Nations Unies
Commission économique pour l'Afrique

Lignes directrices pour une loi type sur les délits informatiques et les délits liés à l'informatique dans les États membres de l'Union africaine

Nations Unies
Commission économique pour l'Afrique

Lignes directrices pour une loi type sur les délits informatiques et les délits liés à l'informatique dans les États membres de l'Union africaine

Pour commander des exemplaires de ***Lignes directrices pour une loi type sur les délits informatiques et les délits liés à l'informatique dans les États membres de l'Union africaine***, veuillez contacter :

Section des publications et de la gestion des conférences
Commission économique pour l'Afrique
B.P. 3001
Addis-Abeba, Éthiopie
Tél: +251-11- 544-9900
Télécopie: +251-11-551-4416
Adresse électronique: eca-info@un.org
Web: www.uneca.org

Premier tirage : mai 2023

Conçu et imprimé à Addis-Abeba par le Groupe de la publication et de l'impression de la CEA, certifié ISO 14001:2015. Imprimé sur du papier sans chlore.

Photos de couverture: Shutterstock.com

Table des matières

PARTIE I : Introduction

Dans ces lignes directrices, des orientations sont données aux États membres de l'Union africaine pour l'élaboration d'une législation sur la cybersécurité et les caractéristiques et avantages essentiels d'une loi normalisée sur la cybersécurité y sont présentés.

1. Contexte

L'application d'une législation sur la cybersécurité constitue un élément essentiel d'une réponse régionale permettant d'assurer la cybersécurité en Afrique. La quatrième recommandation formulée dans le Plan d'action de coopération numérique des Nations Unies (A/74/821) porte sur la promotion de la confiance, de la sécurité et de la stabilité numériques. À la suite d'une déclaration adoptée en 2019 par le Comité technique spécialisé de la Commission de l'Union africaine sur les communications et les technologies de l'information et des communications (AU/STC-CICT-3/MIN//Decl.), la Commission de l'Union africaine a élaboré une stratégie de transformation numérique pour l'Afrique (2020-2030), qui souligne la nécessité d'une plus grande capacité à détecter et à atténuer les cyberattaques ; la stratégie met aussi l'accent sur la responsabilité fondamentale qui incombe aux gouvernements africains de créer un environnement propice en mettant en œuvre des politiques et des réglementations qui favorisent une transformation numérique reposant sur des piliers fondamentaux, dont la cybersécurité[1]. Il est également dit dans la stratégie que les mesures et les outils de collaboration en vue de réglementer les technologies de l'information et des communications constituent la nouvelle frontière pour les organismes de réglementation et les décideurs qui s'efforcent de maximiser les possibilités offertes par la transformation numérique dans toutes les industries[2]. Certes, la transformation numérique offre à l'Afrique d'immenses possibilités, mais une transformation numérique efficace et efficiente ne peut être réalisée en Afrique que s'il y a la cybersécurité.

1 Union africaine, « La stratégie de transformation numérique pour l'Afrique (2020-2030) », p. 7.
2 Ibid.

Il est nécessaire d'établir des lignes directrices pour l'élaboration d'une loi type qui puisse aider les États membres de l'Union africaine à rédiger une législation sur la cybersécurité compatible avec les meilleures pratiques. Afin de réunir un ensemble minimum de normes de référence grâce auxquelles les gouvernements africains pourront trouver une solution au problème de la cybersécurité, les présentes lignes directrices ont été établies en tenant dûment compte des législations nationales sur la cybersécurité existantes en Afrique, de la Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles de 2014, de la Convention du Conseil de l'Europe sur la cybercriminalité de 2001 et des normes des Nations Unies sur le comportement responsable des États dans le cyberespace établies par le Groupe d'experts gouvernementaux sur la promotion d'un comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale. Les lignes directrices s'appuient également sur d'autres efforts régionaux et internationaux qui sont en cours dans le domaine de la cybersécurité, notamment les efforts tendant à l'élaboration d'une convention mondiale des Nations Unies sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles.

2. Champ d'application des lignes directrices

Les lignes directrices sont un ensemble de principes directeurs non contraignants que les États membres de l'Union africaine peuvent suivre lorsqu'ils commencent à établir des normes pour assurer la cybersécurité et pour rédiger des lois sur la cybercriminalité. Les lignes directrices ne restreignent pas l'application de toute loi nationale ou régionale, existante ou future, qui réglemente expressément ou implicitement la cybersécurité ou qui interdit une activité considérée comme une infraction cybercriminelle dans une juridiction donnée. Les lignes directrices ne fournissent pas de texte législatif spécifique pour la rédaction des dispositions des lois sur la cybersécurité ou la cybercriminalité ou pour l'application de ces lois ; compte tenu de la souveraineté des États et de la diversité de leurs systèmes juridiques nationaux, la formulation précise de ces lois est laissée à la discrétion des États.

3. Objet des lignes directrices

La législation sur la cybersécurité couvre la réglementation, l'entretien et la promotion des activités de cybersécurité, des infrastructures nationales

critiques et des services informatiques. Les lignes directrices sont conçues pour aider les États membres de l'Union africaine à établir, réformer et moderniser leurs lois sur la cybersécurité afin de prendre en compte les caractéristiques et les besoins particuliers de la promotion de la cybersécurité dans la région. Les lignes directrices sont destinées aux États africains ainsi qu'aux décideurs et législateurs africains qui veulent comprendre les éléments importants d'une loi type sur la cybersécurité.

Les lignes directrices visent à établir un lien entre les meilleures pratiques concernant les infractions substantielles, les pouvoirs et l'entraide judiciaire, telles que celles énoncées dans les traités régionaux et internationaux sur la cybersécurité ; des exemples spécifiques de normes, de principes et de mesures qui définissent les différents éléments à inclure dans la législation sur la cybersécurité sont donnés. Les lignes directrices contiennent également des orientations sur les dispositions relatives au respect des droits de l'homme, aux normes en matière d'application de la loi et au contrôle judiciaire ou à d'autres types de contrôle. Des lois sur la cybersécurité mal rédigées et s'écartant des meilleures pratiques internationales peuvent avoir un effet négatif sur les efforts de promotion de la cybersécurité et sur la coopération régionale et internationale. Des lois types rédigées de manière inefficace peuvent également amener les pays à promulguer une législation inadéquate sur la cybercriminalité, tout en érigeant en infractions pénales et en qualifiant de cybercriminels des comportements que d'autres pays ne considèrent peut-être pas comme tels. Il est donc important que les pays suivent un modèle approprié pour élaborer une législation sur la cybersécurité.

