RÉPUBLIQUE DE VANUATU

LOI N°22 DE 2021 SUR LA CYBERCRIMINALITE

Sommaire

Sous-titre 3 Données relatives aux abonnés, données relatives au traficet données relatives au contenu

Sous-titre 4 Divulgation à un organisme étranger chargé del'application de la loi

Sous-titre 5 Mandat d'interception

Sous-titre 6 Dispositions relatives aux mandats informatiques

RÉPUBLIQUE DE VANUATU

Promulguée : **20/07/2021**
Entrée en vigueur : **22/09/2021**

LOI N° DE 2021 SUR LA CYBERCRIMINALITÉ

Loi prévoyant la réglementation de l'utilisation des systèmes, programmes etdonnées informatiques et les questions connexes.

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

TITRE 1 DISPOSITIONS PRÉLIMINAIRES

1 Définitions

Dans la présente Loi, sous réserve du contexte :

agent autorisé désigne un agent de police nommé en tant que tel en vertu de l'article 69 ;

agent de police désigne tout membre du Corps de Police de Vanuatu établi par la Loi sur la Police [CAP 105] ;

Commissaire désigne le Commissaire de police nommé en vertu de la Loi sur la Police [CAP 105] ;

communication désigne le transfert de signes, de signaux, d'écrits, d'images, de sons, de données ou de renseignements de toute nature transmis en tout ou en partie par des moyens électroniques ;

Cour signifie la Cour Suprême de Vanuatu ;

délit grave a la même signification que dans la Loi sur les Produits d'activité criminelle [CAP 284] ;

délit grave étranger a la même signification que dans la Loi sur les Produits d'activité criminelle [CAP 284] ;

dispositif désigne tout matériel ou équipement qui remplit une ou plusieurs fonctions spécifiques et fonctionne avec toute forme ou combinaison d'énergie électrique et comprend, sans s'y limiter, les éléments suivants :

a) les composants de systèmes informatiques tels que les ordinateurs, les cartes graphiques, les téléphones mobiles ou les puces à mémoire ; ou

b) des éléments de stockage tels que les disques durs, les cartes mémoire, les disques compacts ou les bandes ; ou

c) des dispositifs de saisie tels que des claviers, des souris, des pavés tactiles, des scanners ou des appareils photo numériques ; ou

d) les appareils de sortie tels que les imprimantes ou les écrans ;

dispositif d'interception a la même signification que dans la Loi N°37 de 2017 sur les Pouvoirs de la Police ;

données désigne toute représentation de faits, de concepts ou d'informations sous une forme qui se prête au traitement dans un système informatique, y compris un programme permettant à un système informatique d'exécuter une fonction ;

données d'abonné :

a) désigne toute donnée détenue par un prestataire de services (sous forme de données informatiques ou sous toute autre forme) concernant une personne utilisant ou louant ses services (un « abonné ») et permettant d'établir ce qui suit :

i) le type de service utilisé, les dispositions techniques prises en relation avec le service et la période de service ;

ii) l'identité de l'abonné, son adresse postale ou géographique, son numéro de téléphone et autre numéro d'accès, ainsi que les informations relatives à la facturation et au paiement, disponibles sur la base du contrat ou de l'accord de service ;et

iii) tout autre donnée sur le site d'installation de l'équipement nécessaire à l'utilisation du service, disponible sur la base du contrat ou de l'accord de service ; et

b) ne comprend pas les données relatives au trafic ou au contenu ;

données du contenu désigne la substance d'une communication spécifique qui est interceptée ;

données informatiques comprennent :

a) les données introduites ou copiées dans un système informatique;

b) les données conservées sur un support de stockage amovible dans un système informatique ;

c) les données conservées sur un support informatique sur un réseau informatique dont le système informatique fait partie ; et

d) les données conservées sur d'autres supports de stockage informatique, y compris « cloud » ;

e) toute représentation d'informations, de connaissances, de faits, de concepts ou d'instructions, qui est en cours d'élaboration ou a été élaborée et qui est destinée à être traitée, est en cours d'élaboration ou a été traitée dans un ordinateur ou un réseau informatique

f) toute forme, qu'elle soit lisible uniquement par un ordinateur ou uniquement par un être humain ou par l'un ou l'autre, y compris, mais sans s'y limiter, les imprimés d'ordinateur, les supports de stockage magnétiques, les cartes perforées ou stockées à l'intérieur de la mémoire de l'ordinateur ;

données relatives au trafic signifient les données électroniques qui :

a) se rapportent à une communication au moyen d'un système informatique ;

b) est généré par un système informatique qui fait partie de la chaîne de communication ; et

c) indique l'origine, la destination, l'itinéraire, l'heure, la date, la taille,la durée ou le type de services sous-jacents de la communication ;

enfant désigne une personne âgée de moins de 18 ans ;

en temps réel signifie lorsque des informations sont générées ou transmises ;

information signifie l'information, qu'elle se présente sous forme de données, de texte, de sons, d'images ou sous toute autre forme ;

infraction spécifiée signifie une infraction à une loi de Vanuatu pour laquelle la peine maximale est un emprisonnement d'au moins 4 ans ;

interception signifie la surveillance ou l'enregistrement de transmissions non publiques de données à destination, en provenance ou à l'intérieur d'un système informatique ;

Loi sur l'Assistance réciproque en matière d'affaires criminelles désigne la Loi sur l'Assistance réciproque en matière d'affaires criminelles [CAP 285] ;

mandat informatique désigne un mandat accordé en vertu de l'article 40 ;

mandat d'interception désigne un mandat autorisé en vertu de l'article 30 ;

mettre à disposition signifie, sans s'y limiter, la description de la manière d'obtenirl'accès, ou la description des méthodes susceptibles de faciliter l'accès ;

Ministre désigne le ministre responsable des technologies de l'information et de la communication ;

mandat informatique urgent désigne un mandat délivré en vertu de l'article 43 ;

mandat d'interception urgent désigne un mandat délivré en vertu de l'article 30.

pays étranger a la même signification que dans la Loi sur l'Assistance réciproque en matière d'affaires criminelles[CAP 285] ;

prestataire de services désigne :

a) une entité publique ou privée qui fournit aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ;

b) toute autre entité qui traite ou stocke des données informatiques pour le compte de cette entité ou de ces utilisateurs ;

c) un prestataire de services au sens de la Loi N°30 de 2009 relative à la Règlementation des télécommunications et des radiocommunications ;

programme désigne les données représentant des instructions ou des déclarations qui, lorsqu'elles sont exécutées dans un système informatique, font en sorte que le système informatique exécute une fonction et les références à un programme comprennent les références à une partie d'un programme ;

représentant autorisé signifie :

a) le directeur général ou le directeur exécutif d'un prestataire de services ou d'une personne morale dont le prestataire de services estune filiale ; ou

b) le secrétaire d'un prestataire de services ou d'une personne morale dont le prestataire de services est une filiale ; ou

c) un employé autorisé, par écrit, par le directeur général ou le secrétaired'un prestataire de services ou d'une personne morale dont le prestataire de services est une filiale ;

réseau informatique désigne tout système qui assure la communication entre un ou plusieurs systèmes informatiques et ses périphériques d'entrée ou de sortie, y compris, mais sans s'y limiter, les terminaux d'affichage et les imprimantes qui sont reliés par des installations de télécommunication ;

sortie intelligible est une information provenant d'un système informatique, sous quelque forme que ce soit, qui peut être lue et comprise.

support de stockage informatique signifie tout article ou matériel à partir duquell'information peut être reproduite, avec ou sans l'aide d'un autre article ou dispositif.

système informatique désigne :

a) un ordinateur ; ou

b) deux ou plusieurs ordinateurs interconnectés ; ou

c) toute liaison de communication entre ordinateurs ou avec des terminaux distants ou un autre dispositif,

qui comprend également toute partie des éléments décrits aux points a) à d) et tous les intrants, extrants, traitements, stockage, logiciels ou installations de communication, « cloud » et les données stockées qui y sont liés ;

2 Objet

La présente Loi a pour objet :

a) de protéger la confidentialité, l'intégrité et la disponibilité des systèmes, programmes et données informatiques ;

b) d'empêcher l'utilisation abusive des systèmes, programmes et données informatiques ; et

c) de permettre la collecte de matériel médico-légal pour l'enquête et la poursuite des infractions à la présente Loi ; et

d) de faciliter la coopération internationale.

TITRE 2 INFRACTIONS INFORMATIQUES

3 Accès illégal

1) Aux fins de l'application du présent article, on entend par **infrastructures critiques** les systèmes informatiques, les installations physiques, les processus, les chaînes d'approvisionnement, les technologies de l'information, les réseaux de communication, les dispositifs, les services publics et les services essentiels.

2) Toute personne qui, intentionnellement et sans excuse légitime, accède à tout ou partie d'un système informatique en enfreignant une mesure de sécurité, commet une infraction qui l'expose sur condamnation :

   a) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 2 000 000VT ou d'emprisonnement n'excédant pas5 ans, ou les deux à la fois ;

   b) dans le cas d'une personne morale, à une peine d'amende n'excédant pas 4 000 000 VT.

3) Toute personne qui, intentionnellement ou sans excuse légitime, accède à tout ou partie d'une infrastructure critique, commet une infraction qui l'expose sur condamnation :

   a) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 2 000 000 VT ou d'emprisonnement n'excédant pas5 ans, ou les deux à la fois ;

   b) dans le cas d'une personne morale, à une peine d'amende n'excédant pas 4 000 000 VT.

4) Une personne ne commet pas d'infraction au titre du présent article si :

   a) elle est autorisée à avoir accès au programme ou aux données ; ou

   b) elle a consenti à avoir accès au programme ou aux données.

4 Interception illégale

1) Une personne ne doit pas, intentionnellement et sans excuse légitime, intercepter par un moyen technique quelconque :

   a) toute transmission non publique de données informatiques à destination, en provenance ou à l'intérieur d'un système informatique ; ou

   b) l'émission électromagnétique d'un système informatique

transportant de telles données informatiques.

2) Nonobstant le paragraphe 1), le Commissaire de Police peut, par ordonnance, autoriserl'interception de toute transmission non publique ou de toute émission électromagnétique.

3) Toute personne qui, intentionnellement et sans excuse légitime, intercepte à tout ou partie d'une infrastructure critique, commet une infraction qui l'expose sur condamnation :

a) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 2 000 000 VT ou d'emprisonnement n'excédant pas5 ans, ou les deux à la fois ;

b) dans le cas d'une personne morale, à une peine d'amende n'excédant pas 4 000 000 VT.

5 Interférences non autorisées

1) Aux fins du présent article, on entend par intervention non autorisée :

a) une personne dont l'acte cause l'interférence et qui n'est pas habilitée à déterminer si l'interférence doit être faite ;

b) une personne qui n'a pas le consentement d'une personne ayant droit à l'intervention.

2) Toute personne qui, intentionnellement et sans autorisation, accomplit un acte qui provoque une interférence non autorisée avec un système, un programme ou des données informatiques commet une infraction qui l'expose sur condamnation :

a) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 7 000 000 VT ou d'emprisonnement n'excédant pas40 ans, ou les deux à la fois ; ou

b) dans le cas d'une personne morale, à une peine d'amenden'excédant pas 100 000 000 VT.

