle a revendiqué l'attaque, affirmant avoir exfiltré 3,2 téraoctets de données.

Depuis, la menace n'a cessé de croître au lieu de reculer. Les rançongiciels ciblant les petits États, dont Vanuatu, sont désormais vendus en tant que service. L'intrusion hostile dans les réseaux gouvernementaux est devenue un instrument de politique étatique tout autant qu'un acte criminel. Vanuatu ne peut plus se contenter d'un dispositif dépourvu de fondement juridique.

Le présent projet de loi établit des garde-fous juridiques clairs et proactifs afin de sauvegarder les IIC, l'économie et les informations numériques de Vanuatu, tout en protégeant les citoyens contre l'escalade des cybermenaces. Cette initiative vise également à sécuriser les services critiques et à instaurer des critères de référence en matière de sécurité. Le projet de loi fixe des normes précises, améliore le partage d'informations sur les menaces, renforce les protections juridiques et introduit des protocoles de notification obligatoire.

Les principales caractéristiques du présent projet de loi sont détaillées ci-dessous :

a) La création de l'Agence nationale de la cybersécurité (« l'Agence ») en tant qu'autorité nationale de référence en matière de cybersécurité.

b) L'Agence élabore et coordonne la politique nationale de cybersécurité, émet des codes de pratique et des normes techniques, conseille le ministre et le Conseil des ministres, et représente Vanuatu à l'échelle internationale sur les questions de cybersécurité et de protection des IIC.

c) La désignation des IIC sur la base de critères énoncés explicitement dans la Loi et liés à une annexe des services essentiels. Les opérateurs désignés doivent faire réaliser des audits annuels de cybersécurité, maintenir des plans de gestion des risques, nommer un responsable de la sécurité des systèmes d'information ou un agent équivalent, signaler les cyberincidents graves, participer aux exercices cybernationaux et informer l'Agence avant d'apporter des modifications importantes à l'architecture de leurs infrastructures. Un système situé hors de Vanuatu peut être désigné dès lors qu'un service essentiel du pays en dépend.

d) Le ministre peut, sur avis du directeur, déclarer l'état d'urgence cybernétique nationale si un cyberincident grave menace la sécurité nationale, la sécurité publique, l'économie ou les services essentiels, et qu'il est susceptible d'entraîner des effets dépassant les capacités des opérations normales de cybersécurité. Une telle déclaration dure habituellement 30 jours, mais peut être révoquée plus tôt ou prorogée. En période d'urgence, le ministre peut ordonner aux organismes publics et aux opérateurs d'IIC d'agir ou de s'abstenir d'agir, et ces derniers sont tenus de s'y conformer nonobstant les dispositions de toute autre loi.

e) Le projet de loi dotera Vanuatu d'une autorité légalement responsable de la sécurité des systèmes dont dépend le pays. Il transforme une capacité informelle en une compétence statutaire, impose

des obligations exécutoires à ceux qui exploitent des systèmes critiques, et donne à l'État une base légale pour agir pendant qu'une attaque est en cours, plutôt qu'uniquement après qu'elle a pris fin. Il offre également aux partenaires régionaux et internationaux un homologue doté de la légitimité nécessaire pour traiter avec eux. Sans ce texte, la transformation numérique de Vanuatu se poursuivrait en présumant, à tort, que rien ne peut défaillir.

Le Premier Ministre

RÉPUBLIQUE DE VANUATU

PROJET DE
LOI N° DE 2026 SUR LA CYBERSECURITE

Table des matières

TITRE 1 DÉFINITIONS

1 Définitions 3

TITRE 2 AGENCE NATIONALE DE CYBERSÉCURITÉ ET DIRECTEUR

Sous-titre 1 Création de l'Agence nationale de cybersécurité

2 Création 6

3 Fonctions 6

Sous-titre 2 Directeur

5 Directeur 7

6 Fonctions du directeur 7

7 Pouvoirs du directeur 8

TITRE 3 CONSEIL CONSULTATIF NATIONAL SUR LA CYBERSÉCURITÉ

8 Création du Conseil 9

9 Composition du Conseil 9

10 Fonction du Conseil 10

11 Présidence et vice-présidence du Conseil 10

12 Réunions du Conseil 10

13 Indemnités de séance des membres du Conseil 11

14 Révocation d'un membre du Conseil 11

TITRE 4 DÉCLARATION D'ÉTAT D'URGENCE CYBERNÉTIQUE NATIONALE

15 Déclaration d'état d'urgence cybernétique nationale 12
16 Diffusion de la déclaration 12
17 Durée de l'état d'urgence cybernétique nationale 12
18 Directives ministérielles aux organismes publics et aux opérateurs d'IIC 13
19 Pouvoirs exceptionnels en période de crise 13

TITRE 5 LUTTE CONTRE LES RANÇONGICIELS ET L'ESPIONNAGE

20 Mesures contre les rançongiciels 14
21 Mesures contre l'espionnage 14

TITRE 6 INFRASTRUCTURES D'INFORMATION CRITIQUES

22 Désignation des infrastructures d'informations critiques 16
23 Désignation d'urgence à titre provisoire 17
24 Désignation des fournisseurs d'informations sur les infrastructures critiques 18

TITRE 7 OBLIGATIONS EN MATIÈRE DE CYBERSECURITÉ

25 Obligations des organismes publics et des entités déclarantes 19
26 Obligations des opérateurs d'IIC 19

TITRE 8 APPLICATION DE LA LOI

27 Agent habilité 20
28 Demande de divulgation des informations et des documents 21
29 Pouvoirs d'accès 21
30 Pouvoirs d'accès 22
31 Récépissé des éléments saisis 23
32 Restitution des éléments saisis 23
33 Assistance de la police aux agents habilités 24
34 Mandats de perquisition 24

TITRE 9 INFRACTIONS ET PENALITÉS

35 Infractions 26
36 Avis de pénalité 28

TITRE 10 DISPOSITIONS DIVERSES

37 Modification de l'annexe 29
38 Rapport annuel 29
39 Immunité 29
40 Règlements 29
41 Entrée en vigueur 30

ANNEXE

RÉPUBLIQUE DE VANUATU

PROJET DE
LOI N° DE 2026 SUR LA CYBERSÉCURITÉ

Loi prévoyant la création, le fonctionnement et la gestion de l'Agence nationale de cybersécurité et d'autres questions connexes.