Les lignes directrices contiennent des mesures standards de cybersécurité, y compris celles qui visent à reconnaître les infractions, et elles définissent les types d'actes auxquels peut être conféré le caractère d'infractions pénales dans une loi type sur la cybersécurité. Les États, les législateurs et les organismes de réglementation sont encouragés à donner des orientations pour la création de programmes de cybersécurité qui soient flexibles, modulables, pratiques et conformes aux meilleures pratiques internationales. Les lignes directrices se terminent par des recommandations sur les normes relatives aux lois et règlements sur la cybersécurité dans les juridictions africaines. Elles contiennent aussi des orientations sur les activités en matière d'application de la loi qui peuvent être entreprises pour assurer la cybersécurité tout en donnant la priorité au respect des droits de l'homme, conformément aux normes internationales et régionales en matière de droits de l'homme.

4. Définitions

(1) Par « autorité compétente », on entend une autorité judiciaire, administrative ou toute autre autorité chargée de l'application de la loi, qui est investie par le droit interne du pouvoir d'ordonner des mesures, d'autoriser la prise de mesures ou de procéder à l'exécution de mesures, en vertu de la législation nationale sur la cybersécurité, dans le cadre d'enquêtes ou de procédures pénales spécifiques.

(2) Par « données informatiques », on entend toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction.

(3) Par « cyberextorsion », on entend une attaque ou une menace d'attaque accompagnée d'une demande d'argent ou de toute autre demande en échange de la réparation des conséquences de l'attaque ou de l'arrêt de celle-ci.

(4) Par « système informatique », on entend tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont l'un ou plusieurs assurent, en exécution d'un programme, un traitement automatisé de données.

(5) Par « société », on entend une entreprise à responsabilité limitée au sens de la législation nationale applicable d'un État.

(6) Par « infrastructures critiques », on entend l'ensemble des actifs, systèmes et réseaux - physiques et virtuels - qui sont essentiels pour le bon fonctionnement de l'économie d'un pays, de ses systèmes de santé publique, de sécurité et de sûreté, ou de toute combinaison de ces éléments.

(7) Par « cybercriminalité », on entend, aux fins des présentes lignes directrices, les comportements définis dans la Partie II. Infractions générales.

(8) Par « cybersécurité », on entend l'état de la protection contre l'utilisation criminelle ou non autorisée des systèmes et des données informatiques, les mesures prises pour assurer pareille protection et les activités nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes victimes de cybermenaces.

(9) Par « cybersquattage », on entend l'enregistrement, la vente ou l'utilisation d'un nom de domaine dans l'intention de tirer profit de

la clientèle attachée à la marque ou à la réputation commerciale d'une autre personne.

(10) Par « cybermenace », on entend toute circonstance, tout événement ou toute action pouvant causer des dommages aux réseaux et aux systèmes d'information, aux utilisateurs de ces systèmes et à d'autres personnes, et pouvant provoquer une perturbation de ces systèmes ou un effet négatif sur ces systèmes et personnes.

(11) Par « responsable du traitement des données », on entend une personne physique ou morale, une autorité, un service ou tout autre organisme publics qui, seul ou avec d'autres, détermine la finalité du traitement des données à caractère personnel et les moyens utilisés à cet effet.

(12) Par « attaques par déni de service », on entend les activités qui empêchent un utilisateur légitime d'accéder à un système informatique, ou les demandes en ligne rapides et continues qui sont envoyées à un serveur ciblé pour en provoquer la saturation.

(13) Par « incitation frauduleuse », on entend les pratiques trompeuses visant à persuader une autre partie d'agir contre son propre intérêt et à l'avantage de la partie qui se livre à la pratique trompeuse.

(14) Par « lignes directrices », on entend le texte législatif sur la cybersécurité pour les États membres de l'Union africaine proposé par la Commission économique pour l'Afrique, texte qui ne fait partie du corpus législatif d'aucun pays et qui vise à aider à l'adoption d'une nouvelle législation ou à la réforme de la législation existante.

(15) Par « interception », on entend la surveillance, la modification, la visualisation ou l'enregistrement de transmissions de données non publiques à destination ou en provenance d'un système informatique ou à partir de celui-ci via un système de télécommunications et, en relation avec une fonction d'un système informatique, le fait d'écouter ou d'enregistrer une telle fonction ou le fait d'acquérir la substance, la signification ou l'objet de pareille fonction.

(16) Par « logiciels malveillants et virus », on entend un ensemble d'instructions-machine conçues pour infecter des programmes informatiques ou des données informatiques, pour modifier,

détruire, enregistrer ou transmettre des données, ou pour perturber le fonctionnement normal d'un système informatique.

(17) Par « dirigeant », on entend, dans le cas d'une société, tout administrateur, associé, directeur général, gérant, secrétaire ou tout autre dirigeant de la société, y compris toute personne prétendant agir en cette qualité ; pour une société dont les affaires sont gérées par ses membres, le terme désigne l'un quelconque de ces membres en sa qualité de dirigeant de la société tel que défini dans le présent paragraphe.

(18) Par « données à caractère personnel », on entend les informations relatives à une personne physique identifiée ou identifiable.

(19) Par « identifiant personnel ou humain », on entend un sous-ensemble d'informations et d'éléments de données qui identifient une personne et peuvent permettre à une autre personne de présumer l'identité de cette personne à son insu ou sans son consentement.

(20) Par « rançongiciel », on entend un logiciel malveillant installé secrètement dans un système informatique, un programme informatique ou des données informatiques afin d'en empêcher l'accès.

(21) Par « État requis », on entend l'État auquel est demandée une assistance judiciaire.

(22) Par « État requérant », on entend l'État qui demande l'assistance judiciaire et il peut s'agir d'une entité internationale envers laquelle un État est tenu de s'acquitter d'une obligation.

(23) Par « clause d'immunité », on entend une disposition juridique nationale qui, dans certaines circonstances, prévoit que la responsabilité d'une personne ou d'une entité ne soit pas engagée pour ses activités.

