AFRICTIVISTES

ANALYSE DE POLITIQUES

Aout 2020

TRADUCTION EN FRANÇAIS

SEPTEMBRE 2020

ENDCODE

Tech. Law. Policy. Africa.

ANALYSE DE LOIS PAR ENDCODE: AOUT 2020

Veuillez noter que notre soumission ci-dessous ne constitue pas une analyse approfondie, ni une comparaison multi-juridictionnelle des lois de la Mauritanie par rapport aux normes internationales. Cet article peut être utilisé comme base d'une analyse plus approfondie.

Analyse des Lois sur la Cybercriminalité et sur la Protection des données en Mauritanie

Situation Actuelle

La **Loi sur la Cybercriminalité (loi n° 2016-007)** a été promulguée il y a 4 ans et n'est pas encore entrée en vigueur. Bien que la promulgation de la loi soit un acte positif et important, l'effet du retard est que la nation ne bénéficie pas d'un cadre réglementaire solide pour la cybercriminalité et la cybersécurité.

Le défi est similaire en ce qui concerne le cadre de la **Loi sur la protection des données personnelles (loi n° 2017-020)**, car la loi a été promulguée en 2017 et n'a pas encore de cadre d'exécution pour que les citoyens exercent leurs droits. En effet, les données personnelles des citoyens mauritaniens restent vulnérables et en cas de violation des données ou de traitement non éthique des données personnelles, les citoyens n'ont pas de recours. À l'heure actuelle, aucune indication n'a été donnée quant à la date d'application de la loi.

En vertu de la loi mauritanienne, le gouvernement doit prendre des décrets d'application pour que les deux lois entrent en vigueur. Il a été signalé que les décrets ont été rédigés, mais ils n'ont pas été publiés. La conséquence est que la Mauritanie ne dispose pas d'un cadre juridique entièrement opérationnel pour la cybercriminalité et la protection des données personnelles, car la législation correspondante n'est pas opérationnelle.

Perspectives sur les cadres juridiques

Comme le reconnaissent les meilleures pratiques internationales, l'objectif de la législation sur la cybercriminalité est d'établir des normes et comportements acceptables pour les utilisateurs des technologies de l'information et des communications. La législation en matière de cybercriminalité vise donc les objectifs suivant :[1]

[1] https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html#:~:text=Cybercrime%20law%20identifies%20standards%20of,infrastructure%2C%20in%20particular%3B%20protects%20human

- Créer des infractions propre au cyber espace et prévoir des sanctions légales pour la cybercriminalité en permettant l'enquête et la poursuite des infractions commises en ligne.
- Protéger les utilisateurs des TIC et atténuer et prévenir les dommages causés aux personnes, aux données, aux systèmes, aux services et aux infrastructures.
- Défendre les droits de l'homme.
- Faciliter la coopération entre les pays en matière de cybercriminalité
- La loi sur la cybercriminalité impose des règles de conduite et des normes de comportement pour l'utilisation de l'internet, des appareils électroniques et des technologies numériques connexes. En outre, elle prévoit des règles de conduite et des normes qui régissent les actions des organisations publiques, gouvernementales et privées ;
- Il établit des principes de procédure pénale et de preuve adaptés aux technologies, ainsi que d'autres questions de justice pénale en ligne. En outre, elle fournit un cadre réglementaire pour réduire les risques et/ou atténuer les dommages causés aux personnes, aux organisations et aux infrastructures en cas de cybercriminalité. En substance, le droit de la cybercriminalité fournit un droit matériel, procédural et préventif.

La législation mauritanienne en matière de cybercriminalité prévoit ce qui suit :

- Les cybercrimes sont criminalisés en vertu du chapitre II de la loi 2016/007, intitulé "Atteintes à la confidentialité, à l'intégrité et à la disponibilité des données et des systèmes informatiques" ; et
- Les articles 4 à 13 prévoient diverses cyberinfractions, notamment les infractions liées à : la violation de la confidentialité d'un ordinateur et/ou des données qui y sont stockées, les atteintes à l'intégrité et à la disponibilité d'un ordinateur, l'utilisation/la distribution de technologies/dispositifs susceptibles d'être utilisés pour commettre des cyberinfractions.