Le Président de la République et le Parlement promulguent le texte suivant-

TITRE 1 DÉFINITIONS

1 Définitions

Dans la présente loi, à moins qu'une intention contraire n'apparaisse :

Agence désigne l'agence nationale de cybersécurité établie en vertu de l'article 2 ;

agent habilité désigne une personne nommée en qualité d'agent habilité en vertu de l'article 27 ;

Conseil désigne le conseil consultatif national de cybersécurité établi en vertu de l'article 8 ;

système informatique a le même sens que dans la Loi n°22 de 2021 sur la Cybercriminalité et s'entend également de tout système de technologie opérationnelle, y compris un système de commande industrielle, un automate programmable industriel, un système de contrôle et d'acquisition de données en temps réel (SCADA) ainsi qu'un système de contrôle commande réparti, que ce système constitue ou non un ordinateur au sens de ladite loi.

infrastructures d'information critiques (IIC) désigne tout système informatique, infrastructure, réseau ou service associé dont l'interruption ou la compromission aurait un impact important sur la sécurité nationale, la sécurité publique, la santé publique, l'économie ou les services essentiels ;

opérateur des infrastructures d'information critiques (opérateur d'IIC) désigne toute personne qui exploite, gère ou contrôle une infrastructure critique désigné ;

incident cybernétique désigne tout événement qualifié compromettant la confidentialité, l'intégrité ou la disponibilité d'un système informatique ou des données.

fournisseur critique désigne un vendeur, un entrepreneur ou un prestataire de services dont les biens, les composants ou les services sont essentiels aux opérations fondamentales, à la sécurité, à la conformité ou à la continuité des activités d'une organisation, de sorte que toute défaillance ou interruption de leur fourniture causerait de graves dommages ou préjudices économiques, opérationnels, financiers, sociétaux ou réputationnels ;

cybermenace désigne toute situation ou tout événement susceptible de nuire à un système informatique.

protection de la cybersécurité désigne la protection des systèmes informatiques, des réseaux et des données contre les attaques, les dommages ou les accès non autorisés ;

risque de cybersécurité désigne la probabilité d'occurrence et l'impact d'un cyberincident ;

cyberespionnage désigne une intrusion non autorisée, parrainée par un État ou organisée, dans des systèmes informatiques à des fins de collecte de renseignements ;

infrastructure désignée désigne une infrastructure d'information critique désignée en vertu de l'article 22 ;

directeur désigne le directeur de l'Agence nationale de cybersécurité ;

directeur général désigne le directeur général du ministère responsable de la cybersécurité

service essentiel désigne tout service désigné comme essentiel à l'Annexe ;

organisme public signifie:

a) un ministère ;

b) une institution constitutionnelle ;

c) un établissement ou un organisme créé par une loi ; ou

d) un organisme crée par voie réglementaire ;

ministre désigne le ministre responsable de la cybersécurité ;

ransomware ou rançongiciel désigne un logiciel malveillant qui chiffre les données et exige un paiement pour leur déchiffrement ;

entité réglementée désigne une organisation, une institution, une entreprise ou un particulier qui est autorisé et tenu d'exercer ses activités en vertu de règles et de lois spécifiques, et qui est soumis à la surveillance continue d'un organisme public ou d'une autorité de réglementation directement lié par les obligations légales de la Loi ;

entité déclarante désigne tout organisme public, organisme statutaire, personne morale, société, organisation, opérateur de CII, fournisseur critique ou toute autre entité tenue, en vertu de la présente loi, d'adresser un rapport à l'Agence ;

incident cyber grave désigne un incident cybernétique compromettant gravement la disponibilité, l'intégrité ou l'exploitation d'une infrastructure d'information critique et des services essentiels ;

faille de sécurité désigne un défaut ou une faiblesse au sein d'un système informatique ou d'un réseau susceptible d'être exploité à des fins malveillantes.

TITRE 2 AGENCE NATIONALE DE CYBERSÉCURITÉ ET DIRECTEUR

Sous-titre 1 Création de l'Agence nationale de cybersécurité

2 Création

Est ainsi créé l'Agence nationale de cybersécurité.

3 Fonctions

L'Agence a les fonctions suivantes :

a) élaborer, réviser et coordonner les politiques et les stratégies nationales en matière de cybersécurité ;

b) gérer les opérations nationales et internationales de cybersécurité ;

c) surveiller et coordonner les mesures d'intervention face aux incidents et aux menaces de cybersécurité ;

d) désigner et contrôler les infrastructures d'information critiques ;

e) veiller à la protection des infrastructures d'information critiques ;

f) mener des enquêtes et collecter des renseignements ;

g) mener des activités de recherche et de développement en matière de cybersécurité et de cybercriminalité ;

h) planifier et mener des simulations et des exercices nationaux de gestion des crises cybernétiques ;

i) promouvoir l'innovation cybernétique et le développement des technologies émergentes ;

j) représenter le Vanuatu à l'échelle internationale pour toutes les questions relatives à la cybersécurité ;

k) mener des campagnes de sensibilisation et d'éducation du public sur la cybersécurité au Vanuatu ;

l) assurer le rôle de point de contact pour la coopération cybernétique nationale et internationale ;

m) élaborer des normes techniques ;

n) conseiller le ministre sur les questions relatives à l'application de la présente loi ; et

o) exercer toutes autres fonctions qui peuvent lui être conférées par la présente loi ou par toute autre loi.

