TechForGood Initiative
https//tfg-initiative.com

e-RIGHTS
Enhancing Digital Rights in Nigeria

AVOCATS SANS FRONTIÈRES FRANCE

Note d'orientation

Réformer Cybersécurité Réglementation au Nigéria

Juillet 2025

Iheanyi Nwankwo, Ph. D.
Angela Uwandu Uzoma - Iwuchukwu

Résumé exécutif

La dépendance de la société aux technologies de l'information et de la communication rend indispensables des mesures de cybersécurité rigoureuses. Les gouvernements du monde entier adoptent diverses réglementations, notamment des lois sur la cybercriminalité, la cybersécurité, la protection des données, la cybersécurité et la cyberguerre, pour contrer la montée des menaces numériques.

Malgré la mise en place de plusieurs mesures réglementaires, le paysage de la cybersécurité au Nigéria est en proie à certains défis : une loi sur la cybercriminalité obsolète et inadéquate ainsi que son utilisation abusive perçue par les autorités chargées de l'application de la loi, l'absence d'une loi complète (horizontale) sur la cybersécurité, une approche législative réactive plutôt que proactive, un cadre de coordination fragmenté et complexe, une faible capacité institutionnelle et une pénurie de professionnels qualifiés en cybersécurité, ainsi qu'une faible sensibilisation du public à la cybersécurité.

Pour relever ces défis, cette note d'orientation recommande une réforme globale du cadre de cybersécurité du Nigéria. Les principales recommandations sont les suivantes :

- Réalisation d'une étude approfondie pour éclairer la modification de la loi sur la cybercriminalité afin de lutter contre les menaces modernes telles que les deepfakes et les ransomwares.
- Adopter une loi globale (horizontale) sur la cybersécurité afin de normaliser les obligations dans tous les secteurs critiques.
- Inclure des mécanismes de révision périodique dans la future législation sur la cybersécurité pour garantir que les lois restent à jour.
- Aborder les questions de soutien aux victimes de cybercriminalité.
- Donner la priorité à l'engagement des parties prenantes et à une plus grande transparence dans les processus législatifs.
- Créer une nouvelle autorité nationale centralisée pour la cybersécurité afin de rationaliser l'application et la coordination, en retirant cette responsabilité à l'ONSA.
- Intégrer la Convention de Budapest sur la cybercriminalité pour renforcer la coopération internationale.
- Mettre en place un cadre national de cyberdéfense s'appuyant sur l'expertise citoyenne.
- Intensifier les initiatives nationales de renforcement des compétences et les campagnes de sensibilisation du public pour favoriser une culture de cyberhygiène.

Ces réformes sont cruciales pour renforcer la sécurité nationale, la stabilité économique et la confiance du public à l'ère numérique du Nigéria.

À propos des auteurs

Le Dr Iheanyi Nwankwo, titulaire d'un doctorat, est juriste et fondateur de l'initiative Tech For Good. Son expertise porte sur le droit des technologies de l'information et de la propriété intellectuelle, ainsi que sur les aspects juridiques de la protection des données et de la cybersécurité.

Il peut être contacté à l'adresse nwankwo@tfg-initiative.com

Angela Uwandu Uzoma-Iwuchukwu est directrice nationale d'Avocats Sans Frontières France au Nigéria et cheffe de projet du projet eRIGHTS, financé par l'Union européenne et l'UNESCO, visant à renforcer les droits numériques au Nigéria. Elle est experte en droit international et en droits de l'homme, notamment en droits numériques.

Elle peut être contactée à : office.nigeria@avocatssansfrontieres-france.org

Introduction

La société moderne dépend fortement des technologies de l'information et de la communication (TIC), des systèmes qu'elles englobent et des infrastructures critiques qu'elles soutiennent. Leur protection nécessite une approche globale, utilisant un large éventail d'outils. Ces outils comprennent des cadres et des méthodologies couvrant les aspects techniques, organisationnels et réglementaires. Les gouvernements du monde entier ont soutenu ces initiatives par diverses mesures réglementaires, allant de l'imposition de principes fondamentaux de conception de sécurité et de bonnes pratiques aux certifications sectorielles validant l'expertise et les produits en matière de cybersécurité. Tous ces efforts visent à endiguer la vague de cybermenaces.