3) Toute personne qui provoque une interférence non autorisée entraînant un préjudice grave dans l'un ou plusieurs domaines suivants :

a) perte financière de plus de 1 000 000 VT;

b) menace la sécurité nationale ;

c) cause un préjudice physique ou la mort d'une personne ;

d) menace la santé ou la sécurité publique ; commet une infraction qui l'expose sur

condamnation :

a) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 50 000 000 VT ou d'emprisonnement n'excédant pas 50 ans, ou les deux à la fois ; ou

b) dans le cas d'une personne morale, à une peine d'amende n'excédant pas 100 000 000 VT.

4) Toute personne qui provoque de manière imprudente une interférence non autorisée commet une infraction qui l'expose sur condamnation :

a) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 10 000 000 VT ou d'emprisonnement n'excédant pas 40 ans, ou les deux à la fois ; ou

b) dans le cas d'une personne morale, à une peine d'amende n'excédant pas 100 000 000 VT.

5) Aux fins du présent article, il est indifférent que l'intervention non autorisée ne soit pas dirigée contre :

a) un système informatique, un programme ou des données en particulier ;

b) un programme ou des données de quelque nature que ce soit ; ou

c) un programme ou des données détenus dans un système informatique particulier.

6) Outre le paragraphe 5), il est indifférent qu'une intervention non autorisée ou tout effet prévu de celle-ci soit permanent ou temporaire.

6 Utilisation abusive de dispositifs

1) Toute personne qui, intentionnellement ou sans excuse légitime, produit, vend, se procure pour utilisation, importe, exporte, distribue ou met à disposition de toute autre manière :

a) un logiciel, un système informatique ou un dispositif électronique ; ou

b) un mot de passe, un code d'accès ou des données similaires permettant d'accéder à tout ou partie d'un système informatique ou de données électroniques ;

pour intercepter ou provoquer une interférence non autorisée, comme une infraction qui l'expose sur condamnation :

a) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 1 000 000 VT ou d'emprisonnement n'excédant pas 3 ans, ou les deux à la fois ; ou

b) dans le cas d'une personne morale, à une peine d'amenden'excédant pas 3 000 000 VT.

2) Nonobstant le paragraphe 1), ne constitue pas une infraction au titre du présent article :

a) tout acte visant à former, tester ou protéger un systèmeinformatique de manière autorisée; ou

b) tout acte entrepris, conforme à une ordonnance de la Cour émisedans l'exercice de tout pouvoir en vertu de la présente Loi ou detoute autre loi.

TITRE 3 DÉLITS INFORMATIQUES

7 Pornographie infantile

1) Aux fins du présent article, **la pornographie infantile (ou pédopornographie)** comprend tout matériel, sans s'y limiter, audio, visuelou textuel qui représente :

   a) un enfant se livrant à un comportement sexuellement explicite ;

   b) une personne apparaissant comme un enfant se livrant à un comportement sexuellement explicite ; ou

   c) des images, des animations ou des vidéos représentant un enfant se livrant à un comportement sexuellement explicite.

2) Toute personne qui, intentionnellement ou sans excuse légitime :

   a) produit de la pornographie infantile en vue de sa diffusion par le biais d'un système informatique ;

   b) offre ou sollicite ou rend disponible de la pornographie infantile par le biais d'un système informatique ;

   c) distribue ou transmet de la pornographie infantile par le biais d'un système informatique ;

   d) obtient ou sollicite de la pédopornographie par le biais d'un système informatique pour son usage personnel ou pour celui d'uneautre personne ; ou

   e) possède de la pornographie infantile dans un système informatique ou sur un support de stockage électronique ;

   commet une infraction qui l'expose sur condamnation :

      a) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 5 000 000 VT ou d'emprisonnement n'excédant pas10 ans, ou les deux à la fois ; ou

      b) dans le cas d'une personne morale, à une peine d'amenden'excédant pas 15 000 000 VT.

8 Hébergement de pédopornographie

1) Une personne commet une infraction si :

   a) elle est un prestataire de service ; e

   b) elle sait ou prend conscience que le service fourni par une personne peut être utilisé pour accéder à un matériel particulier par rapport auquel elle a des motifs

raisonnables de croire :

i) qu'il s'agit d'un matériel pédopornographique; et

ii) qu'il ne communique pas les détails du matériel aux forces de Police de Vanuatu dans un délai raisonnable après avoir pris connaissance de l'existence du matériel,

2) Une personne qui commet une infraction en vertu du paragraphe 1) s'expose sur condamnation :

a) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 5 000 000 VT ou d'emprisonnement n'excédant pas10 ans, ou les deux à la fois ; ou

b) dans le cas d'une personne morale, à une peine d'amenden'excédant pas 10 000 000 VT.

9 Délit lié à l'identité

Toute personne qui, intentionnellement ou sans excuse légitime, utilise un système informatique pour :

a) transférer ;

b) posséder ; ou

c) utiliser,

l'identification d'une autre personne dans l'intention de commettre une activité illégale, de l'aide, de l'encourager ou de la relier à une activité illégale, commetune infraction qui l'expose sur condamnation :

i) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 3 000 000 VT ou d'emprisonnement n'excédant pas 3 ans, ou les deux à la fois ;

ii) dans le cas d'une personne morale, à une peine d'amenden'excédant pas 5 000 000 VT.

10 Cyberharcèlement

1) Aux fins du présent article, cyberharcèlement signifie un acte visant à contraindre, intimider, harceler, insulter ou ennuyer une personne au moyen de systèmes informatiques ou de dispositifs électroniques.

2) Toute personne qui, directement ou indirectement, utilise une communication électronique à des fins de cyberharcèlement commet une infraction qui l'expose sur condamnation :

a) dans le cas d'une personne physique, à un peine d'amende n'excédant pas 1 000 000 VT ou d'emprisonnement n'excédant pas3 ans, ou les deux à la fois ;

b) dans le cas d'une personne morale, à une peine d'amenden'excédant pas 3 000 000 VT.

11 Sollicitation d'enfants

Toute personne qui utilise un système informatique :

a) pour proposer à un enfant ; ou

b) proposer à une personne qu'elle croit être un enfant,

de la rencontrer ou de rencontrer une autre personne dans l'intention de l'exploiter sexuellement, que cette proposition ait été suivie ou non d'actes matériels, commet une infraction qui l'expose sur condamnation à une peine d'amende n'excédant pas 2 000 000 VT ou d'emprisonnement n'excédant pas 5 ans, ou les deux à la fois.

12 Falsification informatique

Toute personne qui, intentionnellement ou sans excuse légitime, produit des données non authentiques dans l'intention de les considérer ou d'y donner suite à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles ou intelligibles, et qui, à tort :

a) obtient ;

b) introduit ;

c) modifie ;

d) supprime ; ou

e) dissimule,

des données électroniques, commet une infraction qui l'expose sur condamnation :

i) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 5 000 000 VT ou d'emprisonnement n'excédant pas12 ans ou les deux à la fois ;

ii) dans le cas d'une personne morale, à une peine d'amende n'excédant pas 10 000 000 VT.

13 Fraude informatique

Toute personne qui, intentionnellement ou sans excuse légitime, cause une perte de biens à

une autre personne par :

a) l'introduction, l'altération, la suppression ou la dissimulation de données ;ou

b) toute interférence avec le fonctionnement d'un système informatique,

dans l'intention frauduleuse de procurer un gain personnel à une autre personne,commet une infraction qui l'expose sur condamnation :

i) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 5 000 000 VT ou d'emprisonnement n'excédant pas12 ans, ou les deux à la fois ;

ii) dans le cas d'une personne morale, à une peine d'amenden'excédant pas 10 000 000 VT.

14 Accès illégal avec intention de commettre ou de faciliter d'autresinfractions

1) Une personne est coupable d'une infraction au titre du présent article si elle commet une infraction en vertu de l'article 3 avec l'intention de :

a) commettre une infraction à laquelle le présent article s'applique ;ou

b) faciliter la perpétration d'une telle infraction (que ce soit parl'auteur de l'infraction ou par toute autre personne),

et l'infraction que la personne a l'intention de commettre ou d'en faciliterla perpétration est une nouvelle infraction.

2) Il est indifférent, aux fins du présent article, que la nouvelle infraction soitcommise en même temps que l'infraction d'accès non autorisé ou à une date ultérieure.

3) Une personne peut être accusée d'une infraction au titre du présent articlemême si les faits sont tels que la perpétration de la nouvelle infraction estimpossible.

4) Toute personne qui accède intentionnellement, sans excuse légitime, à tout ou partie d'un système informatique et commet ou facilite la perpétration d'une nouvelle infraction, s'expose sur condamnation :

a) dans le cas d'une personne physique, à un peine d'amende n'excédant pas 7 000 000 VT ou d'emprisonnement n'excédant pas7 ans, ou les deux à la fois ; ou

b) dans le cas d'une personne morale, à une peine d'amenden'excédant pas 9 000 000 VT.

TITRE 4 PROCÉDURES

Sous-titre 1 Divulgation d'informations, assistance et la production de données informatiques

15 Divulgation d'informations relatives à une enquête

1) Aux fins du présent article, un prestataire de services comprend tout ou partie des employés, agents et sous-traitants du prestataire de services.

2) Un prestataire de services qui reçoit une ordonnance d'un tribunal, relative à une enquête pénale, qui prévoit que la confidentialité doit être maintenue ou que cette obligation est prévue par la loi et que le prestataire de servicesdivulgue ou continue de divulguer :

a) le fait qu'une ordonnance a été rendue ; ou

b) tout ce qui est fait en vertu de l'ordonnance ; ou

c) toute donnée recueillie ou enregistrée en vertu de l'ordonnance, commet une infraction qui l'expose sur condamnation :

i. dans le cas d'un particulier – à une peine d'amende n'excédant pas 2 000 000 VT ou d'emprisonnement n'excédant pas 5 ans, ou les deux à la fois ; ou

ii. dans le cas d'une personne morale – à une peine d'amenden'excédant pas 5 000 000 VT.

16 Assistance

Une personne qui n'est pas suspectée d'un crime en vertu de la présente Loi, mais qui possède ou contrôle un dispositif ou des données faisant l'objet d'un mandat informatique en vertu du Sous-titre 6, doit, à ses propres frais, autoriser ou aider un agent autorisé à effectuer la perquisition et :

a) accéder et utiliser l'appareil ou les données ;

b) obtenir une copie de ces données ;

c) utiliser l'appareil pour faire des copies ; et

d) obtenir une sortie intelligible d'un appareil dans un format lisible.

17 Production de données informatiques

1) Le présent article s'applique si un agent de police demande à un tribunal que des données contenues dans un support de stockage de données, un réseau d'ordinateurs ou un système informatique, ou un imprimé ou toute autre information, soit raisonnablement nécessaire pour une enquête ou une procédure pénale impliquant une infraction spécifiée aux lois de Vanuatu ou une infraction grave aux lois d'un pays étranger.