4 Pouvoirs

1) L'Agence a le pouvoir de prendre toutes les mesures nécessaires ou utiles à l'exercice de ses fonctions en vertu de la présente loi.

2) Sans limiter la portée du paragraphe 1), l'Agence a le pouvoir d'accomplir tout ou partie des actes suivants :

a) émettre des directives ;

b) publier des codes de bonnes pratiques en matière de cybersécurité ; et

c) réaliser des audits et évaluations de cybersécurité auprès des entités réglementées.

Sous-titre 2 Directeur

5 Directeur

1) Le directeur est responsable de la gestion et de l'administration quotidienne de la présente loi.

2) Le directeur conseille et assiste le ministre et le directeur général sur toute question relative à l'Agence conformément aux exigences de la présente loi.

6 Fonctions du directeur

Le directeur a les fonctions suivantes :

a) conseiller le Conseil consultatif et le ministre sur toute question relative à l'application de la présente loi ;

b) rendre compte au ministre, de toute menace, tout incident et tout risque émergent en matière de cybersécurité qui affectent le Vanuatu ;

c) conseiller le ministre et le Conseil des ministres, après avis du Conseil consultatif, sur les questions relatives à la cybersécurité ;

d) gérer et superviser les opérations de l'Agence ; et

e) élaborer chaque année un programme de travail national sur la cybersécurité ; et

f) assurer le suivi et la mise en œuvre de la stratégie nationale de cybersécurité et rendre compte au ministre de son progrès ; et

g) exercer toute autre fonction qui peut lui être conférée par la présente loi ou toute autre loi.

7 Pouvoirs du directeur

1) Le directeur a le pouvoir de prendre toutes les mesures nécessaires ou utiles à l'exercice de ses fonctions en vertu de la présente loi.

2) Sans préjudice à la portée générale du paragraphe 1), le directeur peut enjoindre par écrit à un organisme public, une entité réglementée, un opérateur d'infrastructures d'information critiques (IIC) ou un fournisseur critique :

   a) de prévenir un incident ou une menace cybernétique, ou d'y remédier ; ou

   b) de se conformer à un code de bonnes pratiques.

TITRE 3 CONSEIL CONSULTATIF NATIONAL SUR LA CYBERSÉCURITÉ

8 Création du Conseil

Est ainsi créé le Conseil consultatif national sur la cybersécurité.

9 Composition du Conseil

1) Le Conseil est composé des personnes suivantes :

   a) le directeur du service des Communications et de la transformation numérique ;

   b) le directeur des Finances et de la trésorerie ;

   c) le conseiller sur la sécurité nationale ;

   d) un officier supérieur représentant du Corps de police nommé par le commissaire de la police ;

   e) un représentant de l'Université nationale de Vanuatu nommé par le son chancelier ; et

   f) un représentant de la Chambre de commerce et d'industrie nommé par son président.

2) Sous réserve des dispositions du paragraphe 4), le ministre nomme les membres visés aux alinéas 1)e) et f).

3) La personne désignée en vertu de l'alinéa 1)d) doit posséder des connaissances opérationnelles ou une expérience pertinente en matière de cybercriminalité, de cybersécurité, d'enquêtes numériques, de renseignement ou dans d'autres domaines connexes de l'application de la loi.

4) Toute personne nommée en vertu de l'alinéa 1)e) ou f) doit :

   a) détenir un diplôme de l'enseignement supérieur en cybersécurité, en infrastructure numérique, en gestion des risques, en informatique, en technologies de l'information, en ingénierie, en droit, en administration publique ou dans un domaine connexe ;

b) justifier d'au moins 5 ans d'expérience dans le domaine de la cybersécurité, des technologies de l'information ou de la sécurité numérique ;

c) ne pas avoir fait l'objet d'une condamnation pour une infraction grave impliquant la malhonnêteté, la corruption, la cybercriminalité ou l'abus de fonctions ; et

d) être citoyen du Vanuatu.

5) Un membre nommé en vertu de l'alinéa 1)e) ou f) l'est pour un mandat de 4 ans renouvelable.

10 Fonction du Conseil

1) La fonction du Conseil est strictement consultative.

2) Le Conseil conseille le directeur sur :

a) toute politique relative à la cybersécurité ;

b) toute question relative aux infrastructures d'information critiques ; et

c) les grandes orientations réglementaires.

3) Pour éviter toute doute, le Conseil ne dispose d'aucun pouvoir décisionnel.

11 Présidence et vice-présidence du Conseil

1) Les membres du Conseil élisent un président parmi eux.

2) Les membres du Conseil élisent un vice-président parmi eux.

3) Le vice-président exerce ses fonctions pour un mandat de 1 an renouvelable.

12 Réunions du Conseil

1) Le Conseil se réunit au moins une fois par trimestre civil et peut tenir toutes autres réunions nécessaires au bon exercice de ses fonctions en vertu de la présente loi.

2) Le président préside toutes les réunions du Conseil et, en son absence, le vice-président y préside.

3) Le quorum requis pour la tenue d'une réunion est fixé à 4 membres présents.

4) Chaque membre présent à la réunion dispose d'une voix. Les décisions du Conseil sont prises à la majorité des suffrages exprimés.

5) En cas de partage égal des voix, le président ou le vice-président (s'il préside la réunion) a voix prépondérante.

6) L'Agence assure le secrétariat du Conseil.

7) L'Agence, après consultation du président, notifie aux autres membres du Conseil le lieu, l'heure et la date de la réunion.