Au fil des ans, une multitude de lois axées sur la cybersécurité ont émergé, tant au niveau national qu'international. Ces lois visent à protéger non seulement les actifs numériques, mais aussi les individus qui interagissent dans le cyberespace. Bien que n'étant pas toujours explicitement qualifiées de « lois sur la cybersécurité », il existe un large consensus sur le fait que la réponse réglementaire aux cybermenaces englobe divers types de législation, notamment des lois générales, des lois sectorielles et le droit pénal.

Bien qu'il soit difficile d'ajouter des classifications strictes à ces lois, une démarcation fonctionnelle pourrait les placer dans les rubriques suivantes :

1. Lois sur la cybercriminalité : Ces lois interdisent et punissent des actions spécifiques commises à l'aide d'ordinateurs ou d'Internet, ou contre des systèmes d'information, telles que l'interception illégale de données sur un réseau public, la fraude ou les escroqueries en ligne, la cyberintimidation, les attaques par rançongiciel, entre autres.
Elles définissent les infractions et décrivent les procédures d'enquête et de poursuite des auteurs. Ces lois sont complétées par des règles de preuve applicables aux documents numériques et des pouvoirs spécifiques en matière d'application de la loi.

2. Lois sur la cybersécurité : Ces réglementations visent à protéger les actifs informatiques (infrastructures publiques et privées) contre les atteintes à leur confidentialité, leur intégrité et leur disponibilité. Elles imposent aux personnes manipulant ces actifs informationnels des exigences de mise en œuvre de mesures proactives et réactives spécifiques visant à protéger le système. Au cœur de ces lois se trouve la nécessité de garantir la résilience et la

Intégrité des systèmes numériques. Parmi ces exigences figurent notamment les mesures de gestion des risques ex ante, les notifications de violation de données et les protocoles de réponse aux incidents.

3. Lois sur la protection des données et la confidentialité : Ces lois régissent le traitement des données personnelles et visent à offrir aux personnes concernées des contrôles et des droits spécifiques contre ceux qui traitent leurs données. La sécurité des données fait partie intégrante de ces lois, exigeant des responsables du traitement et des sous-traitants qu'ils mettent en œuvre des mesures techniques et organisationnelles appropriées pour protéger les données personnelles dont ils ont la charge.

4. Lois sur la cybersécurité : Alors que des personnes de tous âges et de tous niveaux de connaissances, y compris des populations vulnérables comme les enfants, utilisent des ressources informatiques au quotidien, il est devenu nécessaire que la loi se concentre sur leur protection. Les lois sur la cybersécurité s'inscrivent dans le prolongement des autres lois axées sur l'utilisation sécurisée de l'espace numérique, conçues pour les groupes vulnérables et les consommateurs, ou pour le grand public. Citons par exemple la loi sur la sécurité en ligne des enfants et la vérification de l'âge (voir la loi britannique sur la sécurité en ligne de 2023) et les cadres de sensibilisation à la cybersécurit

5. Lois sur la cyberguerre : Elles reflètent les aspects militaires et offensifs de la cyberdéfense. Elles régissent l'utilisation des capacités cybernétiques dans les opérations militaires et étatiques, notamment en période de conflit ou de tension entre nations (voir la loi japonaise sur la cyberdéfense active de 2025).

En pratique, ces lois se chevauchent. Il est courant de voir une loi sur la cybersécurité inclure des aspects de cybersécurité, des dispositions prohibitives ou des sanctions pénales.

Outre cette catégorisation floue, il convient de noter que divers domaines de l'interaction humaine intègrent désormais une dimension numérique. Cela a conduit à l'élaboration de lois réglementant ces interactions, notamment sectorielles, intégrant des dispositions spécifiques relatives à la cybersécurité. Par exemple, le droit de la propriété intellectuelle (PI), bien que principalement axé sur les droits des créateurs, inclut désormais des aspects interdisant le contournement des mesures techniques de protection conçues pour protéger les droits de PI. De même, les lois sur la protection des consommateurs abordent actuellement la cybersécurité. Dans l'UE, par exemple, une modification récente du règlement sur la responsabilité du fait des produits inclut la cybersécurité comme facteur d'évaluation de la sécurité des produits (voir Directive (UE) 2024/2853, art. 7(2)(f)).