2) Le tribunal peut ordonner :

a) qu'une personne ayant le contrôle du support de stockage des données, du réseau d'ordinateurs ou du système informatique produise d'une manière précisée dans l'ordonnance des données spécifiques ou une impression ou toute sortie intelligible de ces données ; et

b) une personne qui a accès à un processus informatique spécifié pour compiler les données détenues dans le système et les donner à une personne spécifiée.

3) Avant de rendre une ordonnance en vertu du paragraphe 2), la Cour doit prendre en considération les éléments suivants :

a) la gravité de l'infraction sur laquelle porte l'enquête ou la procédure pénale ;

b) la fiabilité des informations sur lesquelles la demande est fondée, y compris la nature de la source des informations ;

c) si l'intérêt public dans la production de données à partir du système informatique ou du support de stockage de données l'emporte sur le droit à la vie privée d'une personne dont la vie peut être affectée du fait de la production ;

d) s'il existe un lien suffisant entre les preuves recherchées et l'infraction à laquelle se rapporte l'enquête ou la procédure pénale ;

e) si une condition doit être incluse dans l'ordonnance ; et

f) toute autre question que la Cour juge pertinente.

Sous-titre 2 Ordonnance de conservation

18 Ordonnance de conservation

1) Le Commissaire peut, aux fins de conserver des données informatiques, y compris les données relatives au trafic ou au contenu, en possession ou sous le contrôle d'une personne, demander au tribunal une ordonnance de conservation.

2) La Cour peut accorder une ordonnance de conservation si elle est convaincue, pour

des motifs raisonnables, que la conservation des données informatiques est raisonnablement nécessaire à des fins répressives ou pour une enquête ou une procédure pénale portant sur une infraction graveà la législation d'un pays étranger.

3) Une ordonnance de conservation :

a) entre en vigueur lorsque le prestataire de services la reçoit ; et

b) reste en vigueur pendant la période indiquée dans l'ordonnance de conservation ou jusqu'à sa révocation par la Cour en vertu de l'article 19.

4) Une ordonnance de conservation ne doit pas rester en vigueur pendant une période de plus de 90 jours.

5) Nonobstant le paragraphe 4), si la Cour est convaincue qu'il faut plus de temps pour obtenir ce qui est requis par l'ordonnance de conservation, il peut prolonger la période pendant laquelle l'ordonnance de conservation est en vigueur, pour 90 jours supplémentaires.

6) La personne à qui une ordonnance de conservation a été délivrée doit garder l'ordonnance et toutes les informations la concernant confidentielles.

7) Une personne qui, sans excuse raisonnable, :

a) ne respecte pas une ordonnance émise en vertu du paragraphe 2) ;

b) ne garde pas confidentielles toutes les informations relatives à l'ordonnance conformément au paragraphe 6)

commet une infraction qui l'expose sur condamnation :

i) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 1 000 000 VT ou d'emprisonnement n'excédant pas 3 ans ou les deux à la fois ; ou

ii) dans le cas d'une personne morale, à une peine d'amende n'excédant pas 2 000 000 VT.

19 Révocation de l'ordonnance de conservation

1) Si la Cour estime pour des motifs raisonnables que l'ordonnance de conservation n'est plus nécessaire, elle doit révoquer l'ordonnance de conservation à tout moment avant expiration.

2) Si une ordonnance de conservation est révoquée, un agent de police doit en informer immédiatement le représentant autorisé du prestataire de services et lui remettre une copie de la révocation.

20 Prestataire de service ou agent autorisé à divulguer des données relatives au trafic

Un prestataire de service ou son agent autorisé faisant l'objet d'une ordonnance de conservation doit divulguer, dès que possible, une quantité suffisante de données relatives au trafic pour permettre à un agent de police d'identifier tout autre prestataire de service impliqué dans la transmission de la communication.

Sous-titre 3 Données relatives aux abonnés, données relatives au traficet données relatives au contenu

21 Demande de divulgation des données relatives aux abonnés

1) Le Commissaire peut, par écrit, demander à un prestataire de services de divulguer les données relatives aux abonnés s'il est convaincu que cette divulgation est nécessaire :

   a) à des fins répressives; ou

   b) pour l'exécution d'une infraction étrangère grave en vertu de la Loi sur l'Assistance réciproque en matière d'affaires criminelles.

2) Le prestataire de services doit se conformer à la demande visée au paragraphe 1) dès que possible après l'avoir reçue.

3) Le prestataire de services qui ne se conforme pas au paragraphe 2) commet une infraction qui l'expose sur condamnation à une peine d'amende n'excédant pas 1 000 000 VT.

22 Demande de divulgation de données relatives au trafic

1) Le Commissaire peut, par écrit, demander à un prestataire de services de divulguer des enregistrements de données relatives au trafic qui ont été créés avant le moment où la divulgation est demandée, si cette divulgationest raisonnablement nécessaire :

a) à des fins d'application de la Loi ; ou

b) pour l'exécution d'une infraction grave commise à l'étranger en vertu de la Loi sur l'Assistance réciproque en matière d'affairescriminelle.

2) Avant de présenter une demande au titre du paragraphe 1), le Commissairedoit :

a) être convaincu que l'intérêt public, lors de la divulgation des données, l'emporte largement sur le droit à la vie privée d'une personne dont la vie privée peut être affectée par la divulgation ; et

b) examiner toute question pertinente pour donner l'approbation, notamment les suivantes :

i) le volume et la nature des données à divulguer ;

ii) la gravité de la conduite faisant l'objet de l'enquête ;

iii) l'utilité probable des données pour l'enquête ; et

iv) la finalité pour laquelle l'accès aux données est demandé.

3) Le prestataire de services doit répondre à la demande visée au paragraphe 1) dès que possible après l'avoir reçue.

4) Le prestataire de services qui ne se conforme pas au paragraphe 3) commet une infraction qui l'expose sur condamnation à une peine d'amende n'excédant pas 2 000 000 VT.

23 Demande d'accès aux données relatives au trafic en temps réel

1) Le Commissaire peut, par écrit, demander à un fournisseur de services de donner accès aux enregistrements de données relatives au trafic en temps réel pendant une période maximale de 90 jours si cet accès est raisonnablement nécessaire pour :

a) l'exécution d'une infraction punie, sur condamnation, d'une peine d'emprisonnement d'au moins 2 ans en vertu de la présente Loi oude toute autre loi ; ou

b) pour l'exécution d'une infraction grave commise à l'étranger en vertu de la Loi sur l'Assistance réciproque en matière d'affairescriminelles.

2) Avant de présenter une demande au titre du paragraphe 1), le Commissairedoit :

a) être convaincu que l'intérêt public à accéder aux documents l'emporte largement sur le droit à la vie privée d'une personne dontla vie privée peut être affectée par l'accès ; et

b) examiner toute question pertinente pour donner l'approbation, notamment les suivantes :

i) le volume et la nature des documents à divulguer ;

ii) la gravité du comportement faisant l'objet de l'enquête;

iii) l'utilité probable des documents pour l'enquête ; ou

iv) la raison pour laquelle l'accès aux documents est demandé.

3) Le Commissaire doit, par écrit, annuler une demande au titre du paragraphe 1) à tout moment avant qu'elle ne prenne fin, s'il est convaincu que la demande n'est plus

nécessaire.

4) Le Commissaire doit, par écrit, informer le prestataire de services ou son représentant autorisé de l'annulation en vertu du paragraphe 3) et lui fournir une copie de l'annulation, immédiatement après l'annulation de lademande.

24 Divulgation des données relatives au contenu

1) Un agent autorisé peut demander à la Cour d'ordonner l'accès aux donnéesrelatives au contenu et leur divulgation comme suit :

a) une personne ayant participé ou soupçonnée pour des motifs raisonnables d'avoir participé à la perpétration de :

i) une infraction spécifique ; ou

ii) une infraction étrangère grave en vertu de la Loi sur l'Assistance réciproque en matière d'affaires criminelles, et

b) un service qui a été utilisé, est utilisé ou est susceptible d'être utilisé par une personne en vertu du paragraphe a).

2) L'agent habilité à présenter une demande au titre du paragraphe 1) doit indiquer dans sa demande :

a) les détails de chaque service fourni sous réserve de l'ordonnance ;et

b) l'infraction ou les infractions auxquelles la demande se rapporte ; et

c) les informations et les preuves invoquées ; et

d) si une ordonnance de conservation a été délivrée.

3) L'agent habilité doit fournir toute information supplémentaire que la Cour requiert concernant les motifs pour lesquels l'ordonnance est demandée.

25 Les données relatives aux abonnés, au trafic et au contenu ne doivent être utilisées qu'à des fins licites

1) Les données relatives aux abonnés obtenues en vertu de l'article 21 doivent être utilisées :

a) aux fins pour lesquelles elles ont été obtenues à l'origine ;

b) pour faire respecter la loi pénale, une loi imposant une sanction pécuniaire ou pour protéger les recettes publiques ; ou

c) pour exécuter une ordonnance étrangère de confiscation ou une ordonnance étrangère de sanction pécuniaire en rapport avec une infraction grave commise à l'étranger en vertu de la Loi sur l'Assistance réciproque en matière d'affaires criminelles.

2) Les données relatives au trafic obtenues en temps réel doivent être utilisées :

a) aux fins pour lesquelles elles ont été obtenues à l'origine ;

b) pour faire respecter la loi pénale, une loi imposant une sanction pécuniaire ou pour protéger les recettes publiques ; ou

c) pour exécuter une infraction grave commise à l'étranger conformément à une autorisation délivrée en vertu de la Loi sur l'Assistance réciproque en matière d'affaires criminelles.

3) Les données relatives au contenu conservées conformément à l'article 18 sont utilisées :

a) aux fins pour lesquelles les données relatives au contenu ont été obtenues à l'origine ; ou

b) pour faire respecter une infraction spécifiée ou une infraction prévue par la présente partie ; ou

c) pour exécuter une infraction grave commise à l'étranger conformément à une autorisation délivrée en vertu de la Loi sur l'Assistance réciproque en matière d'affaires criminelles.

4) Si le Commissaire est convaincu que les informations obtenues ne sont plus nécessaires, il doit faire en sorte que la destruction des données et toute reproduction des données soient placées sous le contrôle des Forces de Police de Vanuatu.

Sous-titre 4 Divulgation à un organisme étranger chargé de l'application de la loi

26 Divulgation à un service répressif étranger

1) Les renseignements obtenus en vertu de la présente partie ne doivent pas être communiqués à un organisme étranger chargé de l'application de la loi, sauf si la communication a été autorisée par le Commissaire.

2) Le Commissaire ne doit pas autoriser une divulgation en vertu de la présente partie à moins qu'il ne soit convaincu que :

a) que la communication est raisonnablement nécessaire pour l'exécution d'un délit grave à l'étranger ; et

b) est appropriée en toutes circonstances.

Sous-titre 5 Mandat d'interception

27 Le Commissaire autorise les demandes

1) Le Commissaire peut autoriser une demande de :

a) un mandat d'interception ;

b) le renouvellement d'un mandat d'interception ; ou

c) un mandat d'interception urgent.