(24) Par « fournisseur de services », on entend toute entité publique ou privée qui offre, aux utilisateurs de ses services, la possibilité de communiquer au moyen d'un système informatique, et toute autre entité traitant ou stockant des données informatiques pour l'entité en question ou les utilisateurs des services de celle-ci.

(25) Par « état d'esprit » d'une personne, on entend les connaissances, l'intention, l'opinion ou la croyance de cette personne, et les raisons qui motivent cette intention, cette opinion ou cette croyance chez cette personne.

(26) Par « accès non autorisé », on entend le fait d'entrer dans des ressources informatiques, de communiquer avec elles, d'y stocker des données, d'en extraire des données ou d'intercepter et de modifier de toute autre manière des ressources informatiques sans autorisation légale.

(27) Par « personne vulnérable », on entend une personne physique pouvant être désavantagée en raison de caractéristiques particulières, notamment l'âge, le handicap, le sexe ou le lieu de résidence.

5. Champ d'application général

(1) La législation des États sur la cybersécurité doit être axée sur la prévention des infractions cyberdépendantes et des infractions informatiques, sur les enquêtes et les poursuites concernant ces infractions, qui sont érigées en infractions pénales par des lois établies conformément à la législation nationale.

(2) Cette législation doit être rédigée en vue de faire face aux menaces ou incidents liés à la cybersécurité, de gérer et de prévenir ces menaces et incidents qui surviennent à l'intérieur et à l'extérieur du pays et qui peuvent menacer la vie et les biens des citoyens et des résidents ainsi que la sécurité nationale et celle de l'État.

(3) D'une manière générale, la législation sur la cybersécurité couvre les cyberservices qui sont essentiels au fonctionnement de la société, de l'État et des autorités locales, des réseaux et des systèmes d'information ainsi que des infrastructures critiques, et elle devrait viser à imposer des mesures adéquates pour assurer la sécurité organisationnelle, physique et de l'information, et pour prévenir, atténuer et résoudre les cybermenaces et les cyberincidents.

(4) Les États doivent veiller à ce que, dans la législation nationale sur la cybersécurité, la priorité soit accordée à la protection des droits de l'homme et des libertés fondamentales, à ce que des partenariats public-privé soient établis, et les États sont encouragés à s'occuper d'éducation, de recherche et de formation au profit du public, afin d'améliorer les connaissances et les compétences en matière de cybersécurité.

PARTIE II : Infractions générales

6. Accès illégal et non autorisé

(1) Les États adoptent les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, lorsque l'acte a été commis intentionnellement et sans autorisation ou au-delà de ce qui a été autorisé, l'accès à tout ou partie d'un système informatique, y compris l'accès à un système informatique connecté à un autre système informatique, ou toute action permettant d'obtenir, d'altérer ou d'empêcher l'accès autorisé.

(2) Les États adoptent les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, lorsque l'acte est commis intentionnellement et sans autorisation ou au-delà de ce qui a été autorisé, tout acte amenant un ordinateur à exécuter toute fonction permettant d'accéder à un programme informatique, à un système informatique ou à des données informatiques contenus dans cet ordinateur, ou permettant d'obtenir ou d'empêcher pareil accès.

7. Interception illégale

Les États adoptent les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, lorsque l'acte est commis intentionnellement, sans autorisation et sans excuse ou justification légitime, l'interception de données informatiques, lors de transmissions à destination, en provenance ou à l'intérieur d'un système informatique, y compris en relation avec un système informatique connecté à un autre système informatique.

8. Utilisation abusive de dispositifs informatiques et de codes d'accès

Les États adoptent les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, lorsque ces actes sont commis intentionnellement et sans justification, la production, la vente, l'obtention pour utilisation, la possession, l'importation et la distribution des éléments suivants :

a) Un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies dans la législation nationale comme une infraction cybercriminelle ;

b) Un mot de passe informatique, un code d'accès ou des données similaires permettant d'accéder à tout ou partie d'un système informatique, dans l'intention de les utiliser pour commettre toute infraction définie dans la législation nationale comme une infraction cybercriminelle.

9. Modification non autorisée d'un programme informatique ou de données informatiques

(1) Les États adoptent les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales le fait de modifier intentionnellement, directement ou indirectement, sans autorisation, le fonctionnement d'un système informatique par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.

(2) Il y a modification d'un programme informatique ou de données informatiques dans les cas suivants :

a) Un programme ou des données contenues dans l'ordinateur sont endommagés, altérés ou effacés sans autorisation ;

b) Un programme ou des données sont ajoutés à un programme ou à un enregistrement électronique conservé dans le système informatique, ou y sont effacés ;

c) Un acte est commis qui nuit au fonctionnement normal d'un ordinateur ou d'un programme qui s'y trouve, ou qui cause une détérioration du fonctionnement normal.

(3) Il est indifférent que la modification ou l'interférence non autorisée soit permanente ou temporaire, ou que l'intention est qu'elle soit permanente ou temporaire.

10. Interférence dans les systèmes informatiques

(1) Les États adoptent les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, lorsque l'acte est commis intentionnellement, sans autorisation et sans excuse ou

justification légitime, le fait d'interférer dans le fonctionnement d'un système informatique ou de gêner une personne qui utilise ou fait fonctionner un ordinateur de manière licite.

(2) L'interférence ou l'entrave comprend, sans s'y limiter :
   a) Le fait d'empêcher le fonctionnement d'un système informatique par quelque moyen que ce soit ;
   b) Le fait de causer des interférences électriques, électroniques ou électromagnétiques dans un système informatique ;
   c) Le fait de provoquer des attaques par déni de service ;
   d) Le fait de causer l'altération de sites web ;
   e) Le fait de corrompre un système informatique par quelque moyen que ce soit, y compris par l'utilisation de logiciels malveillants et de virus.

(3) Il est indifférent que l'interférence non autorisée soit permanente ou temporaire, ou que l'intention est qu'elle soit permanente ou temporaire.

11. Pornographie mettant en scène des enfants

(1) Les États adoptent les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, en relation avec la protection des enfants, les actes suivants lorsqu'ils sont commis intentionnellement ou par négligence :
   a) Publication de matériel pornographique mettant en scène des enfants par le moyen d'un système informatique ;
   b) Diffusion de matériel pornographique mettant en scène des enfants par le moyen d'un système informatique ;
   c) Production de matériel pornographique mettant en scène des enfants en vue de sa publication ou de sa diffusion par le moyen d'un système informatique ;
   d) Détention de matériel pornographique mettant en scène des enfants dans un système informatique ou sur un support de stockage de données informatiques.