8) Sous réserve des dispositions de la présente loi, le Conseil détermine et régit ses propres règles de procédure.

13 Indemnités de séance des membres du Conseil

Le ministre peut, sur avis du directeur, fixer par arrêté les indemnités de séance des membres du Conseil.

14 Révocation d'un membre du Conseil

Un membre nommé en vertu de l'alinéa 9 1)e) ou f) est révoqué de ses fonctions si il :

a) n'assiste pas à 3 réunions consécutives du Conseil sans l'autorisation de ce dernier ;

b) fait l'objet d'une suspension de l'exercice de sa profession ; ou

c) est incapable de remplir ses fonctions de membre.

TITRE 4 DÉCLARATION D'ÉTAT D'URGENCE CYBERNÉTIQUE NATIONALE

15 Déclaration d'état d'urgence cybernétique nationale

1) Le ministre peut, sur avis du directeur, déclarer par arrêté l'état d'urgence cybernétique nationale sur tout ou une partie de Vanuatu en raison d'un cyberincident.

2) Pour procéder à la déclaration visée au paragraphe 1), le ministre doit être convaincu que le cyberincident :

   a) constitue un incident cybernétique grave menaçant la sécurité nationale, la sécurité publique, l'économie ou les services essentiels ; et

   b) est susceptible d'entrainer des effets qui dépassent les capacités des opérations normales de cybersécurité.

16 Diffusion de la déclaration

Après la déclaration d'un état d'urgence cybernétique nationale en vertu de l'article 15, le ministre doit en informer le public par voie médiatique.

17 Durée de l'état d'urgence cybernétique nationale

1) La déclaration d'état d'urgence cybernétique nationale prend effet immédiatement le jour où elle est prise.

2) La déclaration d'état d'urgence cybernétique nationale n'empêche pas la déclaration d'un nouvel état d'urgence lié au même incident cybernétique nationale ou à un incident différent.

3) La déclaration d'état d'urgence cybernétique nationale prend fin 30 jours après le jour où elle a été prise, à moins que, sur avis de l'Agence :

   a) le ministre ne révoque la déclaration d'état d'urgence cybernétique nationale plus tôt si elle n'est plus nécessaire ; ou

   b) le ministre ne proroge la déclaration d'état d'urgence cybernétique nationale pour une nouvelle période, conformément à la recommandation du directeur.

18 Directives ministérielles aux organismes publics et aux opérateurs d'IIC

1) Si une déclaration d'état d'urgence cybernétique nationale est e-n vigueur, le ministre peut, sur avis de l'Agence, ordonner à tout organisme public ou opérateurs d'infrastructures d'information critiques (IIC) d'accomplir ou de s'abstenir d'accomplir tout acte, ou d'exercer ou de s'abstenir d'exercer toute fonction.

2) Lorsqu'une directive est donnée à un organisme public ou à un opérateur d'IIC en vertu du présent article, ceux-ci sont tenus de s'y conformer, les dispositions de toute autre loi.

19 Pouvoirs exceptionnels en période de crise

1) Les pouvoirs prévus au présent article s'appliquent uniquement pendant un état d'urgence cybernétique nationale.

2) Si le directeur est convaincu que cela est nécessaire dans l'intérêt de la sécurité, il peut autoriser un agent de l'Agence :

a) à ordonner à une personne d'accomplir l'un ou l'ensemble des actes suivants :

i) quitter des locaux particuliers et s'éloigner d'une zone d'urgence cybernétique nationale ;

ii) ne pas pénétrer dans une zone d'urgence cybernétique nationale ;

iii) divulguer toute information ou tout document ; ou

b) à fermer tout lieu public ou privé pendant l'urgence cybernétique nationale.

3) Si la personne ne se conforme pas à la directive visée au paragraphe 2), l'agent de l'Agence peut prendre toutes les mesures raisonnablement nécessaires pour en assurer le respect, en faisant usage de la force si les circonstances le justifient raisonnablement.

4) Un officier de police peut, à la demande du directeur, prêter assistance à ce dernier dans l'exercice des pouvoirs qui lui sont conférés en vertu du paragraphe 2).

TITRE 5 LUTTE CONTRE LES RANÇONGICIELS ET L'ESPIONNAGE

20 Mesures contre les rançongiciels

1) Tout organisme public, entité déclarante ou opérateur d'IIC qui détecte un cyberincident grave impliquant une attaque par rançongiciel doit adresser une alerte précoce à l'Agence dans les 24 heures suivant sa détection.

2) Outre l'envoi de l'alerte précoce visée au paragraphe 1), l'organisme public, l'entité déclarante ou l'opérateur d'IIC doit, dans les 72 heures suivant cet envoi, déterminer s'il s'agit d'un cyberincident grave impliquant une attaque par rançongiciel et notifier cette décision à l'Agence

3) Sur demande, l'Agence doit, dans les 24 heures suivant la notification reçue en vertu du paragraphe 2), répondre à l'organisme public, à l'entité déclarante ou à l'opérateur d'IIC en lui fournissant un premier retour d'information ainsi que des orientations en matière d'atténuation des risques.

4) Dès lors qu'il est établi qu'un cyberincident grave impliquant une attaque par rançongiciel a eu lieu, l'Agence doit :

   a) réaliser une évaluation initiale des risques ;

   b) coordonner les mesures de confinement et de rétablissement ;

   c) fournir des orientations techniques ;

   d) demander les informations pertinentes ; et

   e) assurer la coordination avec la police, les organismes de sécurité nationale et les autres autorités compétentes, lorsque cela s'avère nécessaire.

5) L'Agence doit fournir un rapport dans les 30 jours suivant le moment où il a été établi qu'une attaque par rançongiciel s'est produite.