2) Le Commissaire ne peut autoriser la demande visée au paragraphe 1) que s'il est convaincu qu'il existe des motifs raisonnables de soupçonner qu'unepersonne :

a) planifie une infraction spécifiée, y participe ou la commet ; ou

b) a planifié, participé ou commis une infraction spécifiée.

28 Demande de mandat d'interception

1) Si le Commissaire a autorisé une demande de mandat d'interception envertu de l'article 27, un agent de police doit demander au tribunal de délivrer le mandat d'interception pour :

a) intercepter une communication privée au moyen d'un dispositifd'interception ; ou

b) enregistrer visuellement ou observer une activité d'une personne au moyen d'un dispositif d'interception ; ou

c) utiliser à la fois un dispositif d'interception et un dispositif desurveillance optique.

2) La demande doit être faite par écrit et sous serment par un officier de police, et doit indiquer :

a) la personne ou le client, s'il est connu, dont la communication doitêtre interceptée ; et

b) le prestataire de services auquel doit être adressée la directive d'intercepter la communication, le cas échéant ; et

c) les faits invoqués pour démontrer qu'il existe des motifs raisonnables de soupçonner qu'une personne prépare ou commetune infraction spécifiée, ou a préparé ou commis une telle infraction, ou y a participé ; et

d) une description de la manière dont il est proposé d'intercepter des communications privées ou d'enregistrer ou d'observer des activités

; et

e) la mesure dans laquelle d'autres méthodes d'enquête sur l'infraction, autres qu'un mandat d'interception, ont été utilisées parl'agent de police ou sont à sa disposition ; et

f) soit :

i) le nom et l'adresse, s'ils sont connus, de la personne dont les communications privées ou un enregistrement ou des observations sur les activités qu'il y a des motifs raisonnables de soupçonner aideront l'enquête de police sur l'affaire ; ou

ii) si le nom et l'adresse du suspect ne sont pas connus, une description générale des locaux, du lieu, de la chose ou du type d'installation pour lesquels il est proposé d'intercepter des communications privées ou d'enregistrer ou d'observer des activités ; et

g) la période pour laquelle un mandat est demandé.

3) Aux fins du présent article, dispositif de surveillance optique a la même signification que dans la Loi N°37 de 2017 sur les Pouvoirs de la police.

29 Contenu et conditions d'un mandat d'interception

1) Le mandat d'interception doit être établi selon la forme prescrite et contenir les informations suivantes :

a) l'infraction ou les infractions pour lesquelles le mandat est accordé

; et

b) si le mandat porte sur l'utilisation d'un dispositif d'interception dans les locaux :

i) le nom et l'adresse du suspect dont les communications privées peuvent être interceptées ou dont les activités peuvent être enregistrées ou observées ; ou

ii) si le nom et l'adresse du suspect ne sont pas connus, une description générale des locaux, du lieu, de la chose ou du type d'installation pour lesquels les communications privéesseront interceptées ou les activités enregistrées ou observées ; et

c) si le mandat autorise l'utilisation d'un dispositif d'interception en ce qui concerne les conversations, les activités ou le lieu où se trouve une personne, indiquer le nom de la personne (s'il est connu) ou le fait que son identité est inconnue ; et

d) toute autre condition que la Cour estime nécessaire pour desraisons d'intérêt public.

2) Un mandat d'interception a pour effet, selon ses termes, d'autoriser

a) l'interception de communications privées au moyen d'un dispositifd'interception ; ou

b) l'enregistrement visuel ou l'observation d'une activité d'une personne au moyen d'un dispositif d'interception ; ou

c) les activités visées aux points a) et b).

3) Outre le paragraphe 2), un mandat d'interception autorise :

a) la récupération d'un dispositif d'interception ; et

b) l'entrée, avec la force raisonnable nécessaire, dans tout local en vue de placer, d'entretenir ou de récupérer un dispositif d'interception ; et

c) la connexion du dispositif d'interception à toute source d'électricité et l'utilisation de l'électricité de cette source pour faire fonctionner le dispositif ; et

d) la fourniture d'une assistance ou d'une expertise technique à l'agent de police principalement responsable de l'exécution du mandat pour l'installation, l'utilisation, l'entretien ou la récupération du dispositif d'interception.

4) Si le mandat autorise le placement d'un dispositif d'interception dans unlieu d'habitation ou d'affaires de :

a) un avocat, d'un membre du clergé ou d'un médecin ; ou

b) une personne désignée par la Cour,

la Cour peut fixer les conditions qu'elle estime nécessaires pour éviter dans la mesure du possible l'interception d'information ou d'enregistrement ou l'observation d'activités de caractère professionnel auxquelles l'avocat, l'ecclésiastique, le médecin ou toute autre personne désignée par la Cour est partie.

5) Pour éviter tout doute, un mandat d'interception ne doit pas nécessairementêtre limité à des locaux particuliers et peut s'appliquer à un dispositif d'interception conçu pour intercepter des communications ou observer ou enregistrer des activités impliquant une personne, où que cette personne setrouve.

30 Octroi d'un mandat d'interception

1) La Cour peut accorder un mandat d'interception si elle est convaincue qu'il existe des motifs raisonnables : :

a) de soupçonner qu'une personne planifie ou commet une infraction spécifiée, ou y participe ou l'a planifiée ou commise, ou y a participé ; et

b) de croire que des preuves pertinentes pour l'enquête sur l'affaire seront obtenues par l'utilisation d'un mandat d'interception pour intercepter des communications privées ou enregistrer ou observerdes activités ; et

c) que l'interception proposée est justifiée par le préjudice social de l'infraction présumée contre laquelle elle est dirigée.

2) Outre le paragraphe 1), la Cour doit, avant d'accorder un mandatd'interception, prendre en considération les éléments suivants :

a) la gravité de l'infraction sur laquelle porte l'enquête ou la procédurepénale ;

b) la fiabilité des informations sur lesquelles la demande est fondée, ycompris la nature de la source des informations ;

c) si l'intérêt public dans la production de données à partir du systèmeinformatique ou du support de stockage des données l'emporte sur le droit à la vie privée d'une personne dont la vie privée peut être affectée par la production ;

d) s'il existe un lien suffisant entre les preuves recherchées et l'infraction à laquelle se rapporte l'enquête ou la procédure pénale ;

e) si une condition doit être incluse dans le mandat ;

f) si le pays étranger a présenté une demande d'entraide en vertu de laprésente Loi ou de la Loi sur l'Assistance réciproque en matière d'affaires criminelles et si le Procureur général a autorisé l'utilisation d'un pouvoir d'investigation légal ; et

g) toute autre question que la Cour juge pertinente.

31 Durée et prolongation du mandat d'interception

1) Un mandat d'interception est valable pour la période spécifiée dans lemandat, soit une période n'excédant pas 90 jours.

2) Sous réserve du paragraphe 1), la Cour peut accorder une prolongation d'un mandat d'interception sur demande faite avant l'expiration du mandat (ou de tout renouvellement en cours du mandat).

3) Une demande de prolongation d'un mandat d'interception doit :

a) fournir la raison et la période pour lesquelles le renouvellement estrequis ; et

b) être accompagnée de renseignements complets, ainsi que des dates et heures, sur toute interception effectuée ou tentée en vertu du mandat et d'une indication de la nature des informations qui ont étéobtenues par cette interception ; et

c) être étayées par toute autre information que la Cour estimenécessaire.

4) La Cour peut prolonger un mandat d'interception si elle est convaincue que les circonstances décrites à l'article 28 sont toujours applicables.

32 Mandat d'interception urgente

1) La Cour peut accorder un mandat d'interception urgente si elle estconvaincue que :

a) les circonstances auxquelles la demande se rapporte sont urgentes ;ou

b) le retard qui serait causé par le fait que la demande soit faite en personne ferait obstacle à l'exécution effective du mandat.

2) Un agent de police peut faire une demande de mandat d'interception urgente oralement, par téléphone, par courrier électronique, par télécopie ou par tout autre moyen électronique.

3) La Cour peut, oralement ou par écrit, décerner un mandat d'interceptionurgente pour :

a) l'interception de communications privées ; ou

b) l'enregistrement d'activités concernant un local particulier ; ou

c) une personne particulière ; ou

d) un lieu particulier ; ou

e) une chose particulière ; ou

f) un type d'installation particulier,et d'une manière particulière.

4) Le contenu et les termes d'un mandat d'interception en vertu de l'article 29s'appliquent au contenu et aux termes d'un mandat d'interception urgent.

5) Un mandat d'interception urgente est valable pendant 48 heures à compter de son émission.

6) Sous réserve du paragraphe 1), la Cour doit, dès que possible, remettre une copie du mandat à l'agent de police qui a demandé le mandat d'interception urgent conformément au paragraphe 2).

7) S'il n'est pas raisonnablement possible pour la Cour de donner une copie du mandat d'interception urgent à l'agent de police :

a) elle doit informer l'agent de police des conditions du mandat ainsi que de la date et de

l'heure de sa signature ; et

b) l'agent de police doit consigner les informations suivantes :

i) le nom du juge qui a émis le mandat d'interception urgent;et

ii) la date et l'heure de la signature du mandat d'interceptionurgent; et

33 Prestataire de services à qui doit être signifié un mandatd'interception

1) Si un mandat d'interception est délivré sous cette division pour intercepter une communication privée, l'agent autorisé doit :

a) informer le prestataire de services de l'existence du mandat ; et

b) de signifier une copie du mandat au prestataire de services.

2) Le prestataire de services doit se conformer au mandat dès qu'il estsignifié.

34 Admissibilité des preuves

1) Toute information ou tout enregistrement obtenu en vertu d'un mandat d'interception ou d'un mandat d'interception urgente est admissible comme preuve dans toute procédure de poursuite d'une infraction spécifiée.

2) Toute information ou tout enregistrement obtenu en violation du paragraphe 29. 4) ne constitue pas une preuve recevable.

35 Défaut mineur en rapport avec le mandat d'interception ou le mandat d'interception urgente

1) Le présent article s'applique si :

a) une information ou un enregistrement est censé être obtenu par l'utilisation d'un dispositif d'interception autorisé en vertu d'un mandat d'interception ou d'un mandat d'interception urgente ; et

b) il y a un défaut ou une irrégularité mineur(e) en relation avec le mandat d'interception ou le mandat d'interception urgente et, sans ce défaut ou cette irrégularité, le mandat d'interception ou le mandat d'interception urgente aurait été une autorité suffisante pour la mesure prise.

2) Le présent article s'applique si :

a) l'utilisation du dispositif d'interception doit être considéré commevalide ; et

b) toute information ou enregistrement obtenu en vertu du mandat d'interception ou du mandat d'interception urgente est admissible comme preuve comme si le mandat d'interception ou le mandat d'interception urgente ne comportait pas cette déformation ou irrégularité.

