

AFRICTIVISTES

ANALYSE DE POLITIQUE

JUNE 2020

TRADUCTION EN FRANCAIS
JUILLET 2020



Thème : Liberté d'expression

Nom du Pays : Niger

Législation en Question : Loi N-0267 sur la lutte contre la cybercriminalité au Niger, 25 juin 2019 ; Constitution du Niger

Le Niger est membre de la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) et a ratifié plusieurs conventions prévoyant le respect des droits humains et droits numériques, telles que la directive C/DIR/1/08/1 de la CEDEAO, et la Convention du Conseil de l'Europe du 23 novembre 2001 sur la cybercriminalité.

Le droit à la liberté d'expression prévu aux termes de l'article 30 de la Constitution de la République du Niger prévoit " le droit à la liberté de pensée, d'opinion, d'expression, de conscience, de religion et de culte ". L'article 30 stipule que ce droit doit être exercé dans le respect de l'ordre public, de la paix sociale et de l'unité nationale et est donc pondéré par rapport à ces trois éléments.

La loi sur la cybercriminalité a été adoptée pour garantir la sécurité des citoyens en ligne et lutter contre la cybercriminalité. La loi prévoit :

- c) la prévention des actes qui portent atteinte à la confidentialité, à l'intégrité et à l'accessibilité des systèmes et données informatiques, ainsi qu'à leur utilisation frauduleuse, et
- d) prévoit les règles de procédure pénale relatives aux infractions concernant les systèmes et données informatiques et les réseaux de communication électronique.

Les sanctions en cas d'infraction sont définies ci-dessous :

- Article 30 : L'article prévoit que quiconque prononce, par voie de communication électronique, toute expression outrageante, toute expression de mépris ou toute critique qui est fautive, peut être puni d'un emprisonnement de 6 mois à 3 ans ou d'une amende de 1 million à 5 millions de francs CFA.
- Article 31 : L'article prévoit que quiconque produit, met à la disposition d'autrui ou diffuse des données susceptibles de troubler l'ordre public ou de porter atteinte à la dignité humaine par le biais d'un système d'information peut être emprisonné de 6 mois à 3 ans et condamné à une amende de 1 million à 5 millions de francs CFA.

Selon les meilleures pratiques internationales, une limitation des droits doit être raisonnable et proportionnelle, dans une société ouverte et juste. La limitation du droit doit être absolument essentielle pour atteindre ledit objectif légitime et satisfaire au critère de proportionnalité. Les limitations raisonnables et proportionnées qui sont objectivement justifiables sont autorisées en termes de lois et de normes internationales. Par conséquent, chaque cas doit être jugé en fonction des circonstances qui lui sont propres. L'emprisonnement au seul motif qu'une communication/expression critique l'État, ne peut être qualifié d'objectif légitime pour utiliser la loi. Toutefois, les circonstances d'une affaire particulière seront le facteur décisif pour déterminer si l'arrestation d'un individu pour infraction à la loi sur la cybercriminalité a été effectuée de manière raisonnable et justifiable ou non. La "critique" n'est pas le critère qui détermine qu'une possible infraction est punissable aux termes de la loi. C'est plutôt la véracité de l'information.

Recommandations stratégiques :

1. Sensibilisation - Des démarches pratiques visant à favoriser les initiatives de formation devraient être entreprises pour faire comprendre la nouvelle loi, la diffusion de fausses données ("fausses nouvelles") et les sanctions en cas de violation délibérée ou involontaire de ces lois.
2. Approche multipartite pour faire des propositions et engager des consultations publiques en vue de clarifier certains articles de la loi qui sont trop généraux ou peu clairs.

Thème : Protection des données et vie privée (Interception des communications)

Nom du Pays : Niger

Législation en Question : Loi portant interception de certaines communications émises par voie électronique au Niger, 29 mai 2020 ("la Loi")

La lutte contre le terrorisme en utilisant des méthodes d'interception de communications électroniques exige un juste équilibre entre la sécurité nationale et le droit à la vie privée (voir ci-dessus). Les critères d'interception des communications doivent être clairement définis à travers un processus consultatif et réfléchi d'élaboration des politiques et de rédaction des textes.