En résumé, compte tenu de l'intégration généralisée du numérique dans tous les aspects de la vie moderne, la cybersécurité ne peut se limiter à un instrument juridique isolé. Au contraire, ses principes et préoccupations s'intègrent à un large éventail de lois régissant l'activité humaine, allant des droits de l'homme à la santé, en passant par la finance, l'éducation, la défense et la protection des consommateurs. Par conséquent, toute approche globale de la réglementation de la cybersécurité doit tenir compte de cette tendance.

L'énoncé du problème

Le Nigéria, comme d'autres pays, est en proie aux cybermenaces et a mis en place, au fil des ans, plusieurs mesures pour les encadrer. Ces efforts de régulation englobent, entre autres, la législation, l'autorégulation, les politiques et stratégies nationales, l'intervention judiciaire, les mesures coercitives et la coopération internationale.

Cependant, malgré des progrès à divers niveaux, l'impact global reste limité, comme en témoignent le classement du Nigéria dans l'indice mondial de cybersécurité et la perception du public du taux de cybercriminalité du pays. Un tel indice, publié par des chercheurs de l'Université d'Oxford, classe le Nigéria au 5e rang dans un rapport mondial sur les sources d'activités de cybercriminalité, derrière la Russie, l'Ukraine, la Chine et les États-Unis, qui occupaient respectivement les première, deuxième, troisième et quatrième positions (voir Miranda Bruce, et al., 2024). Cette position est inconfortable, étant donné que le Nigéria n'est pas aussi avancé technologiquement que les autres pays de la liste.

Une telle position exige une réévaluation du paysage réglementaire et des capacités technologiques du Nigéria en matière de cybersécurité afin de renforcer les points faibles. Plusieurs faiblesses réglementaires illustrent ce problème :

1. Une loi sur la cybercriminalité obsolète La loi sur la cybercriminalité (interdiction, prévention, etc.) de 2015 a été promulguée à une époque où les crimes commis via des systèmes informatiques étaient naissants.
La loi a été modifiée en février 2024 pour résoudre certains problèmes, notamment le respect de la décision de la Cour de la CEDEAO, qui a estimé que l'article 24 de la loi sur la cybercriminalité violait la Charte africaine des droits de l'homme et des peuples.

Toutefois, cet amendement n'était pas suffisamment substantiel pour remédier aux lacunes de la loi, notamment à la lumière de l'évolution des cybermenaces au Nigéria et de l'ampleur et de la sophistication croissantes de ces menaces.

Les infractions visées par la loi étaient courantes au moment de son adoption, mais de nouvelles cybercriminalités sont apparues depuis, et les anciennes continuent d'évoluer. Ce problème n'a pas été entièrement pris en compte dans l'amendement. Bien que certaines dispositions de la loi puissent être étendues pour couvrir de nouvelles méthodes de

En matière de cybercriminalité, il est douteux que la loi soit suffisamment souple et adaptable pour faire face aux menaces émergentes telles que la pornographie vengeresse, l'abattage de porcs, la désinformation, les deepfakes et les rançongiciels. La clarté de la définition des infractions est cruciale en droit pénal, et les ambiguïtés résultant de l'extension des définitions existantes à de nouveaux crimes pourraient entraver la justice.

De plus, les sanctions prévues par la Loi sur la cybercriminalité ne sont pas suffisamment dissuasives pour prévenir ces crimes dans certains cas. De nombreuses amendes sont bien inférieures aux dommages potentiels causés aux systèmes d'information et aux personnes par la cybercriminalité (par exemple, article 12(3)).

De plus, la loi ne prévoit pas de dispositions adéquates pour le soutien aux victimes en termes d'assistance psychologique pour les personnes touchées par le cyberharcèlement ou le harcèlement en ligne.

Enfin, bien que le Nigéria ait adhéré à la Convention du Conseil de l'Europe sur la cybercriminalité en juillet 2022, la Convention n'aura pas d'effet local tant qu'elle ne sera pas transposée dans le droit national conformément à l'article 12 de la Constitution nigériane.