3) La référence au paragraphe 1) à un défaut ou à une irrégularité en rapport avec un mandat d'interception ou un mandat d'interception urgente est une référence à un défaut ou à une irrégularité (autre qu'un défaut ou une irrégularité substantielle) :

a) dans le cadre ou en relation avec la délivrance d'un document censé être ce mandat d'interception ou ce mandat d'interception urgente ; ou

b) en rapport avec l'exécution de ce mandat d'interception ou de ce mandat d'interception urgente ou avec l'exécution d'un document censé être ce mandat d'interception ou ce mandat d'interception urgente.

36 Interdiction de divulguer les communications interceptées et les enregistrements

1) Une personne qui :

a) intercepte ou aide à intercepter une communication privée conformément à un mandat d'interception ou à un mandatd'interception urgente ; ou

b) acquiert la connaissance d'une communication privée comme résultat direct ou indirect de cette interception ; ou

c) consigne les activités d'une personne,

cette communication ne doit pas divulguer en tout ou partie la substance ou la signification de ou de cet enregistrement .

2) Toute personne qui enfreint le paragraphe 1) commet une infraction qui l'expose sur condamnation :

a) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 2 000 000 VT ou d'emprisonnement n'excédant pas5 ans, ou des deux à la fois ; ou

b) dans le cas d'une personne morale, à une peine d'amende n'excédant pas 4 000 000 VT.

37 Révocation du mandat d'interception ou du mandat d'interception urgent

1) Un agent de police peut, à tout moment, demander à la Cour de révoquer un mandat d'interception ou un mandat d'interception urgent.

2) La Cour doit révoquer un mandat d'interception ou mandat d'interception urgent si elle est convaincue que le mandat n'est plus nécessaire.

3) Si un mandat d'interception ou mandat d'interception urgent visant à intercepter une communication privée est révoqué, l'agent de police doit informer le prestataire de services ou son représentant autorisé de la révocation, et donner au prestataire de services ou à son représentant autorisé une copie de la révocation, immédiatement après que le mandat aété révoqué.

Sous-titre 6 Dispositions relatives aux mandats informatiques

38 Le commissaire autorisera les demandes

1) Le commissaire peut autoriser une demande de :

a) un mandat informatique ou le renouvellement d'un mandatinformatique ; ou

b) un mandat informatique urgent.

2) Le Commissaire ne doit pas autoriser la demande visée au paragraphe 1), sauf s'il est convaincu qu'il existe des motifs raisonnables de soupçonner qu'il peut y avoir sur la personne ou sur le lieu un support de stockage de données, ou un réseau ou un système informatique qui :

a) peut constituer une preuve matérielle de la commission d'uneinfraction déterminée ;

b) peut constituer une preuve matérielle de la commission d'uneinfraction grave étrangère ;

c) a été acquise par une personne à la suite de la commission d'uneinfraction.

39 Demande de mandat informatique

1) Si le commissaire a autorisé une demande de mandat informatique en vertu de l'article 38, un agent autorisé doit demander à la Cour d'accorder un mandat informatique pour l'accès à :

a) un lieu spécifié dans le mandat ; ou

b) un support de stockage des données à l'endroit indiqué dans lemandat ; ou

c) un réseau informatique à l'endroit indiqué dans le mandat ;

d) un système informatique à l'endroit indiqué dans le mandat.

2) La demande doit être faite par écrit et sous serment par un agent habilité, et doit contenir :

a) si une personne doit être fouillée, ses nom, âge et adresse ; et

b) si un lieu doit être fouillé :

i) une description du lieu à fouiller ; et

ii) si le lieu est occupé, le nom et l'âge des occupants du lieu,s'ils sont connus ; et

c) l'infraction à laquelle la demande se rapporte ; et

d) une description de la nature du support de stockage des données, du réseau informatique, du système informatique ou de tout élément de preuve présumé ; et

e) les informations sur lesquelles se fonde le soupçon raisonnable de preuve de la perpétration d'une infraction :

i) se trouve sur ou sous le contrôle de la personne ou dans le lieu où est exécuté le mandat informatique ;

ii) est susceptible d'être sur ou sous le contrôle de la personneou à l'endroit où le mandat informatique est exécuté ; et

f) si un mandat informatique a déjà été délivré en rapport avec lapersonne ou le lieu ; et

g) si l'autorisation d'exécuter le mandat relatif aux ordinateurs la nuit est demandée, pourquoi il est nécessaire d'exécuter le mandat relatif aux ordinateurs la nuit ; et

h) la période pendant laquelle le mandat informatique est requis.

40 Octroi d'un mandat informatique

1) La Cour peut accorder un mandat informatique si elle est convaincue que la demande de l'agent autorisé est faite conformément aux paragraphes 391) et 2).

2) Sans limiter le paragraphe 1), avant d'accorder un mandat informatique, la Cour doit prendre en considération les éléments suivants :

a) la gravité de l'infraction sur laquelle porte l'enquête ou la procédurepénale ;

b) la fiabilité des informations sur lesquelles la demande est fondée, ycompris la nature de la source des informations ;

c) si l'intérêt public dans la production de données à partir du systèmeinformatique ou du support de stockage des données l'emporte sur le droit à la vie privée d'une personne dont la vie privée peut être affectée par la production ;

d) s'il existe un lien suffisant entre les preuves recherchées et l'infraction à laquelle se rapporte l'enquête ou la procédure pénale ;

e) si une condition doit être incluse dans le mandat informatique; et

f) la durée proposée du mandat informatique ; et

g) toute autre question que la Cour juge pertinente.

41 Contenu du mandat informatique

Un mandat informatique doit mentionner les informations suivantes :

a) si une personne doit être fouillée, son nom, son âge et son adresse ;et

b) si un lieu doit être fouillé :

i) une description du lieu à fouiller ; et

ii) si le lieu est occupé, le nom et l'âge des occupants du lieu,s'ils sont connus ; et

c) l'infraction à laquelle la demande se rapporte ; et

d) les types de pièces justificatives qui peuvent être recherchées; et

e) le pouvoir d'un agent autorisé de sécuriser ou de rendre inaccessible un support de stockage de données, un réseau ou unsystème informatique ; et

f) la date et l'heure d'expiration du mandat informatique ; et

g) toute condition imposée en relation avec l'exécution du mandatinformatique.

42 Prolongation d'un mandat informatique

1) La Cour doit préciser dans le mandat informatique la date et l'heure de lafin du mandat de perquisition.

2) La Cour peut prolonger la date et l'heure de fin d'un mandat informatique si elle est convaincue que l'objectif pour lequel le mandat a été octroyé nepeut être atteint avant l'expiration du mandat.

43 Demande d'un mandat informatique urgent

1) Si le commissaire a autorisé une demande de mandat urgent d'accès à unordinateur en vertu de l'article 38, un agent autorisé peut demander à la Cour d'accorder un mandat urgent d'accès à un ordinateur :

a) à un lieu spécifié dans le mandat ; ou

b) un support de stockage des données à l'endroit indiqué dans lemandat ; ou

c) un réseau informatique à l'endroit indiqué dans le mandat ;

d) un système informatique à l'endroit indiqué dans le mandat.

2) Un agent habilité peut faire une demande pour un mandat d'interception urgent oralement, par téléphone, courriel, télécopie ou par tout autre moyen électronique.

3) L'agent habilité présentant une demande conformément au paragraphe 2)doit spécifier :

a) si une personne doit être fouillée, ses nom, âge et adresse ; et

b) si un lieu doit être fouillé :

i) une description du lieu à fouiller ; et

ii) si le lieu est occupé, le nom et l'âge des occupants du lieu,s'ils sont connus ; et

c) l'infraction à laquelle la demande se rapporte ; et

d) une description de la nature du support de stockage des données, du réseau informatique, du système informatique ou de tout élément de preuve présumé ; et

e) les informations sur lesquelles se fonde le soupçon raisonnable de preuve de la commission d'une infraction :

i) se trouve sur ou sous le contrôle de la personne ou dans lelieu

ii) est susceptible d'être sur ou sous le contrôle de la personne ou à l'endroit où un mandat informatique urgent est exécuté ; et

f) si un mandat informatique urgent a déjà été délivré en rapport avec la personne ou le lieu ; et

g) si l'autorisation d'exécuter un mandat urgent pour ordinateur la nuitest demandée, pourquoi il est nécessaire d'exécuter le mandat urgent pour ordinateur la nuit ; et

h) la période pendant laquelle un mandat informatique urgent estnécessaire.

4) L'agent habilité doit, dès que possible, après l'octroi du mandat informatique urgent, adresser sa demande, par écrit, à la Cour.

44 Octroi d'un mandat informatique urgent

1) La Cour peut accorder un mandat informatique urgent si elle est satisfaite de la demande présentée par l'agent habilité en vertu de l'article 43.

2) Sans limiter la portée du paragraphe 1), avant d'accorder un mandat urgent pour ordinateur, la Cour doit prendre en considération les éléments suivants :

a) l'urgence de la situation nécessitant un mandat urgent relatif auxordinateurs ; et

b) la gravité de l'infraction sur laquelle porte l'enquête ou la procédure pénale ; et

c) la fiabilité des informations sur lesquelles la demande est fondée, y compris la nature de la source des informations ; et

d) si l'intérêt public dans la production de données à partir du systèmeinformatique ou du support de stockage des données l'emporte sur le droit à la vie privée d'une personne dont la vie privée peut être affectée par la production ; et

e) s'il existe un lien suffisant entre les preuves recherchées et l'infraction à laquelle se rapporte l'enquête ou la procédure pénale ;et

f) si une condition doit être incluse dans le mandat informatique ; et

g) la durée proposée du mandat informatique ; et

h) toute autre question que la Cour juge pertinente.

45 Effets du mandat informatique et du mandat informatique urgent

1) L'agent habilité est autorisé, en vertu d'un mandat informatique ou d'un mandat informatique urgent accordé en vertu des articles 40 et 44, à :

a) saisir un objet dont l'agent autorisé a des motifs raisonnables decroire qu'il est :

i) un élément de preuve en rapport avec une infraction viséepar le mandat ; ou

ii) un élément de preuve pertinent pour une autre infraction àla présente Loi ou à toute autre loi ; et

b) accéder à un support de stockage de données, à un réseau informatique ou à un système informatique afin d'obtenir des informations et des enregistrements, et rassembler, copier ouextraire des données ; et

c) accéder, saisir ou sécuriser tout équipement, support de stockage dedonnées ou autre élément permettant de stocker des informations, des enregistrements ou des données ; et

d) demander à une personne ayant connaissance d'un support de données, d'un réseau informatique ou d'un système informatique d'aider l'agent habilité à accéder au support de données, au réseau informatique ou au système informatique ; et

e) si un agent habilité a des motifs raisonnables de soupçonner que les données accessibles à partir du système informatique pourraient être les données auxquelles on pourrait avoir accès, qu'il pourrait rassembler ou saisir en vertu du mandat ou d'un autre élément visé au point a), l'agent habilité peut :

i) faire fonctionner le système informatique pour accéder auxdonnées ; ou

ii) utiliser un autre système informatique accessible à partir du système informatique exploité en vertu du point i) pour accéder aux données ; ou

iii) copier tout ou partie des données sur un autre support de stockage des données ou sur un réseau ou un système informatique ; ou

iv) si, en utilisant les installations du lieu, les données peuvent être mises sous forme documentaire, exploiter les installations pour mettre ces données sous cette forme et saisir les documents produits ; et

f) déplacer le support de stockage des données ou un réseau informatique ou un système informatique du lieu perquisitionné vers un autre lieu pour examen afin de déterminer s'il contient des données auxquelles on pourrait accéder, qu'on pourrait collationner ou qu'on pourrait saisir en vertu du mandat, le cas échéant ;

i) l'occupant du lieu y consent ; ou

ii) il est nettement plus facile de le faire compte tenu du temps nécessaire pour copier les données et il existe des motifs raisonnables de soupçonner que les données auxquelles on pourrait accéder, qu'on pourrait rassembler ou qu'on pourrait saisir en vertu du mandat ; et

g) faire tout ce qui est raisonnablement nécessaire pour prévenir la perte, la destruction ou l'endommagement de tout ce qui est lié à l'infraction ou à toute autre infraction ; et

h) faire appel à d'autres agents ou personnes autorisés dans la mesure raisonnablement nécessaire à l'exécution du mandat ; et

i) de fouiller une personne qui se trouve sur les lieux au moment de l'exécution du mandat si l'ordonnateur soupçonne, pour des motifs raisonnables, que cette personne a des éléments de preuve en sa possession.