21 Mesures contre l'espionnage

1) Si une personne prend connaissance :

   a) d'un accès non autorisé à un système informatique ; ou

b) d'une utilisation non autorisée d'un système informatique,

dans des circonstances suggérant raisonnablement que des informations sont collectées au profit d'un État étranger ou d'un groupe organisé, elle doit signaler les faits à l'Agence dans les meilleurs délais possibles.

2) Une personne qui signale de bonne foi en vertu du paragraphe 1) n'encourt aucune responsabilité civile, pénale ou professionnelle pour manquement à ses obligations, et ne peut faire l'objet d'aucun préjudice dans le cadre de son emploi en raison de ce signalement.

3) Sous réserve du paragraphe 2), l'identité de la personne auteur du signalement doit être protégée, sauf consentement de sa part ou sur ordonnance du tribunal.

4) Après réception d'un signalement en vertu du paragraphe 1), l'Agence doit mener une enquête sur les faits présumés de cyberespionnage.

5) À l'issue de l'enquête, l'Agence doit remettre un rapport au Conseil de sécurité nationale.

TITRE 6 INFRASTRUCTURES D'INFORMATION CRITIQUES

22 Désignation des infrastructures d'informations critiques

1) Le ministre peut, par arrêté, sur recommandation du directeur, après consultation des régulateurs sectoriels et des opérateurs concernés, désigner une infrastructure d'information critique.

2) Le ministre, lorsqu'il procède à une désignation en vertu du paragraphe 1), doit être convaincu que :

   a) le système informatique est nécessaire à la prestation continue d'un service essentiel ;

   b) la perte, la perturbation ou la compromission du système ou du réseau informatique serait susceptible d'avoir un effet délibéré sur la disponibilité, l'intégrité ou la prestation de ce service à Vanuatu ; et

   c) il est situé entièrement ou partiellement à Vanuatu, ou est utilisé pour fournir un service essentiel à Vanuatu.

3) Avant de formuler une recommandation en vertu du paragraphe 1), le directeur doit notifier à l'opérateur son intention de désigner l'infrastructure d'information critique.

4) Une notification en vertu du paragraphe 3) doit informer l'opérateur de ce qui suit :

   a) l'infrastructure d'information critique devant être désignée ;

   b) l'objet de la désignation de l'infrastructure d'information critique ; et

   c) le fait que l'opérateur de l'infrastructure d'information critique dispose de 14 jours ouvrables pour présenter des observations écrites au directeur.

5) Le directeur examine les observations de l'opérateur et doit :

a) soit recommander la désignation de la totalité ou d'une partie spécifiée du système informatique, soit décider de ne pas la recommander ; et

b) notifier par écrit sa décision motivée à l'ensemble des destinataires de l'avis d'intention.

6) Lorsqu'une infrastructure d'information critique est désignée en vertu du présent article, la personne qui la possède ou la contrôle cette en est l'opérateur d'IIC désigné.

7) L'Agence établit et tient à jour un registre pour la désignation des infrastructures d'information critiques.

23 Désignation d'urgence à titre provisoire

1) Afin de protéger la sécurité nationale ou de faire face à un incident cybernétique grave affectant un service essentiel, le directeur peut, par notification écrite, désigner une personne en tant que fournisseur critique à l'égard d'une infrastructure d'information critique.

2) Le directeur, lorsqu'il désigne une personne en tant que fournisseur critique, doit être convaincu que :

a) la personne fournit des biens ou des services à l'opérateur d'IIC ; et

b) l'incident cybernétique grave aura un effet délibéré sur la disponibilité, l'intégrité ou la prestation du service essentiel auquel se rapporte l'infrastructure d'information critique.

3) Un fournisseur critique doit :

a) se conformer à tout code de pratique expressément applicable aux fournisseurs critiques ;

b) signaler au directeur tout incident cybernétique grave affectant les biens ou services fournis ; et

c) notifier à l'opérateur d'IIC et au directeur tout changement important apporté aux biens ou services fournis qui affecte leur sécurité.

24 Désignation des fournisseurs d'informations sur les infrastructures critiques

1) Le ministre peut, par arrêté, sur recommandation du directeur après consultation des régulateurs sectoriels et des opérateurs concernés, désigner un fournisseur d'infrastructures d'information critiques.

2) Le directeur, lorsqu'il formule une recommandation en vertu du paragraphe 1), doit être convaincu que :

a) les biens et services sont nécessaires au fonctionnement ou à la sécurité de l'infrastructure d'information critique ; et

c) un incident cybernétique grave affectant ces biens ou services peut perturber la prestation de services essentiels.

3) Le directeur doit, avant de formuler une recommandation en vertu du paragraphe 1), notifier au fournisseur son intention de le désigner.

4) Une notification en vertu du paragraphe 3) doit informer le fournisseur de ce qui suit :

a) les biens et services d'infrastructure d'information critique devant être désignés ; et

b) l'objet de la désignation du fournisseur d'infrastructure d'information critique.

5) Après examen des observations du fournisseur, le directeur doit soit recommander la désignation de la totalité ou d'une partie déterminée du système informatique, soit décider d'y renoncer. Sa décision motivée est notifiée par écrit à tous les destinataires de la notification d'intention. La possibilité de limiter la désignation à une partie du système permet ainsi de répondre à toute objection relative au champ d'application.

6) Le pouvoir de ne désigner qu'une partie permet de faire face à une objection quant au champ d'application.

TITRE 7 OBLIGATIONS EN MATIÈRE DE CYBERSECURITÉ

25 Obligations des organismes publics et des entités déclarantes

Un organisme public ou une entité déclarante doivent :

a) se conformer au Cadre national de cybersécurité établi par l'Agence ;

b) nommer un point de contact désigné pour la cybersécurité ;

c) réaliser des évaluations annuelles des risques de cybersécurité ;

d) appliquer les contrôles de sécurité de base prescrits par le Code de pratique de la cybersécurité ; et

e) signaler tout incident cybernétique à l'Agence dans les 72 heures suivant sa détection.