(2) Le matériel pornographique mettant en scène des enfants comprend le matériel qui représente visuellement :
   a) Un enfant se livrant à un comportement sexuellement explicite ;
   b) b) Une personne qui apparaît comme un enfant se livrant à un comportement sexuellement explicite ;

c) Des images représentant un enfant se livrant à un comportement sexuellement explicite ;
d) Des images non autorisées d'enfants nus.

(3) Par « enfant », on entend une personne âgée de moins de 18 ans ou autrement définie comme tel dans la législation nationale.
(4) Par « publier », on entend le fait de transmettre, de diffuser, de distribuer, de livrer ou d'exposer.
(5) Par « distribuer », on entend le fait d'échanger, de troquer, de prêter, de vendre ou de proposer à la vente, de mettre en location ou de proposer à la location, de proposer de toute autre manière ou de mettre à disposition de quelque manière que ce soit.
(6) Par « possession », on entend le fait d'avoir en sa possession, sous sa garde ou sous son contrôle.
(7) Par « produire », on entend le fait d'imprimer, de photographier, de copier ou de fabriquer de toute autre manière.

12. Contenu trompeur ciblant les enfants

Les États peuvent adopter les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales l'utilisation de mots ou d'images numériques trompeurs sur l'Internet ciblant les enfants et visant à mettre en confiance les enfants pour permettre la commission d'actes criminels, y compris la création de noms de domaine sur l'Internet pour tromper les mineurs et permettre la commission d'actes qui peuvent être considérés comme criminels au regard de la législation nationale.

13. Infractions liées à l'identité

Les États peuvent adopter les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales les actes suivants lorsqu'ils sont commis intentionnellement :

a) Le fait d'assumer l'identité d'une autre personne (vivante ou décédée, physique ou morale) par le moyen d'un système informatique ou par l'accès à ce système ou en relation avec d'autres normes énoncées dans la législation nationale ;
b) Le fait d'obtenir, de divulguer ou de se procurer les données à caractère personnel ou l'identifiant personnel ou humain d'une personne vivante ou décédée afin d'assumer l'identité de cette

personne dans l'intention de commettre une infraction pénale ou d'en faciliter la commission par le moyen d'un système informatique ou par l'accès à ce système.

14. Attaques par déni de service

Les États peuvent adopter les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales les actes suivants lorsqu'ils sont commis intentionnellement :

a) Le fait d'inonder de trafic la bande passante ou les ressources d'un système informatique ou de serveurs ciblés, empêchant ainsi les utilisateurs légitimes d'accéder aux informations ou aux services ;

b) Le fait de compromettre plusieurs ordinateurs présentant des failles de sécurité et d'en prendre le contrôle afin de les utiliser pour commettre l'acte décrit à l'alinéa a) ci-dessus.

15. Rançongiciel et cyberextorsion

Les États peuvent adopter les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales l'installation intentionnelle et secrète de logiciels malveillants ou de virus sur un système informatique, empêchant ainsi l'accès à ce dernier, suivie d'une demande de paiement d'une rançon en échange du rétablissement de l'accès au système informatique ou de la non-publication ou de la non-divulgation des données contenues dans le système informatique.

16. Incitation frauduleuse

Les États peuvent adopter les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales l'envoi intentionnel et frauduleux par voie électronique de messages non demandés ou non sollicités, ou la création de sites web ou d'hyperliens Internet trompeurs, afin d'obtenir des informations personnelles ou financières de victimes sans méfiance, dans l'intention d'utiliser ces informations à des fins frauduleuses ou à d'autres fins présentant un intérêt pour l'auteur de l'infraction.

17. Violation en ligne des droits d'auteur et des droits connexes

Les États peuvent adopter les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales la violation en ligne des droits d'auteur, y compris en précisant la responsabilité des intermédiaires lorsqu'ils agissent en dehors du champ d'application des clauses d'immunité.

18. Cybersquattage

Les États peuvent adopter les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales le fait de prendre ou d'utiliser intentionnellement un nom, une raison sociale, une marque, un nom de domaine ou tout autre mot ou expression déposé, détenu ou utilisé par une autre personne sur l'Internet ou tout autre réseau informatique, sans autorisation ni droit et dans l'intention d'en tirer profit.

19. Obtention illégale de données à caractère personnel

(1) Les États peuvent adopter les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales tout acte commis par une personne sciemment ou de propos délibéré dans l'intention :

a) D'obtenir ou de divulguer des données à caractère personnel sans le consentement d'un responsable du contrôle des données ;

b) D'obtenir la divulgation de données à caractère personnel à une autre personne sans le consentement d'un responsable du contrôle des données ;

c) De conserver des données à caractère personnel sans le consentement de la personne qui était le responsable du contrôle des données au moment où celles-ci ont été obtenues ;

d) De vendre ou d'offrir à la vente des données à caractère personnel obtenues dans les circonstances mentionnées dans le présent paragraphe.

(2) Le paragraphe 1 ci-dessus peut ne pas s'appliquer, si l'obtention, la divulgation, l'acquisition ou la conservation de données à caractère personnel :

a) Était nécessaire aux fins de prévenir ou de détecter des infractions ;
b) Était requise ou autorisée par la promulgation d'une loi, d'une règle ou par l'ordonnance d'une cour ou d'un tribunal ;
c) Était justifiée comme étant conforme à l'intérêt public.

PARTIE III : Procédure pénale et détermination de la responsabilité

20. Intention criminelle

Les États adoptent les mesures législatives et autres nécessaires pour établir l'intention, lorsqu'une personne, au moyen de tout ou partie d'un ordinateur, est considérée avoir l'intention de commettre ou de contribuer à commettre une infraction établie dans la législation nationale et résultant de l'utilisation d'un système informatique ou d'une intervention dans un tel système.

21. Négligence criminelle

Les États adoptent les mesures législatives et autres nécessaires pour établir la négligence criminelle, lorsqu'une personne, au moyen de tout ou partie d'un ordinateur, est considérée avoir causé un événement par négligence, si, sans avoir l'intention de causer l'événement, la personne le cause par une action volontaire résultant de l'utilisation d'un système informatique ou d'une intervention dans un tel système, sans la prudence qui serait raisonnablement nécessaire dans de telles circonstances.