2) Si un agent habilité saisit un support de stockage de données, un réseau informatique, un système informatique, un équipement, un dispositif ou un autre article en vertu du paragraphe 1), l'agent autorisé :

a) peut en prendre possession ; et

b) peut le conserver pendant la durée qu'il estime nécessaire aux fins de la présente Loi.

4) Un agent habilité doit restituer tout objet détenu en vertu du paragraphe 2) à son propriétaire si :

a) il n’est plus nécessaire de saisir l’objet ; ou

b) il est décidé que l'objet ne doit pas être utilisé à des fins de preuve,sauf si l'agent habilité a des motifs raisonnables de croire que la possession de données peut constituer une infraction.

46 Accès aux données saisies

1) Sous réserve du paragraphe 2), sur demande, l'agent de Police qui exécuteun mandat informatique doit :

a) permettre à une personne qui avait la garde ou le contrôle du support de stockage des données, du réseau d'ordinateurs ou dusystème informatique, ou à une personne agissant en son nom, d'accéder aux données et de les copier ; ou

b) donner à cette personne une copie de ces données détenues dans le système informatique.

2) L'agent de Police peut refuser de donner accès à des données détenues dans un support de stockage de données, un réseau d'ordinateurs ou un système informatique ou de fournir des copies de ces données s'il a des motifs raisonnables de croire que le fait de donner l'accès ou de fournir descopies peut :

a) constituer une infraction à la présente loi ou à toute autre loi ; ou

b) porter atteinte à une enquête ou à une procédure pénale.

47 Sécuriser ou rendre inaccessibles des données en vertu d'un mandat informatique ou d'un mandat informatique urgent

1) Aux fins du présent article, expert s'entend d'un expert en criminalistiquenumérique

2) Un agent habilité exécutant un mandat informatique ou un mandat informatique urgent peut faire tout ce qui est nécessaire pour sécuriser ourendre accessible un support de stockage de données, un réseau d'ordinateur ou un système informatique s'il a des motifs raisonnables desoupçonner que :

a) les preuves de la commission d'une infraction peuvent être accessibles en utilisant le support de stockage de données, le réseaud'ordinateur ou le système informatique ;

b) une assistance d'expert est nécessaire pour faire fonctionner le support de stockage des données, le réseau d'ordinateurs ou lesystème informatique ; et

c) si il ne prend pas des mesures en vertu du présent paragraphe, leséléments de preuve peuvent être détruits, modifiés ou altérés de toute autre manière.

3) L'agent de Police doit, par voie de notification, informer la personne qui ala garde ou le contrôle du support de stockage des données, du réseau d'ordinateur ou du système informatique :

a) de son intention de sécuriser ou de rendre inaccessible le support de stockage des données, le réseau d'ordinateur et le système informatique ; et

b) que le support de stockage des données, le réseau d'ordinateurs et le système informatique peuvent être sécurisés ou inaccessibles pendant 28 jours au maximum.

4) Le support de stockage des données, l'ordinateur ou le système informatique peuvent être sécurisés ou inaccessibles jusqu'à ce que l'une des situations suivantes se produise :

a) 28 jours après que le support de stockage des données, le réseau d'ordinateurs ou le système informatique ait été sécurisé ou renduinaccessible pour la première fois ; ou

b) le support de stockage des données, le réseau d'ordinateur ou le système informatique a été exploité par un expert.

5) L'agent de Police peut demander au tribunal une prolongation du délai visé à l'alinéa 3) a), s'il a des motifs raisonnables de croire que l'assistance d'un expert ne sera pas disponible dans ce délai.

6) L'agent de Police peut présenter plus d'une demande en vertu duparagraphe 4) jusqu'à ce que l'expertise soit disponible.

7) L'agent de Police, par voie de notification, informe la personne qui a la garde ou le contrôle du support de stockage des données, du réseau d'ordinateurs ou du système informatique :

a) son intention de demander une prolongation ; et

b) que la personne a le droit d'être entendue en ce qui concerne lademande.

48 Aide à un fonctionnaire de police dans l'exécution d'un mandat informatique

1) Un agent de Police peut ordonner à une personne en possession ou en contrôle du support de stockage des données, du réseau d'ordinateur ou du système informatique, ou ayant connaissance de ceux-ci, de l'aider à :

a) accéder au support de stockage des données, au réseau d'ordinateur ou au système informatique et de l'utiliser pour accéder à toute donnée informatique (y compris les données stockées en tout lieu ou sur un support de stockage des données distinct) ;

b) obtenir et copier les données ;

c) utiliser des équipements pour faire des copies des données ;

d) obtenir une sortie intelligible du système informatique dans unformat lisible ; et

e) faire tout ce que l'agent de Police peut raisonnablement exiger.

2) Toute personne qui, sans excuse raisonnable, ne se conforme pas à une instruction donnée en vertu du paragraphe 1) commet une infraction quil'expose sur condamnation :

a) dans le cas d'un particulier – à une peine d'amende n'excédant pas 1000 000 VT ou d'emprisonnement n'excédant pas 3 ans, ou des deux à la fois; ou

b) dans le cas d'une personne morale – à une peine d'amenden'excédant pas 2 000 000 VT.

49 Faire preuve d'une diligence raisonnable

1) Aux fins de la présente section, les dommages, liés aux données, comprennent les dommages causés par l'effacement des données ou l'ajout d'autres données, mais n'incluent pas l'altération raisonnable des données par des procédés de médecine légale numérique.

2) Un agent de Police, ou une personne qui l'assiste lors de l'examen ou de la conservation d'un support de stockage de données, d'un réseau informatique ou d'un système informatique en vertu d'un mandat informatique ou d'un mandat informatique urgent, doit prendre des mesures raisonnables pour éviter tout dommage aux éléments suivants :

a) au support de stockage des données, au réseau d'ordinateur ou au système informatique ; et

b) les données stockées sur le support de stockage des données, le réseau d'ordinateur ou le système informatique, ou auxquelles on accède en utilisant ce dernier ; et

c) les programmes associés à l'utilisation du support de stockage des données, du réseau d'ordinateur ou du système informatique, ou à l'utilisation des données stockées dans le support de stockage des données, le réseau d'ordinateur ou le système informatique.

50 Réception de biens saisis en vertu d'un mandat informatique

1) Aux fins du présent article, on entend par reçu un inventaire de tous lesobjets recueillis pendant l'exécution du mandat informatique ou mandatinformatique urgent.

2) Si un mandat informatique autorise un agent de police à saisir une chose, l'agent de police doit, après avoir saisi la chose, remettre à la personne fouillée ou à l'occupant du lieu fouillé un reçu pour la chose saisie ; ou laisser un reçu pour la chose saisie dans

un endroit bien visible du lieu.

3) Le reçu doit comporter des informations suffisantes pour identifier les éléments suivants :

a) la chose qui a été saisie ;

b) l'heure à laquelle la chose a été saisie ;

c) la personne qui a saisi la chose ;

d) le lieu où la chose a été prise ; et

e) l'heure à laquelle la chose doit être rendue.

4) Le présent article ne s'applique pas si un agent de police a des motifs raisonnables de croire que :

a) aucune personne ne semble être en possession de la chose; ou

b) la chose est abandonnée.

51 Mesures visant à contrôler la conservation du support de stockage desdonnées, du réseau informatique ou du système informatique saisi

1) Un agent de Police qui saisit un support de stockage de données, un réseau informatique ou un système informatique en vertu d'un mandat informatique ou mandat informatique urgent, doit prendre des mesures raisonnables pour réduire la nécessité d'une conservation prolongée du support de stockage de données, du réseau informatique ou du système informatique à titre de preuve en prenant l'une des mesures suivantes dèsque possible :

a) en faisant en sorte que le support de stockage des données, le réseau informatique ou le système informatique, ou une partie decelui-ci, soit copié ; ou

b) en faisant procéder à tout test ou examen nécessaire du support destockage des données, du réseau informatique ou du système informatique ; ou

c) en recueillant toute autre preuve secondaire disponible en rapport avec le support de stockage des données, l'ordinateur ou le systèmeinformatique.

2) Malgré le paragraphe 1), un officier de police peut conserver le support destockage de données, le réseau informatique ou le système informatique pendant une durée raisonnable s'il a des motifs raisonnables de croire que cela est nécessaire pour empêcher la commission d'une infraction.

52 Destruction de certaines données saisies en vertu d'un mandat informatique ou mandat informatique urgent

Si le commissaire est convaincu que les données consultées ou copiées en vertu d'un mandat informatique ou mandat informatique ne sont plus utiles aux fins de l'application de la loi, il doit prendre les dispositions nécessaires pour la destruction des données, et toute reproduction, sous le contrôle des forces de police de Vanuatu.

53 Interdiction de divulgation d'informations, de dossiers et de données

1) La personne qui obtient des informations, des extraits, des dossiers ou des données à la suite d'une demande, d'une ordonnance ou d'un mandat en vertu de la présente partie ne doit pas, dans l'exercice de ses fonctions, divulguer sciemment, en tout ou en partie, les informations, extraits, dossiers ou données.

2) Toute personne qui enfreint le paragraphe 1) commet une infraction et qui l'expose sur condamnation :

   a) dans le cas d'une personne physique, à une peine d'amende n'excédant pas 1 000 000 VT ou d'emprisonnement n'excédant pas3 ans, ou les deux à la fois ; ou

   b) dans le cas d'une personne morale – à une peine d'amende n'excédant pas 2 000 000 VT.

54 Certificats de preuve pour les prestataires de services

1) Un représentant autorisé peut délivrer une attestation sous serment du représentant, exposant les faits qu'il juge pertinents par rapport aux actes ou choses faits par le prestataire de services ou en relation avec lui afin de :

   a) donner suite à une demande de divulgation de données relatives aux abonnés ou de données relatives au trafic en vertu des articles21, 22 et 24 ; ou

   b) répondre à une demande d'accès aux données relatives au trafic entemps réel en vertu de l'article 23 ; ou

   c) se conformer à une ordonnance de conservation rendue en vertu de l'article 2 ; ou

   d) permettre l'exécution d'un mandat d'interception.