26 Obligations des opérateurs d'IIC

Un opérateur d'IIC doit :

a) se conformer aux codes de pratique de la cybersécurité propres à son secteur ;

b) faire réaliser des audits annuels de cybersécurité par un auditeur agréé par l'Agence et lui en soumettre les rapports ;

c) tenir à jour un plan de gestion des risques de cybersécurité ;

d) nommer un responsable de la sécurité des systèmes d'information (RSSI) ou responsable de fonction équivalent ;

e) signaler les incidents cybernétiques graves à l'Agence dans les 6 heures suivant leur détection ;

f) participer aux exercices cybernétiques nationaux ; et

g) notifier l'Agence avant d'apporter des modifications importantes à l'architecture d'une infrastructure d'information.

TITRE 8 APPLICATION DE LA LOI

27 Agent habilité

1) Le directeur peut nommer :

a) un cadre supérieur de l'Agence ; ou

b) toute autre personne,

pour agir en qualité d'agent habilité aux fins de la présente loi.

2) Une personne nommée en application de l'alinéa 1)b) doit remplir les critères suivants :

a) posséder les qualifications, la formation, les connaissances techniques ou l'expérience pertinentes en matière de cybersécurité, de technologies de l'information et de la communication, d'informatique légale, de conformité, d'enquêtes ou d'application de la loi ; et

b) ne pas être un dirigeant, un employé ou un mandataire d'un opérateur d'IIC, d'un fournisseur critique, d'une entité déclarante ou d'une personne fournissant des services de cybersécurité à titre commercial à Vanuatu.

3) Le directeur doit remettre une carte d'identité à la personne nommée en qualité d'agent habilité.

4) La carte d'identité doit être signée par le directeur et comporter une photographie de l'agent habilité ainsi que sa signature.

5) Dans l'exercice des fonctions ou des pouvoirs qui lui sont conférés par la présente loi, l'agent habilité doit présenter sa carte d'identité si la demande lui en est faite.

6) L'agent habilité doit notifier le directeur s'il se trouve en situation de conflit d'intérêts dans l'exercice de ses fonctions ou de ses pouvoirs en vertu de la présente loi.

7) Après en avoir été informé en vertu du paragraphe 6), le directeur doit remplacer l'agent habilité et ne tenir aucun compte de toute décision prise par cet agent habilité.

28 Demande de divulgation des informations et des documents

1) Un agent habilité peut exiger par écrit d'une personne qu'elle divulgue toute information ou tout document s'il est convaincu que cette divulgation est nécessaire à une enquête de cybersécurité.

2) Toute personne doit se conformer à la demande formulée en vertu du paragraphe 1) dans un délai de 14 jours à compter de sa réception.

3) Quiconque manque de se conformer au paragraphe 2) commet une infraction et est passible, sur déclaration de culpabilité, d'une amende n'excédant pas 1 000 000 VT.

29 Pouvoirs d'accès

1) Un agent habilité peut pénétrer :

a) dans tous locaux, à tout moment, avec le consentement de l'occupant des lieux ;

b) dans des locaux commerciaux, pendant ses heures d'ouverture ; ou

c) dans des locaux lorsqu'ils sont ouverts au public.

2) Avant de pénétrer dans des locaux, l'agent habilité doit donner un préavis d'un jour à l'occupant des lieux et solliciter son consentement avant d'y accéder.

3) Après obtention du consentement de l'occupant des locaux en vertu du paragraphe 2), l'agent habilité doit :

a) présenter sa carte d'identité ; et

b) informer l'occupant des locaux :

i) de l'objet de l'accès ;

ii) que tout élément trouvé et saisi pourra être utilisé comme moyen de preuve devant le tribunal ; et

iii) qu'il peut refuser de donner son consentement

4) Lors du déroulement d'une inspection, l'agent habilité doit :

a) éviter tout dommage ou désagrément ;

b) ne pas demeurer sur les lieux plus longtemps qu'il n'est raisonnablement nécessaire ; et

c) laisser les locaux, dans la mesure du possible, dans le même état qu'au moment où il y a pénétré avant l'inspection.

30 Pouvoirs d'accès

1) Dans l'exercice du pouvoir d'accès prévu à l'article 29, un agent habilité peut accomplir tout ou partie des actes suivants :

a) accéder à un système informatique situé sur les lieux, l'inspecter et l'examiner, et faire des copies ou des images des données qui y sont conservées ou qui y sont accessibles ;

b) perquisitionner les locaux et fouiller tout objet s'y trouvant ;

c) inspecter un document ou un enregistrement électronique conservé dans les locaux, en faire des copies ou en prendre des extraits ;

d) prendre des photographies, effectuer des enregistrements vidéo ou dresser des croquis des locaux ou de tout objet s'y trouvant ;

e) saisir tout élément se trouvant dans les locaux que l'agent habilité estime, pour des motifs raisonnables, devoir saisir afin d'en empêcher la dissimulation, la perte, l'altération ou la destruction ;

f) introduire dans les locaux tout équipement ou matériel dont l'agent habilité a raisonnablement besoin pour exercer un pouvoir en vertu de la présente partie ; ou

g) exiger de l'occupant des locaux, ou de toute personne s'y trouvant, qu'il fournisse à l'agent habilité une assistance raisonnable pour l'exercice d'un pouvoir en vertu du présent Titre.

2) Un agent habilité doit obtenir un mandat avant d'entreprendre l'exécution des pouvoirs prévus au paragraphe 1).