22. Tentative, complicité et entente

(1) Les États adoptent les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, lorsqu'elle est commise intentionnellement, la tentative de commettre une cyberinfraction établie dans la législation nationale.

(2) Les États peuvent adopter les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, lorsqu'elle est commise intentionnellement, la complicité dans la commission de toute infraction établie comme infraction cybercriminelle conformément à la législation nationale.

(3) Les États peuvent adopter les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, lorsqu'elle est commise intentionnellement, l'entente en vue de commettre toute infraction établie en infraction cybercriminelle dans la

législation nationale, que le support utilisé soit en tout ou partie activé par ordinateur.

23. Responsabilité des personnes

(1) Les États veillent au respect et à l'application effective de la législation sur la cybersécurité en prononçant des verdicts de culpabilité, en imposant des peines et des mesures punitives pour la commission des infractions énoncées dans la législation.

(2) Les États peuvent adopter les mesures législatives et autres qui se révèlent nécessaires, en conformité avec leur droit interne et sous réserve de celui-ci, pour faire en sorte que les personnes morales autres que l'État et les institutions publiques puissent être tenues pour responsables des infractions établies dans la législation nationale sur la cybersécurité qui sont commises pour leur compte par leurs organes ou représentants.

(3) Cette responsabilité peut être pénale, civile ou administrative et n'exclut pas la responsabilité pénale des personnes physiques qui ont commis ces infractions, et est sans préjudice de la responsabilité pénale de ces personnes physiques.

(4) Les États tiennent les personnes physiques et morales pour responsables de la commission des infractions établies conformément à leurs lois nationales sur la cybersécurité en appliquant des sanctions efficaces, nécessaires et proportionnées.

24. Infractions commises par des sociétés

(1) Les États peuvent veiller à ce que, dans le cadre d'une procédure pour infraction à la législation nationale sur la cybersécurité, il soit prouvé que la société se trouvait dans un état d'esprit particulier en relation avec un acte particulier, lorsqu'il existe des éléments de preuve établissant :

a) Qu'un dirigeant, un employé ou un agent de la société a agi dans le cadre de ses pouvoirs réels ou apparents ;

b) Que le dirigeant, l'employé ou l'agent se trouvait dans cet état d'esprit.

(2) Lorsqu'une société commet une infraction qualifiée d'infraction cybercriminelle dans la législation nationale, une personne est

tenue pour responsable de la même infraction que la société si cette personne est :

a) Soit un dirigeant de la société ou un membre de la société (dans le cas où les affaires de la société sont gérées par ses membres) ;

b) Soit une personne impliquée dans la gestion de la société et en mesure d'influencer le comportement de la société en relation avec la commission de l'infraction.

(3) Lorsqu'une société commet une infraction qualifiée d'infraction cybercriminelle dans la législation nationale, une personne est tenue pour responsable de la même infraction que la société si cette personne :

a) Soit a consenti à la commission de l'infraction, a été de connivence ou a conspiré avec d'autres pour commettre l'infraction;

b) Soit a été, de toute autre manière, par action ou par omission, intentionnellement partie prenante à la commission de l'infraction par la société ;

c) Soit savait ou devait raisonnablement savoir que l'infraction commise par la société allait être ou était en train d'être commise, et n'a pas pris toutes les mesures raisonnables pour empêcher ou faire cesser la commission de cette infraction.

PARTIE IV : Procédure pénale et application de la loi

25. Pouvoirs en matière de procédure et de fond

Les États mettent en place et maintiennent un système national de justice pénale efficace et fondé sur l'état de droit, un système capable d'assurer que toute personne poursuivie pour des infractions visées dans la législation nationale sur la cybersécurité est traduite en justice, tout en veillant à la pleine protection des droits de l'homme et des libertés fondamentales conformément à la Charte africaine des droits de l'homme et des peuples et à d'autres instruments internationaux relatifs aux droits de l'homme.

26. Champ d'application des mesures procédurales

(1) Les États adoptent les mesures législatives et autres qui se révèlent nécessaires pour établir les pouvoirs et procédures requis aux fins d'enquêtes ou de procédures pénales spécifiques.

(2) Les États appliquent ces pouvoirs et procédures :

a) Aux infractions établies dans leur législation nationale en tant qu'infractions cybercriminelles ;

b) À la collecte des éléments de preuve sous forme électronique ou numérique d'une infraction pénale établie dans leur législation nationale en tant qu'infraction cybercriminelle.

27. Conditions et garanties

Les États veillent à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et des procédures soient soumis aux conditions et garanties prévues dans leur droit interne, qui doivent assurer une protection totale des droits de l'homme et des libertés fondamentales, conformément aux normes internationales et régionales en matière de droits de l'homme, y compris les droits découlant des obligations que les États peuvent avoir souscrites en application de la Charte africaine des droits de l'homme et des peuples.

28. Conservation et divulgation des données informatiques

Sous réserve des normes et des considérations juridiques internes appropriées, les États peuvent adopter les mesures qui se révèlent nécessaires pour permettre à leurs autorités compétentes d'ordonner la conservation et la divulgation de données qui ont été stockées au moyen d'un programme ou d'un système informatique, en particulier lorsque ces données sont pertinentes à des fins d'enquête, d'application de la loi ou de procédures judiciaires.

29. Production et obtention de données informatiques

Les États adoptent les mesures qui se révèlent nécessaires pour conférer à leurs autorités compétentes le pouvoir d'ordonner ce qui suit :

a) La soumission par des personnes se trouvant sur leur territoire de données informatiques spécifiques qui sont en la possession ou sous le contrôle de ces personnes ;

b) La soumission par un fournisseur de services offrant ses services sur leur territoire de données ou d'informations relatives à ses services ou aux utilisateurs de ses services qui sont en sa possession ou sous son contrôle.

30. Perquisition et saisie de données informatiques stockées

(1) Les États adoptent les mesures qui se révèlent nécessaires pour conférer à leurs autorités compétentes le pouvoir de perquisition ou d'accès concernant :

a) Un système informatique ou une partie de celui-ci ainsi que les données informatiques qui y sont stockées ;

b) Un support de stockage de données informatiques permettant de stocker des données informatiques sur leur territoire.