2. L'utilisation abusive perçue de la loi sur la cybercriminalité pour cibler les défenseurs des droits de l'homme et les journalistes Ces dernières
années, de nombreux rapports indiquent que certaines dispositions de la loi nigériane sur la cybercriminalité ont été injustement appliquées pour cibler des militants et violer les droits de l'homme. Bien qu'une décision de la Cour de la CEDEAO ait pu motiver la récente modification de l'article 24 de la loi, cette modification ne concernait qu'un paragraphe de la disposition. D'autres paragraphes, tels que l'article 24(2), restent inchangés.

L'article 24(2) traite de la responsabilité pénale pour les communications menaçantes, harcelantes ou liées à l'extorsion via des systèmes ou des réseaux informatiques.
Cependant, les termes utilisés dans cette disposition – tels que « intimider », « harceler », « menace », « réputation » et « crainte de violence » – manquent de définitions claires. Cette ambiguïté laisse leur interprétation ouverte au jugement subjectif des forces de l'ordre et des procureurs. Par conséquent, les critiques, notamment dans un éditorial du journal américain
La Mission des États-Unis au Nigéria soutient à juste titre que cette disposition est vague, trop large et susceptible d'être
abusive (voir l'éditorial d'opinion de la Mission des États-Unis au Nigéria).

En effet, cette disposition a été utilisée pour arrêter des blogueurs, des journalistes et des utilisateurs de réseaux sociaux simplement pour avoir critiqué des individus, et non pas nécessairement pour avoir proféré des menaces ou s'être livrés à des actes d'extorsion.
Cette pratique donne un poids considérable aux arguments concernant l'utilisation abusive de la loi.

3. Absence d'une approche globale (horizontale)
Droit de la cybersécurité
Alors que la cybercriminalité (interdiction, prévention, etc.)
La loi de 2015 a constitué une étape législative importante visant à lutter contre les cybermenaces et à promouvoir la cybersécurité au Nigéria, mais elle ne parvient pas à fournir un cadre juridique complet pour une gouvernance nationale holistique de la cybersécurité.

L'énoncé du problème

L'un de ses objectifs déclarés est d'améliorer la cybersécurité dans tout le pays ; cependant, depuis son adoption, il n'y a pas eu de législation de suivi d'application générale – ce que l'on appelle souvent une loi horizontale sur la cybersécurité – pour concrétiser systématiquement cet objectif.

Au lieu de cela, le Nigéria s'est appuyé uniquement sur une approche fragmentée, certains secteurs comme la finance et les télécommunications ayant élaboré des réglementations sectorielles en matière de cybersécurité. Bien que ces domaines soient importants, la majorité des secteurs critiques – notamment la santé, l'éducation, l'industrie manufacturière et les transports – manquent de réglementation claire et applicable en matière de cybersécurité.

Ce vide réglementaire crée des incohérences dans la gestion des cyberrisques et laisse d'importantes vulnérabilités au sein de l'infrastructure numérique nationale. En effet, l'absence d'un cadre juridique harmonisé en matière de cybersécurité fragilise la chaîne d'approvisionnement globale et compromet la résilience du cyberespace nigérian.

4. Intervention législative réactionnaire L'approche législative essentiellement réactive du Nigéria en matière de cybersécurité aggrave le problème. Les interventions juridiques et politiques sont souvent motivées par des incidents, tels que des fraudes financières, des violations de données ou une surveillance internationale, plutôt que d'être fondées sur la prévoyance ou une évaluation proactive des risques. La loi sur la cybercriminalité de 2015 elle-même était une réponse à la pression croissante visant à freiner la vague croissante de cyberfraude et à redorer l'image du Nigéria à l'échelle internationale. Cependant, près d'une décennie plus tard, l'innovation législative en matière de cybersécurité stagne, alors même que le paysage des menaces a considérablement évolué.

La situation est encore compliquée par les propositions législatives qui interprètent mal les besoins en matière de cybersécurité en se concentrant de manière disproportionnée sur le contrôle des contenus, la surveillance ou la régulation des réseaux sociaux, au détriment des garanties techniques, de la protection des infrastructures critiques et du renforcement des capacités. De tels amalgames non seulement détournent l'attention des véritables priorités en matière de cybersécurité, mais risquent également de porter atteinte aux libertés civiles sans pour autant renforcer la cyber-résilience nationale.