3) Quiconque refuse ou omet, sans excuse raisonnable, de se conformer à l'exigence visée à l'alinéa 1)g) commet une infraction et est passible, sur déclaration de culpabilité, d'une amende n'excédant pas 1 000 000 de VT.

31 Récépissé des éléments saisis

1) Immédiatement après avoir saisi un objet auprès d'une personne, l'agent habilité doit lui en remettre un reçu écrit.

2) Si, pour quelque raison que ce soit, il n'est pas possible de se conformer au paragraphe 1), l'agent autorisé doit laisser le reçu écrit bien en évidence dans un endroit visible pour l'occupant des lieux.

32 Restitution des éléments saisis

1) Si un agent habilité saisit un élément, il doit prendre des mesures raisonnables pour le restituer à la personne auprès de qui il a été saisi dès lors que le motif de sa saisie n'existe plus.

2) Si l'élément n'a pas été restitué dans un délai de 14 jours après sa saisie, l'agent habilité doit prendre des mesures raisonnables pour le restituer, à moins que :

   a) des poursuites n'aient été engagées et que ces poursuites ne soient pas terminées ; ou

   b) le tribunal ne rende une ordonnance en vertu du paragraphe 4) prolongeant le délai de 14 jours.

3) Un agent habilité peut, avant l'expiration du délai de 14 jours ou dans un délai prorogé par le tribunal, demander à ce dernier une prolongation de ce délai.

4) Le tribunal peut ordonner une prolongation s'il est convaincu que la rétention de l'élément est nécessaire aux fins d'une enquête visant à déterminer si une infraction a été commise, ou pour permettre d'obtenir des preuves d'une infraction aux fins de poursuites.

5) L'agent habilité doit notifier à la personne concernée toute demande formulée en vertu du paragraphe 3).

33 Assistance de la police aux agents habilités

Un agent habilité peut demander l'assistance d'un agent de police pour prendre toute mesure autorisée par la présente loi.

34 Mandats de perquisition

1) Les personnes suivantes peuvent demander un mandat de perquisition auprès du tribunal :

a) le directeur ; ou

b) un agent habilité, avec l'approbation du directeur.

2) Une demande présentée en vertu du paragraphe 1) peut viser l'obtention d'un mandat autorisant la personne qui y désignée à :

a) pénétrer dans les lieux ; ou

b) perquisitionner les lieux et copier ou emporter tout document, équipement ou matériel s'y trouvant.

3) La demande présentée en vertu du paragraphe 1) peut viser :

a) des lieux appartenant à un opérateur d'infrastructures d'information critiques (IIC), ou se trouvant en sa possession ou sous son contrôle ; ou

b) tout autre lieu où le directeur ou l'agent habilité a des motifs raisonnables de croire que se trouvent des documents utiles à une enquête.

4) Le tribunal peut délivrer un mandat de perquisition s'il a des motifs raisonnables de croire que :

a) il existe un élément particulier (« la preuve ») dans les locaux liés à une infraction à la présente loi ;

b) le fait de ne pas obtenir le mandat de perquisition porterait préjudice à une enquête ; ou

c) il existe une probabilité raisonnable que les documents recherchés se trouvent dans les locaux et puissent être altérés, détruits ou retirés.

5) Si un agent habilité retire un document des locaux en vertu d'un mandat de perquisition, il doit laisser une copie de ce document dans les locaux.

6) Le mandat est valide pour la période qui y est spécifiée, cette période ne pouvant excéder 90 jours.

7) Sous réserve des dispositions du paragraphe 6), la Cour peut accorder la prorogation d'un mandat sur demande présentée avant l'expiration de celui-ci.

8) La demande de prorogation d'un mandat doit :

a) préciser le motif de la prorogation et la durée pour laquelle elle est requise ; et

b) être étayée par toute autre information que le tribunal pourrait juger nécessaire.

9) La Cour peut proroger un mandat s'il est convaincu que les circonstances décrites au paragraphe 4) s'appliquent toujours.

TITRE 9 INFRACTIONS ET PENALITÉS

35 Infractions

1) Quiconque omet de signaler un incident cybernétique dans le délai prescrit en vertu de la présente loi commet une infraction et est passible, sur déclaration de culpabilité :

a) s'il s'agit d'une personne physique : d'une amende n'excédant pas 3 000 000 VT ou d'une peine d'emprisonnement n'excédant pas 3 ans, ou des deux à la fois ; ou

b) s'il s'agit d'une personne morale : d'une amende n'excédant pas 20 000 000 VT.

2) Quiconque ne se conforme pas à une directive du directeur commet une infraction et est passible, sur déclaration de culpabilité :

a) s'il s'agit d'une personne physique : d'une amende n'excédant pas 3 000 000 VT ou d'une peine d'emprisonnement n'excédant pas 3 ans, ou des deux à la fois ; ou

b) s'il s'agit d'une personne morale : d'une amende n'excédant pas 20 000 000 VT.

3) Quiconque ne se conforme pas à une directive du ministre pendant un état d'urgence cybernétique nationale commet une infraction et est passible, sur déclaration de culpabilité :

a) s'il s'agit d'une personne physique : d'une amende n'excédant pas 3 000 000 VT ou d'une peine d'emprisonnement n'excédant pas 3 ans, ou des deux à la fois ; ou

b) s'il s'agit d'une personne morale : d'une amende n'excédant pas 20 000 000 VT.

4) Quiconque contrevient à une disposition de la présente loi commet une infraction et est passible, sur déclaration de culpabilité :

a) s'il s'agit d'une personne physique : d'une amende n'excédant pas 10 000 000 VT ou d'une peine d'emprisonnement n'excédant pas 5 ans, ou des deux à la fois ; ou

b) s’il s'agit d’une personne morale : d’une amende n’excédant pas 20 000 000 VT.