(2) Les États adoptent les mesures qui se révèlent nécessaires pour veiller à ce que, lorsque leurs autorités procèdent à une perquisition concernant un système informatique spécifique ou accèdent d'une façon similaire à ce système ou à une partie de celui-ci, et qu'elles ont des raisons de penser que les données recherchées se trouvent ou sont stockées dans un autre système informatique, ou sont connectées à un autre système informatique sur leur territoire ou en font partie, et que ces données sont légalement accessibles

à partir du système initial ou disponibles pour celui-ci, lesdites autorités soient investies du pouvoir, dans le respect des normes légales, d'étendre la perquisition à l'autre système informatique ou d'avoir accès à celui-ci.

(3) Les États adoptent les mesures législatives et autres qui se révèlent nécessaires pour conférer à leurs autorités compétentes le pouvoir de saisir les données informatiques consultées ou d'en prendre possession, au besoin. Ces mesures comprennent le pouvoir de :

a) Saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci ou un support de stockage de données informatiques ;

b) Réaliser et conserver une copie de ces données informatiques ;

c) Préserver l'intégrité des données informatiques stockées pertinentes ;

d) Rendre inaccessibles ou de supprimer les données informatiques contenues dans le système informatique consulté.

31. Mandats autorisés

(1) Les États autorisent les autorités compétentes, sur demande adressée à un tribunal compétent de la juridiction appropriée, à délivrer un mandat d'interception pour faciliter la demande, la collecte et/ou l'enregistrement de données informatiques, lorsque ces données spécifiées sont nécessaires à l'application de la loi, à une enquête criminelle ou à une procédure pénale.

(2) Les États prévoient que, s'ils sont convaincus, sur la base d'une demande adressée à une juridiction compétente par un agent des services de détection et de répression, qu'un élément spécifié de données informatiques est raisonnablement nécessaire aux fins d'une enquête criminelle ou d'une procédure pénale, le tribunal peut ordonner :

a) Qu'une personne ayant sous son contrôle un système informatique produise les données informatiques spécifiées ;

b) Qu'un fournisseur de services Internet produise les données informatiques spécifiées ou produise des informations sur les personnes qui s'abonnent à ces services ou les utilisent d'une autre manière.

32. Blocage, filtrage et suppression des contenus illicites

En tenant compte des principes de légitimité, de nécessité et de proportionnalité, les États peuvent adopter les mesures législatives et autres qui se révèlent nécessaires pour conférer aux autorités compétentes des pouvoirs de blocage, de filtrage et de suppression de contenus illicites sur décision d'un tribunal, sur la base de certains motifs juridiques précis, dans le but d'assurer la cybersécurité ou le respect des droits des citoyens en relation avec des activités de cybercriminalité.

33. Champ d'application

(1) Les États adoptent les mesures qui se révèlent nécessaires pour exercer leur compétence pénale à l'égard des infractions informatiques établies conformément à leur droit interne, si l'une des deux conditions suivantes est remplie :

a) L'infraction est commise sur le territoire de l'État concerné ;

b) L'infraction est commise à bord d'un navire battant pavillon de l'État concerné ou d'un aéronef immatriculé selon les lois de cet État au moment où l'infraction est commise ;

c) L'infraction est commise par l'un des citoyens de l'État concerné, si l'infraction est punissable en vertu de la loi nationale sur la cybercriminalité à l'endroit où elle a été commise, ou si l'infraction est commise en dehors de la juridiction territoriale de tout État.

(2) Les États peuvent aussi exercer leur compétence à l'égard d'une telle infraction lorsque :

a) L'infraction est commise à l'encontre d'un citoyen de l'État concerné ;

b) L'infraction est commise par un citoyen de l'État concerné ou par un apatride qui a sa résidence habituelle sur le territoire dudit État.

(3) Les États peuvent également adopter les mesures qui se révèlent nécessaires pour exercer leur compétence à l'égard des infractions visées par leur législation nationale sur la cybersécurité, lorsque l'auteur présumé de l'infraction est présent sur le territoire de l'État concerné et que celui-ci, à la suite d'une demande d'extradition, n'extrade pas l'auteur de l'infraction en raison de la nationalité de celui-ci.

(4) En tenant compte du principe de la double incrimination, les États qui ont l'intention d'exercer leur compétence à l'égard des infractions cybercriminelles établies dans leur législation nationale sur la cybersécurité se consultent, dans les cas où un ou plusieurs États ont déjà initié une enquête, des poursuites ou une procédure judiciaire concernant un même comportement, sans préjudice des normes du droit international général, en vue de coordonner leurs actions en ce qui concerne l'exercice de leur compétence.

PARTIE V : Coopération en matière de cybersécurité

34. Coopération et entraide judiciaire

(1) Les États élaborent des politiques appropriées pour coordonner l'échange d'informations sur la cybersécurité entre les secteurs de sécurité concernés, afin d'accroître le volume, la rapidité et la qualité de l'échange d'informations sur les cybermenaces, de manière à ce que les États puissent mieux se protéger et se défendre contre les cybermenaces.

(2) Les États élaborent des politiques appropriées pour coordonner les programmes volontaires d'échange d'informations entre les entités des secteurs public et privé, en vue d'améliorer l'échange d'informations classifiées sur les cybermenaces et d'informations techniques entre les services de détection et de répression et les autres parties prenantes fournisseurs de services de cybersécurité.

35. Mesures visant à renforcer la coopération en matière d'application de la loi

(1) Les États peuvent prendre des mesures appropriées pour assurer la coopération en matière d'application de la loi. Les États coopèrent étroitement entre eux, conformément à leurs systèmes juridiques et administratifs nationaux respectifs, pour renforcer l'efficacité des mesures d'application de la loi visant à lutter contre les infractions cybercriminelles visées par leur législation nationale sur la cybersécurité. Les États adoptent notamment des mesures efficaces visant à :

a) Améliorer et, si nécessaire, à établir des canaux de communication entre leurs autorités, organismes et services compétents, afin de faciliter l'échange sécurisé et rapide d'informations concernant tous les aspects des infractions visées par leur législation nationale sur la cybersécurité ;

b) Coopérer avec d'autres États pour mener des enquêtes sur les infractions visées par leur législation nationale sur la cybersécurité, y compris pour ce qui concerne :
   i) L'identité des personnes soupçonnées d'être impliquées dans ces infractions, l'endroit où elles se trouvent et leurs activités, ou l'endroit où se trouvent d'autres personnes concernées ;
   ii) Le mouvement des produits du crime ou des biens provenant de la commission de ces infractions ;
   iii) Le mouvement des biens, des matériels ou d'autres instruments utilisés ou destinés à être utilisés dans la commission de ces infractions ;

c) Fournir, lorsqu'il y a lieu, les informations nécessaires à des fins d'analyse ou d'enquête ;

d) Faciliter une coordination efficace entre leurs autorités, organismes et services compétents et favoriser l'échange de personnel et d'experts, sous réserve de l'existence d'accords ou d'arrangements bilatéraux ou multilatéraux entre les États concernés ;

e) Échanger des informations et coordonner les mesures administratives et autres prises, comme il convient, pour détecter au plus tôt les infractions visées par leur législation nationale sur la cybersécurité.