5. Coordination de supervision peu claire et application faible Plusieurs agences jouent des

rôles différents dans l'application de la cybersécurité au Nigéria, notamment le Bureau du conseiller à la sécurité nationale (ONSA), le procureur général de la Fédération, les organismes chargés de l'application de la loi (police, EFCC, Commission indépendante des pratiques de corruption, etc.), l'équipe nigériane d'intervention en cas d'urgence informatique (ngCERT), NITDA, Conseil consultatif sur la cybercriminalité, Commission nigériane de protection des données (NDPC), NCC, CBN, etc. Dans la hiérarchie, l'ONSA est responsable des efforts de coordination de la cybersécurité au Nigéria, mais on ne sait pas comment la coordination en aval de l'

Les autres agences sont en cours de réalisation. Les capacités techniques, juridiques et organisationnelles de l'ONSA à répondre aux défis de cybersécurité à tous les niveaux de gouvernance de la cybersécurité au Nigéria sont limitées. Cela pose d'importants défis en matière d'application de la loi.

L'ONSA semble dépassée par ses responsabilités de coordination des questions de sécurité nationale, tant traditionnelles que cybernétiques, notamment compte tenu de la complexité des cybermenaces contemporaines. Ces lacunes en matière d'application de la loi créent un environnement où les cyberattaques sont souvent dissimulées et où les organisations hésitent à signaler les violations, ce qui affaiblit les systèmes de notification des violations de données par le déni et les contre-accusations.

6. Faiblesse des capacités institutionnelles et déficit de compétences critiques Le
paysage de la cybersécurité au Nigéria est considérablement compromis par la fragilité institutionnelle et une pénurie prononcée de professionnels qualifiés.
Les organismes de réglementation semblent manquer de capacité opérationnelle, de cohérence stratégique et de profondeur technique pour faire face à l'évolution rapide des cybermenaces modernes. Cette situation est aggravée par des contraintes de ressources persistantes qui freinent le développement et la mise en œuvre d'un cadre de cybersécurité résilient. De nombreux secteurs, notamment les institutions gouvernementales et les PME, ne sont pas en mesure d'allouer des budgets suffisants aux infrastructures de cybersécurité. Cela implique non seulement des outils avancés de détection et de réponse aux menaces, mais aussi la formation professionnelle continue nécessaire pour rester en phase avec les normes mondiales de cybersécurité.

Le déficit de compétences, en particulier, demeure un obstacle majeur : il existe une pénurie de personnel qualifié capable de concevoir, de gérer et de maintenir des environnements numériques sécurisés. Sans investissements ciblés dans la réforme institutionnelle et les initiatives de renforcement des capacités, le Nigéria reste vulnérable à l'escalade des cybermenaces qui menacent la sécurité nationale, la stabilité économique et la confiance du public.

7. Faible sensibilisation du public à la cybersécurité.
L'analphabétisme numérique généralisé au Nigéria compromet la cyber-résilience du pays. De nombreux individus et organisations manquent d'hygiène informatique de base, ce qui les rend vulnérables au phishing, au vol d'identité et à d'autres menaces. Cette situation est aggravée par une éducation publique limitée et l'absence de cybersécurité dans les programmes scolaires.

À mesure que l'utilisation d'Internet se développe, notamment via les appareils mobiles, les habitudes numériques non informées représentent un risque national croissant.

Recommandations

Les lacunes identifiées ci-dessus soulignent la nécessité d'une réforme globale de la réglementation en matière de cybersécurité au Nigéria. L'amendement de 2024 à la loi sur la cybercriminalité ne suffit pas à résoudre ces problèmes. C'est pourquoi les recommandations suivantes sont adressées aux acteurs législatifs.

1. Mener une étude approfondie sur l'efficacité et la mise en œuvre de la loi sur la cybercriminalité Une étude approfondie devrait être menée pour évaluer
l'efficacité et la mise en œuvre de la loi sur la cybercriminalité au cours des dix dernières années depuis sa promulgation. Cela permettrait d'identifier les lacunes dans le droit matériel et les mécanismes d'application et de suggérer des moyens de combler ces lacunes à l'avenir.

Quoi qu'il en soit, cette étude devrait conduire à la modification de plusieurs dispositions de la loi, notamment celles relatives aux infractions et aux sanctions (dont l'article 24 (2)). Cette modification devrait tenir compte des cybercrimes nouveaux et émergents, notamment compte tenu des avancées technologiques telles que l'intelligence artificielle, la blockchain et l'informatique quantique, entre autres.