Il est évident que la loi sur la cybercriminalité vise à fournir des normes et comportements acceptables pour les utilisateurs des technologies de l'information et de la communication, et cela est conforme aux normes internationales.
En outre, la loi sur la cybercriminalité crée des infractions et prévoit des sanctions le cas échéant, qui sont également des aspects essentiels des normes internationales en matière de cybercriminalité.

Les normes internationales évoquées ci-dessus exigent également que la législation sur la cybercriminalité protège les utilisateurs des TIC et les infrastructures cruciales - à cet égard, il est à noter que la loi sur la cybercriminalité de la Mauritanie répond à ces exigences.

Outre la loi sur la cybercriminalité, le gouvernement mauritanien envisage l'élaboration d'une Stratégie nationale de cybersécurité et a institué le Service de sécurité informatique, qui fait partie de la Direction générale des technologies de l'information et des communications (DGITC) et qui est spécifiquement chargé d'enquêter sur les cybercrimes (Union africaine & Symantec, 79). La Mauritanie, cependant, ne dispose pas d'une équipe d'intervention d'urgence informatique (CERT) officielle et opérationnelle.

Les lignes directrices de l'Organisation de coopération et de développement économiques (OCDE) sur la protection des données personnelles[2] sont reconnues comme un modèle accepté par rapport auquel le régime mauritanien de protection des données peut être comparé. Les lignes directrices sont formulées comme suit :

- **Limitation de la collecte** : La collecte de données ne doit avoir lieu qu'à la connaissance et avec le consentement de la personne concernée.
- **Qualité des données** : On ne peut recueillir que des informations pertinentes et exactes pour un objectif particulier.
- **Participation individuelle** : La personne concernée doit être informée que ses données personnelles ont été collectées et doit pouvoir y accéder.
- **Spécification de la finalité** : L'utilisation prévue des données à caractère personnel doit être divulguée au moment de la collecte.
- **Limitation de l'utilisation** : Les données collectées ne peuvent être utilisées à d'autres fins que celles qui ont été divulguées au moment de la collecte.
- **Garanties de sécurité** : Des mesures raisonnables doivent être mises en œuvre pour protéger les données personnelles contre toute utilisation, destruction, modification ou divulgation non autorisée.
- **Transparence** : Les personnes concernées doivent pouvoir accéder à leurs données personnelles telles qu'elles ont été collectées et être en mesure de contacter l'entité qui collecte leurs données.
- **Redevabilité** : Les responsables du traitement des données doivent être tenus pour responsables de toute violation des principes ci-dessus. Une personne dédiée responsable de la conformité doit être nommée.

La loi mauritanienne sur la protection des données consacre des principes fondamentaux similaires en matière de traitement des données, ce qui constitue une caractéristique importante et est conforme aux lignes directrices de l'OCDE. Les principes fondamentaux prévoient ce qui suit :

- La collecte, le stockage, le traitement, la conservation des données personnelles doivent être licites, équitables et non frauduleux.

[2] https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

- Les données à caractère personnel doivent être proportionnées, pertinentes et non excessives au regard des finalités pour lesquelles elles ont été collectées et traitées.
- Les données à caractère personnel ne peuvent être conservées pendant une durée excédant le temps nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées ou traitées.
- Les données à caractère personnel doivent être exactes et mises à jour si nécessaire. Des mesures raisonnables doivent être prises pour garantir que les données inexactes ou incomplètes soient effacées ou rectifiées.
- Le traitement des données ne peut être effectué que dans le respect du principe de transparence de la part du responsable du traitement.
- Les données personnelles doivent être gardées confidentielles et sont protégées conformément à la loi, en particulier lorsque les données sont transmises par le biais d'un réseau.
- Le traitement des données personnelles ne peut être effectué que sous réserve d'un accord juridique écrit entre les parties.

Les principes internationalement acceptés de limitation de la collecte, de spécification des objectifs, de qualité des données, de participation individuelle, de garanties de sécurité sont prévus dans la législation. Selon l'évaluation des Lignes directrices de l'OCDE, la loi mauritanienne sur la protection des données semble satisfaire aux normes internationales. En outre, l'exigence d'un contrat écrit entre les parties va au-delà des Lignes directrices et offre un plus grand degré de protection aux personnes concernées. Il est toutefois préoccupant de constater que la loi sur la protection des données ne prévoit pas la participation individuelle et la transparence.