(2) Afin d'assurer la cybersécurité, les États peuvent envisager de conclure des accords ou des arrangements bilatéraux ou multilatéraux prévoyant une coopération directe entre leurs services de détection et de répression et, lorsque de tels accords ou arrangements existent déjà, de les modifier pour y intégrer des objectifs de cybersécurité.

36. Coopération internationale

(1) La mise en œuvre de la législation nationale sur la cybersécurité doit se faire en liaison avec les dispositions établies par les accords et mécanismes internationaux et en tenant compte de celles-ci.

(2) Les États mettent en place des régimes prévoyant des mécanismes pouvant servir de point de contact unique pour les incidents et la résolution de ces incidents par des mesures mises en œuvre

en coopération au niveau international entre gouvernements, services de détection et de répression, et secteurs.

(3) Les États utilisent les moyens existants de la coopération internationale en vue de faire face aux cybermenaces, d'améliorer la cybersécurité et de stimuler le dialogue entre les parties prenantes. Ces moyens peuvent être internationaux, régionaux, intergouvernementaux ou fondés sur des partenariats public-privé.

37. Partenariats public-privé

(1) Les États élaborent des modèles de collaboration multipartite pour les partenariats public-privé en vue de la surveillance, de la prévention et de l'atténuation de la cybersécurité et pour renforcer la résilience et la confiance en matière de cybersécurité dans la région africaine.

(2) Pour promouvoir les partenariats public-privé, les États peuvent créer des entités chargées de définir pour le secteur privé des normes de cybersécurité relatives à la sécurité et au bien-être, y compris des organismes de surveillance et de mise en œuvre, tels qu'un comité national de cybersécurité, pour administrer la mise en œuvre des partenariats public-privé.

PARTIE VI : Gestion de la cybersécurité

38. Infrastructures critiques

(1) Les États veillent à ce que la législation nationale sur la cybersécurité impose des obligations strictes en matière d'entretien et de protection des réseaux informatiques qui, autrement, pourraient causer des perturbations, des destructions et des interférences importantes dans les infrastructures critiques et les systèmes d'information.

(2) Les États recensent les infrastructures critiques les plus exposées aux cybermenaces.

(3) Les États utilisent une approche fondée sur les risques pour recenser les infrastructures critiques dans lesquelles un incident de cybersécurité pourrait raisonnablement avoir des effets catastrophiques au niveau régional ou national sur la santé publique ou la sécurité publique, la sécurité économique et financière ou la sécurité nationale.

(4) Chaque État veille à ce que sa législation nationale sur la cybersécurité énumère et définisse ce qui sera considéré comme une « infrastructure critique » et établisse un cadre réglementaire pour l'entretien et la protection de cette « infrastructure critique ».

39. Intervention en cas d'urgence informatique

(1) Les États mettent en place des organismes et des équipes spécialisés dans la gestion de la cybersécurité et élaborent des plans d'intervention d'urgence.

(2) Les États peuvent également ordonner la mise en place d'équipes nationales et sectorielles chargées d'intervenir dans les situations d'urgence concernant les réseaux informatiques et de coordonner ces interventions à l'échelle nationale et/ou sectorielle. Les équipes nationales et sectorielles travailleront en coordination pour intervenir en cas de cyberincidents et de cybermenaces et pour atténuer les effets de ces incidents et menaces.

(3) Les États peuvent confier aux équipes nationales et sectorielles chargées des interventions d'urgence le soin d'établir un registre ou une base de données des cyberincidents dans leurs juridictions

respectives, aux fins de collecter et de compiler des données sur les cyberincidents, d'analyser ces incidents et d'exercer des fonctions de supervision de la cybersécurité.

40. Points de contact pour la cybersécurité

Pour assurer une coopération opérationnelle rapide en matière de cybersécurité dans la région africaine, les États prennent les mesures appropriées pour désigner un point de contact, doté d'un personnel formé pour faciliter le fonctionnement du réseau, disponible vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer la fourniture d'une assistance immédiate aux fins d'enquêtes ou de procédures relatives aux infractions établies en tant qu'infractions cybercriminelles dans la législation nationale, ou pour la collecte d'éléments de preuve électroniques nécessaires à des fins d'enquête ou d'application de la loi.

41. Stratégies et cadre de cybersécurité

(1) Les États conçoivent et développent des stratégies et des cadres appropriés de cybersécurité pour identifier, évaluer, surveiller, prévenir et atténuer les cybermenaces dans leurs juridictions respectives.

(2) La stratégie et le cadre de cybersécurité comprennent un ensemble de normes, de méthodes, de procédures et de processus qui harmonisent les approches en matière de politiques, d'opérations et de technologies pour faire face aux cybermenaces dans la juridiction de l'État concerné.

(3) La stratégie de cybersécurité intègre les normes et les meilleures pratiques mondiales et régionales faisant l'objet d'un consensus. Dans la stratégie de cybersécurité, l'accent est mis sur le recensement des normes et lignes directrices intersectorielles en matière de sécurité, qui sont applicables à la cybersécurité.

(4) La stratégie de cybersécurité identifie également les domaines à améliorer pour permettre l'innovation technique ainsi que le suivi et la mesure des normes d'organisation et elle contient des orientations qui permettent aux secteurs nationaux de la cybersécurité de fournir des services conformes aux normes, méthodes, procédures et processus mis au point pour faire face aux cybermenaces.