2. Adopter une loi horizontale sur la cybersécurité Une législation fédérale d'application générale sur la cybersécurité devrait être promulguée pour répondre aux obligations proactives en matière de cybersécurité tout au long de la chaîne d'approvisionnement des TIC et dans tous les secteurs au Nigéria. Une telle loi horizontale sur la cybersécurité devrait contenir des dispositions sur la sécurité des réseaux et de l'information, la gestion des risques, la cyber-résilience, les certifications, le renforcement des compétences et les campagnes de sensibilisation du public.

Des dispositions de cybersécurité pour les groupes vulnérables tels que les enfants devraient être incluses, à moins que le législateur n'envisage de promulguer une loi autonome sur la cybersécurité.

3. Inclure des mécanismes d'examen périodique dans les réglementations en matière de
cybersécurité Les futures lois sur la cybersécurité au Nigéria devraient inclure des dispositions pour des examens et des mises à jour périodiques afin de garantir qu'elles restent pertinentes à la lumière de l'évolution des cybermenaces et des innovations technologiques. Cet examen périodique devrait être mené par de multiples parties prenantes impliquant des agences gouvernementales, des experts du secteur, des universitaires et la société civile, et devrait donner lieu à des ajustements fondés sur des données probantes des cadres juridiques, techniques et opérationnels afin de faire face aux risques émergents, de combler les lacunes réglementaires et de s'aligner sur les meilleures pratiques internationales.
consultations

4. Aborder le soutien aux victimes de cybercriminalité La législation sur la cybersécurité au Nigéria devrait prévoir un soutien aux victimes, y compris une assistance physique et psychologique, en particulier pour les victimes de cyberharcèlement, de harcèlement en ligne et de vol d'identité.
Cela impliquerait de modifier la loi actuelle sur la cybercriminalité afin d'y inclure des dispositions claires imposant des services d'assistance aux victimes, tels que des services de conseil, une aide juridique, des lignes d'assistance téléphonique pour le signalement et des mécanismes de réparation rapide, tout en exigeant que les organismes chargés de l'application de la loi soient formés aux approches sensibles aux victimes et en assurant la coordination avec les services sociaux et les ONG concernés.

5. Engagement des parties prenantes et plus grande transparence du processus législatif. Des mécanismes devraient être mis en place pour garantir un engagement significatif avec les parties prenantes concernées, notamment les experts en cybersécurité, la société civile et l'industrie technologique, lors de la révision et de la réforme des lois sur la cybercriminalité et la cybersécurité. Cela favorisera des processus législatifs plus approfondis et plus éclairés et contribuera à combler les lacunes et les insuffisances des réformes juridiques.

6. Domestication des instruments internationaux pertinents en matière de cybercriminalité Afin de renforcer le
cadre juridique du Nigéria contre la cybercriminalité et de l'aligner sur les normes mondiales, l'Assemblée nationale devrait prendre des mesures urgentes pour intégrer la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest), conformément à l'article 12 de la Constitution de 1999 (telle que modifiée). La domestication permettra aux forces de l'ordre, aux autorités judiciaires et aux autres parties prenantes nigérianes de tirer parti des dispositions de la Convention sur la coopération internationale, le partage des preuves et l'harmonisation des infractions de cybercriminalité.

7. Créer une autorité centralisée pour l'application de la cybersécurité Une autorité nationale centralisée chargée
de coordonner et d'appliquer les politiques, les normes et la réponse aux incidents de cybersécurité dans tous les secteurs devrait être créée, en retirant cette responsabilité de la NSA. Cette autorité devrait disposer de pouvoirs juridiques clairs pour superviser la conformité, enquêter sur les cybermenaces, coordonner les efforts nationaux de cyberdéfense et faciliter la collaboration entre les agences gouvernementales, le secteur privé et les partenaires internationaux. Son mandat devrait inclure le partage de renseignements sur les menaces, l'établissement de normes de sécurité, le renforcement des capacités, la fourniture de conseils et la garantie d'une réponse rapide aux cyberincidents, éliminant ainsi les efforts fragmentés et renforçant la posture globale du Nigéria en matière de cybersécurité.