2) Un certificat de preuve délivré en vertu du paragraphe 1) :

   a) doit être reçu comme preuve dans la procédure sans autre preuve ;et

   b) constitue une preuve concluante des éléments qui y sont énoncés.

55 Entrave ou obstruction à l'exercice légal des pouvoirs

1) Une personne commet une infraction si sans excuse raisonnable :

a) elle entrave ou empêche un agent de Police, ou une personne qui l'assiste, dans l'exercice de ses fonctions en vertu de la présente Loi ; ou

b) a l'intention d'entraver ou de gêner l'agent de Police ou unepersonne qui l'assiste.

2) Toute personne qui commet l'infraction visée au paragraphe 1) s'expose sur condamnation :

a) dans le cas d'une personne physique - à une peine d'amende n'excédant pas 1 000 000 VT ou d'emprisonnement n'excédant pas3 ans, ou les deux à la fois ; ou

b) dans le cas d'une personne morale – à une peine d'amenden'excédant pas 2 000 000 VT.

56 Obligations des prestataires de services

1) Un prestataire de services doit empêcher que les réseaux et les installations de communication soient utilisés dans le cadre ou en relation avec la commission d'infractions à la présente loi ou à toute autre loi.

2) Un prestataire de services ou un représentant autorisé qui reçoit une demande d'information en vertu de la présente Loi doit préserver la confidentialité de toute procédure et de toute information relative à lademande.

3) Un prestataire de services ou un représentant autorisé qui ne se conforme pas, sans excuse raisonnable, au paragraphe 2) commet une infraction qui l'expose sur condamnation, à une peine d'amende n'excédant pas 2 000 000 VT.

4) Un prestataire de services ou un représentant autorisé commet une infraction s'il ne se conforme pas à une demande légale faite par un agentde police en vertu de la présente Loi et s'expose sur condamnation, à unepeine d'amende n'excédant pas 2 000 000 VT.

5) Dans le présent article, la référence à l'assistance comprend une référence à l'assistance raisonnablement nécessaire aux fins suivantes :

a) l'application du droit pénal et des lois imposant des sanctionspécuniaires ; et

b) aider à l'application des lois pénales en vigueur dans un Étatétranger ; et

c) la protection des recettes publiques ; et

d) la protection de la sécurité nationale.

TITRE 5 COOPÉRATION INTERNATIONALE

57 Principes généraux relatifs à l'assistance réciproque

Vanuatu peut coopérer avec tout pays étranger, tout organisme étranger ou tout organisme international aux fins d'enquêtes ou de procédures concernant des infractions liées aux systèmes et données informatiques ou pour la collecte de preuves sous forme électronique d'une infraction pénale en vertu de la présente Loi et de la Loi sur l'Assistance réciproque en matière d'affaires criminelles.

58 Le Procureur général doit présenter des demandes d'assistance réciproque et y donner suite

1) Le Procureur général peut présenter des demandes d'assistance réciproque dans le cadre de toute enquête ou procédure engagée à Vanuatu, concernant toute infraction informatique ou liée à l'informatique.

2) Le Procureur général peut, en ce qui concerne toute demande d'un pays étranger d'assistance réciproque dans le cadre d'une enquête ou d'une procédure engagée dans ce pays étranger :

   a) faire droit à la demande, en tout ou en partie, selon les modalités et conditions qu'il juge appropriées ; ou

   b) refuser conformément aux dispositions prévues aux articles 8, 9 et 10 de la Loi sur l'Assistance réciproque en matière d'affaires criminelles ; ou

   c) après avoir consulté l'autorité compétente du pays étranger, reporter la demande, en tout ou en partie, au motif que le fait d'accéder immédiatement à la demande risquerait de nuire à laconduite d'une enquête ou d'une procédure à Vanuatu.

3) Une demande d'assistance réciproque en vertu du présent article doit être exécutée conformément aux procédures spécifiées par le pays étranger, sauf en cas d'incompatibilité avec les lois de Vanuatu.

4) Avant de refuser ou de reporter l'assistance, le Procureur général doit, le cas échéant après avoir consulté le pays étranger, examiner si la demande peut être acceptée en partie ou sous certaines conditions.

5) Le Procureur général doit immédiatement informer le pays étranger du résultat de l'exécution d'une demande d'entraide.

6) Outre le paragraphe 5), le Procureur général doit informer l'État étranger des motifs de la demande :

   a) rendre impossible l'exécution de la demande ; ou

   b) pour retarder sensiblement l'exécution de la demande ; ou

   c) de reporter la demande ; ou

d) de refuser la demande.

7) L'État étranger peut demander au Procureur général de garder confidentiels le fait de toute demande faite en vertu de la présente Loi ou de la Loi sur l'Assistance réciproque en matière d'affaires criminelles ainsi que son objet, sauf dans la mesure nécessaire à son exécution.

8) Si le Procureur général ne peut pas se conformer à la demande de confidentialité en vertu du paragraphe 7), il doit immédiatement en informer le pays étranger si la demande doit encore être exécutée.

9) Le paragraphe 8) applique mutatis mutandis lorsque le Procureur général est le pays demandeur.

10) Si le pays étranger ne peut pas remplir les conditions visées au paragraphe 2), il doit en informer le Procureur général, qui déterminera alors si l'information doit encore être fournie.

11) Si le pays étranger accepte les informations sous réserve de ces conditions, il est lié par celles-ci.

12) Les paragraphes 1), 2) et 3) s'appliquent mutatis mutandis lorsque des informations spontanées sont fournies au procureur par un pays étranger.

59 Informations complémentaires

1) Le Procureur général peut, sous réserve de la présente Loi et sans demande préalable, transmettre à un pays étranger des informations obtenues dans le cadre de ses propres enquêtes lorsqu'il estime que la divulgation de ces informations est nécessaire :

a) pour aider le pays étranger à engager ou à mener à bien des enquêtes ou des procédures ; ou

b) et pourrait conduire à une demande de coopération de la part du pays étranger en vertu de la présente Loi.

2) Avant de fournir ces informations, le Procureur général peut demander que celles-ci soient tenues confidentielles ou qu'elles ne soient utilisées que sous certaines conditions.

60 Conservation accélérée des données informatiques stockées

1) Un pays étranger peut demander ou obtenir de toute autre manière une conservation

accélérée des données stockées au moyen d'un système informatique, situé sur le territoire de Vanuatu et pour lequel le pays étranger requérant, l'agence étrangère ou toute agence internationale a l'intention de soumettre une demande d'assistance mutuelle pour la recherche ou l'accès similaire, la saisie ou la sécurisation similaire, ou ladivulgation des données.

2) Une demande de conservation accélérée faite en vertu du paragraphe 1)doit préciser :

a) l'autorité qui demande la conservation ; et

b) l'infraction qui fait l'objet d'une enquête ou d'une procédure pénale et un bref résumé des faits qui s'y rapportent ; et

c) les données informatiques stockées à conserver et leur relation avecl'infraction ; et

d) toute information disponible permettant d'identifier le dépositaire des données informatiques stockées ou l'emplacement du systèmeinformatique ; et

e) la nécessité d'une conservation accélérée ; et

f) que le pays étranger a l'intention de présenter une demande d'assistance mutuelle pour la perquisition ou l'accès similaire, la saisie ou la sécurisation similaire, ou la divulgation des donnéesinformatiques stockées.

3) Dès réception d'une demande en vertu du paragraphe 1), le procureur doit prendre toutes les mesures appropriées pour conserver rapidement les données spécifiées conformément aux procédures et aux pouvoirs prévuspar la présente loi.

4) Toute conservation accélérée effectuée en réponse à la demande doit être d'une durée d'au moins 60 jours, afin de permettre à l'État étranger de soumettre une demande de perquisition ou d'accès similaire, de saisie ou de sécurisation similaire, ou de divulgation des données et, suite à la réception d'une telle demande, les données doivent continuer à être conservées de manière accélérée jusqu'à ce qu'une décision finale soit prisesur cette demande en attente.

5) Les paragraphes 1) et 2) doivent s'appliquer mutatis mutandis lorsqu'une demande de conservation accélérée de données informatiques stockées estfaite par Vanuatu.

61 Divulgation accélérée des données relatives au trafic conservées

1) Au cours de l'exécution d'une demande en vertu de l'article 22 ou autrement en relation avec une infraction grave dans un État étranger, leservice répressif, en ce qui concerne une communication spécifiée, découvre qu'un prestataire de services dans un autre pays est impliqué dans la transmission de la communication, le Procureur général se doit :

a) de divulguer rapidement au pays étranger requérant une quantité suffisante de données relatives au trafic pour identifier ce prestataire de services ; et

b) de révéler le chemin par lequel la communication a été transmise.

2) La divulgation accélérée de données relatives au trafic conservées en vertu du paragraphe 1) ne peut être retirée que si :

a) la demande concerne une infraction politique ou une infraction liée à une infraction politique ; ou

b) le Procureur général estime que l'exécution de la demande est susceptible de porter atteinte à la souveraineté de Vanuatu, à sa sécurité ou à l'intérêt public.

62 Assistance mutuelle en matière d'accès aux données informatiques stockées

1) Un pays étranger peut demander d'ordonner ou de perquisitionner ou d'accéder de manière similaire, de saisir ou de sécuriser de manière similaire, et de divulguer des données stockées au moyen d'un système informatique situé sur le territoire de Vanuatu, en relation avec une infraction étrangère grave, y compris les données qui ont été conservéesconformément à l'article 18.

2) Une demande d'entraide concernant l'accès à des données informatiquesstockées doit, dans la mesure du possible :

a) indiquer le nom de l'autorité qui mène l'enquête ou la procédure à laquelle la demande se rapporte ;

b) donner une description de la nature de l'affaire pénale et une déclaration présentant un résumé des faits et des lois pertinentes ;

c) décrire l'objet de la demande et la nature de l'assistance recherchée ;

d) dans le cas d'une demande de saisie ou de confiscation d'avoirs dont on a des motifs raisonnables de penser qu'ils se trouvent dansle pays requis :

i) donner des précisions sur l'infraction en question ; ou

ii) les détails de toute enquête ou procédure engagée en rapport avec l'infraction,

et être accompagnée d'une copie de toute décision de restriction ou de confiscation pertinente ;

e) donner des précisions sur toute procédure que le pays requérant souhaite voir suivre par le pays requis pour donner suite à la demande, en particulier dans le cas d'une demande d'obtention depreuves ;

f) comprend une déclaration exposant les souhaits éventuels du pays demandeur concernant la confidentialité relative à la demande et les raisons de ces souhaits ;

g) indiquer le délai dans lequel le pays demandeur souhaite que la demande soit satisfaite ;

h) le cas échéant, donner des précisions sur les biens, l'ordinateur, le système informatique ou le dispositif à localiser, à retenir, à saisir ou à confisquer, ainsi que sur les motifs permettant de penser queces biens se trouvent dans le pays requis ;

i) donner des détails sur les données informatiques stockées, les données ou le programme à saisir et leur relation avec l'infraction ;

j) donner toute information disponible permettant d'identifier le dépositaire des données informatiques stockées ou l'emplacement de l'ordinateur, du système ou du dispositif informatique ;

k) comporter un accord sur la question du paiement des dommages etintérêts ou des frais d'exécution de la demande; et

l) donner toute autre information susceptible de contribuer à donnersuite à la demande.