42. Mise en place d'une autorité centrale pour la réglementation de la cybersécurité

Les États veillent à ce que leur législation nationale sur la cybersécurité comprenne des dispositions établissant l'autorité ou les autorités chargées de réglementer les mesures de cybersécurité sur leur territoire et déterminant le champ d'application et les pouvoirs de cette autorité ou de ces autorités. L'autorité nationale en matière de cybersécurité est chargée des tâches suivantes :

a) Suivre les tendances en matière de cybersécurité, telles que les vulnérabilités, la gestion des risques, les pratiques de gouvernance et les violations pouvant affecter le cyberespace national ;
b) Effectuer des analyses stratégiques à long terme des cybermenaces et des cyberincidents, afin d'identifier les nouvelles tendances et de contribuer à la prévention des incidents ;
c) Interagir avec les services gouvernementaux qui interviennent en cas de cyberincidents et apporter un appui à ces services ;
d) Promouvoir au sujet de la cybersécurité la communication entre les secteurs et les départements s'occupant de cybersécurité ;
e) Conseiller les institutions, organes, bureaux et organismes nationaux sur les besoins et les priorités en matière de recherche sur la cybersécurité en vue d'interventions efficaces face aux risques et cybermenaces actuels et émergents ;
f) Superviser l'élaboration d'orientations réglementaires pour des interventions de cybersécurité, afin d'aider l'État à poursuivre l'atténuation des cybermenaces ;
g) Soutenir l'État dans la mise en œuvre des lois, politiques et stratégies nationales en matière de cybersécurité et contribuer aux efforts de mise en œuvre tendant à la ratification et à l'adoption de traités régionaux et internationaux dans le domaine de la cybersécurité ;
h) Collaborer avec les parties prenantes nationales et internationales dans les efforts de gestion et d'évaluation de la cybersécurité ;
i) Sensibiliser le public aux risques liés à la cybersécurité et donner des conseils aux utilisateurs individuels, aux organisations et aux entreprises sur les bonnes pratiques, notamment en matière de cyberhygiène et de cyberculture.

43. Cybersécurité et assistance et soutien aux victimes

(1) Dans le cadre de l'obligation qui leur incombe de surveiller et de prévenir les menaces liées à la cybersécurité et de veiller au bien-être des citoyens, les États peuvent mettre en place des systèmes d'appui pour conseiller, soutenir et protéger les victimes d'infractions établies dans la législation nationale sur la cybersécurité, notamment en créant à cet effet des organismes qui seront chargés d'apporter un soutien aux victimes.

(2) Chaque État prend les mesures appropriées, dans la mesure de ses moyens, pour fournir une assistance et une protection aux victimes d'infractions visées dans la législation nationale sur la cybersécurité, notamment en cas de menace de représailles ou d'intimidation, en accordant une attention particulière aux groupes les plus vulnérables de la société.

(3) Chaque État établit des procédures appropriées pour donner accès à l'indemnisation et à la restitution aux victimes d'infractions visées dans la législation nationale sur la cybersécurité.

(4) Chaque État, sous réserve de ses lois nationales sur la cybersécurité, permet que les vues et préoccupations des victimes soient présentées et examinées aux stades appropriés de la procédure pénale engagée contre l'accusé, d'une manière qui ne soit pas préjudiciable aux droits de celui-ci et qui soit compatible avec la protection des droits que lui reconnaît la loi.

44. Éducation et formation

(1) Il est rappelé aux États que les régimes de cybersécurité imposent aux gouvernements, au secteur privé, aux institutions et aux citoyens des obligations importantes en matière d'entretien et de protection des systèmes ; par conséquent, l'importance de la fonction d'éducation et de sensibilisation du public doit être prise en considération de la même façon que la fonction importante de la réglementation.

(2) Chaque État adopte des mesures visant à renforcer les capacités en dispensant aux différentes parties prenantes des formations portant sur tous les domaines de la cybersécurité.

(3) Les États encouragent la formation technique des professionnels des technologies de l'information et des communications, à l'intérieur et à l'extérieur des organismes gouvernementaux, par la

certification et la normalisation de la formation, le classement par catégories des qualifications professionnelles et l'élaboration et la diffusion de matériel didactique, en fonction des besoins.

(4) Dans le cadre du plan de promotion de l'éducation et de la formation du public, les États peuvent :

a) Élaborer et mettre en œuvre des programmes et des initiatives visant à sensibiliser, éduquer, former les citoyens sur les questions de cybersécurité et diffuser des informations à leur intention sur ces questions ;

b) Encourager le développement d'une culture de la cybersécurité dans les entreprises ;

c) Favoriser l'implication de la société civile ;

d) Lancer un programme national complet et détaillé dans les établissements d'enseignement pour les étudiants.

(5) Les États, dans le cadre de l'obligation qui leur incombe de surveiller et de prévenir les menaces liées à la cybersécurité et de veiller au bien-être des citoyens, peuvent mettre en place des systèmes de soutien pour conseiller les groupes vulnérables de la société sur les questions de cybersécurité.

45. Recherche-développement en matière de cybersécurité

(1) Les États apportent un appui aux programmes de recherche-développement visant à guider l'orientation générale de la cybersécurité nationale et le développement des technologies de l'information et des systèmes de mise en réseau pour atteindre les objectifs de cybersécurité, notamment en vue :

a) De concevoir et de construire des systèmes complexes à forte composante logicielle qui favorisent la cybersécurité ;

b) De mettre en place de nouveaux protocoles pour assurer une sécurité solide sur l'Internet ;

c) De Développer et de concevoir des solutions de cybersécurité au niveau local ;

d) D'élaborer des solutions qui protègent les infrastructures nationales critiques ;

e) De protéger la vie privée tout en améliorant la sécurité, y compris la protection de l'identité des personnes, des informations les concernant et leurs transactions légales

lorsqu'elles sont stockées dans des systèmes distribués ou transmises sur des réseaux ;

f) De lutter contre les cybermenaces internes et externes ;

g) D'améliorer l'éducation des consommateurs et leur culture numérique pour prendre en compte les facteurs humains qui contribuent à la cybersécurité ;

h) De protéger les informations traitées, transmises ou stockées à l'aide de l'informatique en nuage ou transmises par des services sans fil ;

i) D'atteindre d'autres objectifs fixés avec l'aide des parties prenantes, notamment les laboratoires, l'industrie et les universités nationaux, comme il convient.

46. Modifications de la législation nationale

Les États adoptent également les mesures nécessaires pour faciliter l'examen et la modification des lois sur la cybersécurité, afin de permettre des interventions souples et appropriées dans les cas de cybermenaces existantes et futures.