Il est à noter que la loi sur la protection des données omet toutefois des dispositions sur la portabilité des données, les notifications de violation, le respect de la vie privée dès la conception et l'obligation de disposer de délégués à la protection des données en fonction dans certains cas. Il est souligné qu'au moins, la loi sur la protection des données devrait prévoir des notifications de violation qui sont une partie essentielle de l'application de la loi pour les autorités mauritaniennes, et sont également un mécanisme vital pour permettre aux citoyens mauritaniens de protéger leur vie privée et leur identité.

Il convient de noter que l'article 10 de la Constitution mauritanienne consacre les droits fondamentaux à la liberté d'expression et à la liberté d'opinion et de pensée, mais que le droit à la vie privée n'est pas consacré.

Human Rights Watch (en janvier 2019) a critiqué le gouvernement mauritanien et a estimé que le gouvernement a utilisé des lois trop générales et inutilement strictes (législation relative à la cybercriminalité, à la diffamation criminelle et autres) comme moyen de réprimer la dissidence et la critique.

Les sanctions et les infractions prévues par la législation pourraient être utilisées pour réprimer les libertés civiles, en particulier le droit à la liberté d'expression. L'ONUDC avertit que le droit international reconnaît qu'il est parfois nécessaire d'imposer des limitations aux droits de l'homme, mais que cela n'est justifiable que dans la poursuite d'un objectif légitime, conformément à la législation existante et nécessaire et proportionné par rapport à l'objectif de la restriction.

La loi sur la cybercriminalité, lorsqu'elle est mesurée à l'aune des critères évoqués ci-dessus, peut présenter des risques pour l'exercice des libertés civiles en Mauritanie.

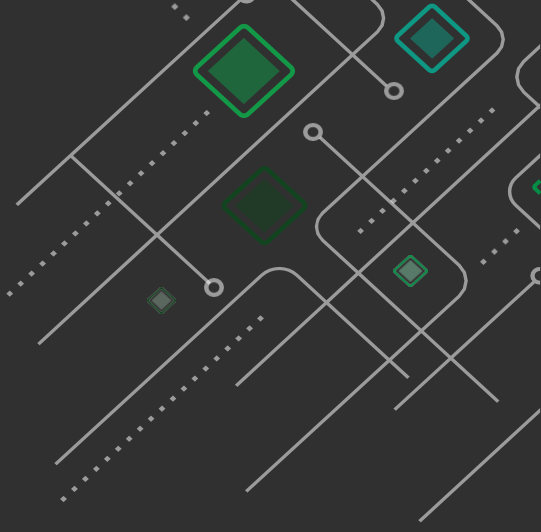
La principale critique formulée à l'encontre de la loi sur la protection des données est qu'elle n'est pas opérationnelle. De plus en plus, les Etats africains sont menacés par les cybercriminels et dans le même temps, les institutions du secteur privé et public sont également exposées à des violations de données, les données personnelles des Mauritaniens sont vulnérables.

L'absence de mise en œuvre de la législation signifie qu'il n'existe aucun recours en cas de violation des données à caractère personnel.

En conclusion

Alors que les experts prévoient que le continent africain comptera un milliard d'internautes d'ici 2022, de nombreux pays sont de plus en plus touchés par la cybercriminalité. Il est donc urgent de mettre en place une législation efficace en matière de cybercriminalité et de protection des données personnelles en Mauritanie et dans d'autres pays africains.

Le retard interminable dans l'entrée en vigueur de ces lois porte atteinte aux préoccupations en matière de cybersécurité. Les Mauritaniens ne bénéficient donc pas des avantages de la législation et sont dans une position désavantageuse pour obtenir des recours contre toute violation de leurs données personnelles.



Silky Oak House | Bally Oaks Office Park | 35 Ballyclare Drive | Bryanston
Johannesburg, South Africa

+27 (0) 11 463 4594
endcode.org
base@endcode.org
@endcode_org

Company Reg No. 2014/ 118528/07