Privacy International a soulevé les préoccupations suivantes au Niger :

- a) **Autorisation et Supervision** : Actuellement, le pouvoir discrétionnaire d'approuver une demande d'interception appartient exclusivement au président. La loi établit le Comité de contrôle des interceptions de sécurité ("CCSI"), qui a des pouvoirs de surveillance limités et dont les conclusions sur une interception de communication ne sont pas contraignantes pour le gouvernement. La composition de la CCSI est la suivante : "tous sauf 2 [sont] nommés par l'exécutif".

Les réformes de la loi doivent prévoir un processus de contrôle judiciaire - les acteurs étatiques qui autorisent toute interception de communications électroniques sont tenus de soumettre, après coup, un rapport écrit à un juge compétent, justifiant la base légale de l'interception. Des sanctions doivent être prévues en cas de manquement à cette obligation. La section 51(1)(a)(i) de la loi sud-africaine 70 de 2002 sur la réglementation de l'interception des communications et la fourniture d'informations liées aux communications prévoit une telle sanction.

- b) **Formulation et contenu de la loi** : La formulation et le contenu de la loi doivent être analysés afin de relever toute ambiguïté et tout débordement, et ensuite être circonscrits à un point où il ne peut y avoir aucune confusion quant aux bases légales sur lesquelles l'État peut s'appuyer pour intercepter des communications. En outre, les définitions doivent être révisées pour assurer la clarté et l'interprétation universelle par toute la République.

- c) **Notification** : il est important que la reconnaissance et la mise en œuvre d'une obligation de notifier ou d'informer les personnes après qu'elles ont été visées par des mesures d'interception par l'État soient incluses dans toute modification de la loi.

Actuellement, les citoyens du Niger soumis à des activités de surveillance et d'interception par l'État n'en ont pas connaissance.

- d) **Limitations de l'implication des opérateurs de télécommunications au Niger** : en vertu de la loi, les opérateurs de télécommunications ne peuvent contester les sanctions encourues par un refus d'aider le gouvernement dans les activités de surveillance et le refus de coopérer est sanctionné par 1 à 3 ans d'emprisonnement et une forte amende.

En conséquence, il est recommandé de modifier la loi afin de limiter le pouvoir de l'État à contraindre les opérateurs de télécommunications à coopérer. Ainsi, les opérateurs ne coopéreront uniquement dans les cas où un intérêt public est apparent, où une autorisation judiciaire a été reçue et/ou lors d'un désastre national ou un état d'urgence dûment déclaré.

L'article 44 de la Constitution souligne que dans l'interprétation et l'application de ses lois, "notamment celles qui concernent les droits fondamentaux tels que la liberté d'expression, la République du Niger doit être attentive aux normes internationales".

Recommandations stratégiques :

1. **L'alignement sur les lignes directrices de l'Union Internationale des Télécommunications -UIT sur l'harmonisation des politiques, de la législation et des procédures réglementaires en matière de TIC dans les Caraïbes (HIPCAR)** concernant l'interception des communications est un bon exemple des facteurs et du niveau de détail qui doivent être pris en compte dans une loi pareille. Le modèle de lignes directrices comprend les éléments suivants :
 - g) Définir les interprétations communes nécessaires pour les termes clés associés à l'interception de la communication électronique ;
 - h) Définir le rôle des acteurs/entités chargés de gérer l'interception des communications électronique ;
 - i) Définir des critères juridiques et des normes auxquels l'interception des communications doit être soumise ;
 - j) Définir les dérogations au respect de l'interception des communications ;
 - k) Etablir des procédures de contrôle, d'exécution, de révision et d'appel en rapport avec l'interception des communications ; et
 - l) Mettre en place un cadre d'interception des communications conjointement avec les politiques publiques sur les questions connexes.
2. **Sensibilisation** - Des mesures pratiques visant à favoriser les initiatives de formation devraient être prises pour faire comprendre la loi et le principe du consentement.
3. **Approche multipartite** pour faire des propositions et entreprendre des consultations publiques en vue de clarifier certains articles de la loi qui sont généraux ou peu explicites.