3) Dès réception de la demande en vertu du présent article, l'organisme d'enquête doit prendre toutes les mesures appropriées pour obtenir l'autorisation nécessaire, y compris tout mandat d'exécution de la demande conformément aux procédures et pouvoirs prévus par la présente loi.

4) Après avoir obtenu l'autorisation nécessaire, y compris tout mandat d'exécution, l'organisme d'enquête peut solliciter l'appui et la coopération du pays étranger pendant la perquisition et la saisie.

5) Lors de l'exécution de la demande de perquisition et de saisie, l'organisme d'enquête doit fournir les résultats de cette perquisition et de cette saisie aupays étranger.

6) Les paragraphes 1) et 2) doivent s'appliquer mutatis mutandis aux demandes de conservation accélérée de données informatiques stockées sur le territoire d'un pays étranger.

63 Accès transfrontalier à des données informatiques stockées avec le consentement de l'intéressé ou lorsqu'elles sont accessibles au public

Un agent de police peut, sans autorisation mais sous réserve des dispositionsapplicables de la présente Loi :

a) accéder à des données informatiques stockées accessibles au public, quel que soit l'endroit où elles se trouvent géographiquement ; ou

b) accéder ou recevoir, par l'intermédiaire d'un système informatique situé sur son territoire, des données informatiques stockées situées sur un autre territoire, si ce fonctionnaire de police ou une autre personne autorisée obtient le consentement

légal et volontaire de lapersonne qui a l'autorité légale de divulguer les données par l'intermédiaire de ce système informatique.

64 Assistance mutuelle dans la collecte en temps réel de données relativesau trafic

1) Un pays étranger peut demander, en relation avec une infraction étrangère grave, d'ordonner ou de fournir une assistance pour la collecte en temps réel de données relatives au trafic associées à des communications spécifiées à Vanuatu, transmises au moyen d'un système informatique.

2) Une demande d'assistance au titre du présent article doit préciser :

   a) l'autorité sollicitant l'utilisation des pouvoirs prévus par le présentarticle ;

   b) l'infraction qui fait l'objet d'une enquête ou d'une procédure pénale et un bref résumé des faits qui s'y rapportent ;

   c) le nom de l'autorité ayant accès aux données relatives au traficpertinentes ;

   d) le lieu où les données relatives au trafic peuvent être conservées ;

   e) la finalité prévue pour les données relatives au trafic requises;

   f) des informations suffisantes pour identifier les données relatives autrafic ;

   g) tout autre détail concernant les données relatives au trafic ;

   h) la nécessité de recourir aux pouvoirs prévus au présent article; et

   i) les conditions d'utilisation et de divulgation des données relatives au trafic à des tiers.

3) Sur réception d'une demande en vertu du paragraphe 1), l'organisme d'enquête doit prendre toutes les mesures appropriées pour obtenir l'autorisation nécessaire, y compris tout mandat d'exécution de la demande conformément aux procédures et aux pouvoirs prévus par la présente Loi.

4) Après avoir obtenu l'autorisation nécessaire, y compris tout mandat d'exécution, l'organisme d'enquête peut solliciter l'appui et la coopération du pays étranger pendant la perquisition et la saisie.

5) Lors de l'exécution des mesures prévues par le présent article, l'organisme d'enquête doit fournir les résultats de ces mesures ainsi que la collecte en temps réel des données relatives au trafic associées aux communications spécifiées vers le pays étranger.

6) Les paragraphes 1) et 2) doivent s'appliquer mutatis mutandis aux demandes de

collecte en temps réel de données relatives au trafic dans unpays étranger.

65 Assistance mutuelle en matière d'interception des données relatives au contenu

1) Un pays étranger peut demander d'ordonner ou de fournir une assistance pour la collecte ou l'enregistrement en temps réel des données relatives au contenu de communications spécifiques transmises au moyen d'un système informatique à Vanuatu.

2) Une demande d'assistance au titre du paragraphe 1) doit, dans la mesure dupossible, préciser :

a) l'autorité qui sollicite l'utilisation des pouvoirs prévus par le présentarticle ;

b) l'infraction qui fait l'objet d'une enquête ou d'une procédure pénale et un bref résumé des faits qui s'y rapportent ;

c) le nom de l'autorité ayant accès à la communication concernée ;

d) le lieu ou la nature de la communication ;

e) l'objectif visé par la communication requise ;

f) des informations suffisantes pour identifier les communications ;

g) les détails des données de l'interception concernée ;

h) le destinataire de la communication ;

i) la durée prévue pour l'utilisation de la communication ;

j) la nécessité de recourir aux pouvoirs prévus au présent article; et

k) les conditions d'utilisation et de divulgation de la communication àdes tiers.

3) Dès réception d'une demande au titre du présent article, le procureur doit prendre toutes les mesures appropriées pour exécuter la demande conformément aux procédures et aux pouvoirs prévus par la présente Loi.

4) Lors de l'exécution des mesures prévues au paragraphe 3), le procureurdoit fournir les résultats de ces mesures ainsi que la collecte ou l'enregistrement en temps réel des données relatives au contenu des communications spécifiées à l'étranger.

5) Les paragraphes 1) et 2) s'appliquent par analogie aux demandes de collecte en temps réel de données relatives au trafic dans un pays étranger.

66 Réseau 24/7

1) Le Procureur général doit veiller à ce que l'organisme d'enquête chargé de la recherche et de la poursuite de la cybercriminalité désigne un point de contact disponible vingt-quatre heures sur vingt-quatre, sept jours sur sept.

2) Un point de contact désigné en vertu du paragraphe 1) doit veiller à ce qu'une assistance soit immédiatement fournie aux fins de :

a) d'enquêtes ou de procédures concernant les infractions pénales liées à des systèmes et données informatiques ; ou

b) pour la collecte de preuves sous forme électronique d'une infraction pénale, cette assistance devant consister à faciliter ou, si la législation et la pratique de Vanuatu le permettent, à l'exécution directe des mesures suivantes :

i) la fourniture de conseils techniques ; et

ii) les données informatiques et la divulgation accélérée des données relatives au trafic conservées ; et

iii) la collecte de preuves, la fourniture d'informations juridiques et la localisation de suspects,

dans les délais rapides prescrits par le règlement.

2) Le point de contact doit être doté des ressources et des capacités nécessaires pour assurer de manière sûre et efficace les communications avec d'autres points de contact dans d'autres territoires, sur une base accélérée.

3) Le point de contact doit avoir le pouvoir et l'autorité de coordonner et de permettre l'accès à l'entraide internationale en vertu de la présente Loi ou, le cas échéant, aux procédures d'extradition, sur une base accélérée.

67 Rapport sur les pouvoirs d'enquête spéciaux

1) Le commissaire doit, au plus tard à la fin du mois de mars de chaque année, soumettre au Conseil des ministres un rapport annuel présentant des informations générales et des statistiques relatives à l'utilisation des pouvoirs d'enquête spéciaux pour l'année précédente.

2) Le rapport doit comprendre au minimum :

a) le nombre d'opérations d'infiltration autorisées

i) le nombre d'ordonnances rendues pour la conservation de données informatiques ;

ii) le nombre de demandes de données relatives au trafic entemps réel ;

iii) le nombre de demandes de production de donnéesinformatiques ; et

b) le nombre de demandes de mandats d'interception et de mandatsinformatiques ;

c) le nombre de demandes de renouvellement de mandats d'interception et de mandats informatiques ;

d) le nombre de demandes de mandats d'interception urgents et de mandats informatiques urgents ;

e) le nombre de livraisons contrôlées de biens autorisées ;

f) le nombre de demandes visées aux points b), c) et d) qui ont été acceptées et le nombre de celles qui ont été refusées ; et

g) le nombre de poursuites qui ont été engagées dans lesquelles des preuves ont été obtenues directement ou indirectement :

i) d'une interception effectuée en vertu d'un mandat d'interception ou d'un mandat d'interception urgente ;

ii) un support de stockage de données, un ordinateur ou un système informatique en vertu d'un mandat informatique oud'un mandat informatique urgent ;

iii) une opération d'infiltration ;

iv) une ordonnance de conservation de données informatiques ;

v) une demande d'accès aux données relatives au trafic et aux données relatives au trafic en temps réel ;

vi) un ordre de production de données informatiques ;

vii) une livraison contrôlée de biens a été présentée, et le résultat de ces poursuites ;

viii) le nombre de mandats d'interception et de mandats informatiques qui n'ont donné lieu à aucune inculpation dans les 90 jours suivant la date d'expiration du mandat ; et

ix) le nombre d'opérations d'infiltration et de livraisons contrôlées de biens qui n'ont donné lieu à aucune inculpation dans les 90 jours suivant la date à laquelle l'opération d'infiltration ou la livraison contrôlée a pris fin.

3) Aucune disposition du présent article n'oblige le commissaire à divulguer publiquement les détails opérationnels d'un cas particulier.

68 L'État n'est pas tenu de s'engager sur les coûts

Malgré toute autre loi, l'État n'est pas tenu de s'engager sur les frais de demande d'un mandat.

TITRE 6 DISPOSITIONS DIVERSES

69 Agent autorisé

1) Le Commissaire peut nommer un agent de Police, agent autorisé à exercer toute fonction ou tout pouvoir pouvant être exercé ou exécuté aux fins de la présente Loi, pour une période déterminée par le Commissaire.

2) Le Commissaire doit fournir à chaque agent autorisé une carte d'identité qui permettra de prouver l'identité de cet agent de police et sa nominationen tant qu'agent autorisé.

3) L'agent autorisé qui est titulaire d'une carte d'identité délivrée en vertu duprésent article doit, à la fin de son mandat, remettre sa carte d'identité au Commissaire.

70 Protection contre la responsabilité

1) Un agent de police ou agent autorisé ne peut faire l'objet d'aucune responsabilité civile ou pénale, action, réclamation ou demande pour toutce qu'il a fait ou omis de faire de bonne foi dans l'exécution ou la prétendue exécution de ses pouvoirs et fonctions en vertu de la présente Loi.

2) Un prestataire de services ou un représentant autorisé n'est pas responsable d'une action ou d'une autre procédure pour des dommages pour ou en relation avec un acte fait ou omis de bonne foi dans l'exécution d'un devoirimposé par la présente Loi.

71 Règlements

Le ministre peut prendre des règlements prescrivant des questions :

a) qui doivent ou peuvent être prescrites en vertu de la présente Loi ;ou

b) qui sont nécessaires ou utiles pour mieux appliquer ou donner effet aux dispositions de la présente Loi.

72 Entrée en vigueur

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