Recommandations

8. Établir un cadre national de cyberdéfense exploitant l'expertise citoyenne. Un cadre national de cyberdéfense intégrant l'expertise citoyenne, notamment des pirates informatiques éthiques, des chercheurs en cybersécurité et des professionnels de la technologie, pour défendre les infrastructures critiques nationales et le cyberespace. Ce cadre devrait créer des canaux de collaboration structurés tels que des programmes de divulgation des vulnérabilités, des partenariats public-privé et un corps de réserve cybernétique volontaire. Il devrait également promouvoir les initiatives de piratage informatique responsable, encourager les contributions citoyennes par des reconnaissances ou des récompenses, et garantir des protections juridiques appropriées aux personnes qui agissent de bonne foi pour renforcer la cybersécurité nationale.

9. Intensifier le renforcement des compétences et l'information du public mesures de sensibilisation

Adopter une politique globale de cybersécurité qui donne la priorité aux initiatives continues de renforcement des capacités et aux stratégies de développement de la main-d'œuvre pour doter les acteurs des secteurs public et privé des compétences nécessaires pour faire face à l'évolution des menaces de cybersécurité.
Cela devrait inclure des programmes de formation spécialisés, des systèmes de certification, des campagnes de sensibilisation du public sur l'hygiène informatique, l'intégration de l'éducation à la cybersécurité dans les programmes universitaires et des partenariats avec des organisations internationales pour s'aligner sur les meilleures pratiques mondiales.

Conclusion

L'intégration généralisée du numérique dans tous les aspects de la vie moderne signifie que la cybersécurité ne peut plus être considérée comme une préoccupation de niche, mais comme un pilier fondamental de la sécurité nationale et de la résilience économique. Cependant, le cadre actuel de cybersécurité du Nigéria peine à suivre l'évolution rapide du paysage des menaces. Le recours à une loi sur la cybercriminalité obsolète, une approche réglementaire fragmentée et sectorielle, la faiblesse des capacités institutionnelles et le manque de sensibilisation du public ont créé d'importantes vulnérabilités.

Les recommandations présentées dans cette note – de l'adoption d'une loi fondamentale et horizontale sur la cybersécurité à la création d'une autorité nationale de contrôle dédiée et à la formation d'une nouvelle génération de citoyens et de professionnels sensibilisés à la cybersécurité – offrent une feuille de route pour une réforme globale. En passant d'une réglementation réactive à une réglementation proactive et globale, le Nigéria peut atténuer efficacement les cybermenaces, bâtir un écosystème numérique résilient et renforcer sa position dans l'économie numérique mondiale. Le temps des ajustements progressifs est révolu ; une refonte audacieuse et stratégique de la gouvernance nationale de la cybersécurité s'impose désormais.

Références

- Abuh Ibrahim Sani et Ibrahim Yakub, « Évaluation de l'état de préparation du Nigéria face aux cyberattaques d'État : étude comparative des politiques de cybersécurité, de la réponse aux incidents et de la coopération internationale ». Journal of Computational Analysis and Applications, VOL. 34, N° 4, 2025.

- Directive 2024/2853 de l'UE du Parlement européen et du Conseil du 23 octobre 2024 relative à la responsabilité du fait des produits défectueux et abrogeant la directive 85/374/CEE du Conseil.

- Iheanyi Nwankwo, « Renforcer la cyberfrontière du Nigéria : renforcer la résilience en matière de cybersécurité grâce à l'innovation juridique. » Commonwealth Cyber Journal vol. 3, 2025, ISSN 2959-3018 (imprimé), ISSN 2959-3026 (en ligne) thecommonwealth.org/cyber-journal.

- Loi japonaise sur la cyberdéfense active 2025.

- Miranda Bruce, et al., « Cartographie de la géographie mondiale de la cybercriminalité avec le World Cybercrime Index », Publié le 10 avril 2024, https://doi.org/10.1371/journal.pone.0297312.

- Loi britannique de 2023 sur la sécurité en ligne.

- Mission des États-Unis au Nigéria, « Prévenir l'utilisation abusive de la loi sur la cybercriminalité : protéger la liberté d'expression et stimuler la croissance économique » Publié le 11 juin 2025, https://ng.usembassy.gov/preventing-misuse-of-the-cybercrimes-act-protecting-free-speech-and-unlocking-economic-growth/