5) Quiconque, de manière téméraire ou négligente, présente en vertu de la présente loi des observations qu'il sait fausses ou trompeuses commet une infraction et est passible, sur déclaration de culpabilité :

a) pour une personne physique : d’une amende n’excédant pas 3 000 000 VT ou d’une peine d’emprisonnement n’excédant pas 3 ans, ou des deux à la fois ; ou

b) pour une personne morale : d’une amende n’excédant pas 20 000 000 VT.

6) Quiconque entrave le directeur ou toute personne habilitée par ce dernier dans l’exercice de l’une quelconque de ses fonctions en vertu de la présente loi commet une infraction et est passible, sur déclaration de culpabilité, d’une amende n’excédant pas 10 000 000 VT ou d’une peine d’emprisonnement n’excédant pas 5 ans, ou des deux à la fois.

7) Quiconque :

a) fournit à un agent habilité des informations qu'il sait fausses ou trompeuses ; ou

b) présente à un agent habilité un document qu'il sait faux ou trompeux,

commet une infraction et est passible, sur déclaration de culpabilité, d’une amende n’excédant pas 10 000 000 VT ou d’une peine d’emprisonnement n’excédant pas 5 ans, ou des deux à la fois.

8) Si une personne, sans excuse raisonnable, entrave ou gêne un agent habilité dans l’exercice de tout pouvoir conféré par la présente loi, elle commet une infraction et est passible, sur déclaration de culpabilité, d’une amende n’excédant pas 10 000 000 VT ou d’une peine d’emprisonnement n’excédant pas 5 ans, ou des deux à la fois.

9) Si une personne usurpe les fonctions d’un agent habilité, elle commet une infraction et est passible, sur déclaration de culpabilité, d’une amende n’excédant pas 10 000 000 VT ou d’une peine d’emprisonnement n’excédant pas 5 ans, ou des deux à la fois.

10) Quiconque entrave intentionnellement une personne dans l'exécution d'un mandat de perquisition délivré en vertu de la présente loi commet une infraction et est passible, sur déclaration de culpabilité, d'une amende n'excédant pas 10 000 000 VT.

36 Avis de pénalité

1) Le directeur peut signifier un avis de pénalité à une personne s'il lui apparaît que celle-ci a commis une infraction à l'une quelconque des dispositions de la présente loi.

2) L'avis de pénalité est un avis informant la personne que si elle ne souhaite pas que l'affaire soit tranchée par un tribunal, elle peut, dans le délai et à la personne spécifiés dans l'avis, payer le montant de la pénalité qui y est indiqué.

3) Un avis de pénalité peut être signifié en personne, par la poste ou par courriel.

4) Si le montant de la pénalité prescrit aux fins du présent article pour une infraction présumée est acquitté en vertu du présent article, aucune autre poursuite ne peut être engagée contre cette personne pour ladite infraction présumée.

5) Le paiement effectué en vertu du présent article n'est pas considéré comme un aveu de responsabilité aux fins de toute procédure civile découlant des mêmes faits, et il ne porte nullement atteinte ni préjudice à une telle procédure.

6) Les règlements peuvent prescrire le montant de la pénalité exigible pour l'infraction si celle-ci est réglée en vertu du présent article.

7) Le montant d'une pénalité prescrit en vertu du présent article pour une infraction ne doit pas excéder le montant maximal de la pénalité prévu par la présente loi.

TITRE 10 DISPOSITIONS DIVERSES

37 Modification de l’annexe

Le ministre peut, par arrêté, sur recommandation du directeur :

a) compléter, modifier ou remplacer l’annexe ; ou

b) supprimer l’un quelconque des services essentiels spécifiés dans l’annexe.

38 Rapport annuel

1) Le directeur doit, dans les 2 mois suivant la fin de chaque année :

   a) fournir au directeur général un rapport sur les activités de l’Agence national pour cette année-là ; et

   b) fournir au directeur général toute information complémentaire que celui-ci pourrait exiger concernant une question contenue dans le rapport.

2) Le directeur général doit inclure le rapport du directeur dans le rapport annuel requis en vertu de la Loi sur la Fonction publique [CAP 246].

39 Immunité

1) Aucune poursuite civile ou pénale ne peut être intentée contre tout membre du personnel de l’Agence, un agent habilité, le directeur ou un membre du Conseil consultatif pour tout acte accompli ou omis de bonne foi dans l’exercice de ses fonctions ou des pouvoirs qui lui sont conférés par la présente loi.

2) Le paragraphe 1) ne s'applique pas s'il est établi qu'un membre du personnel de l'Agence, un agent habilité, le directeur ou un membre du Conseil consultatif a agi de mauvaise foi dans l'exercice de ses fonctions ou de ses pouvoirs en vertu de la présente loi.

40 Règlements

Le ministre peut, sur avis du directeur, prendre des règlements prescrivant les mesures :

a) devant ou pouvant être prescrites en vertu de la présente loi ; ou

b) nécessaires ou utiles à prescrire pour mieux appliquer ou donner effet aux dispositions de la présente loi.

41 Entrée en vigueur

La présente loi entre en vigueur à la date de sa publication au Journal officiel.

ANNEXE

Sont classés comme services essentiels :

a) l'énergie et les services publics ;

b) l'eau et l'assainissement ;

c) les télécommunications et l'infrastructure numérique ;

d) la banque, les paiements et la finance, l'assurance, la gestion de paie et les fonctions comptables de base ;

e) l'aviation ;

f) les activités maritimes et les ports ;

g) le transport terrestre et la logistique ;

h) les soins de santé et les services médicaux ;

i) les services d'urgence et la gestion des catastrophes ;

j) l'administration publique ;

k) la gestion des frontières et la sécurité nationale ;

l) les élections ;

m) la sécurité alimentaire ;

n) l'éducation ; et

o) les tribunaux.