Loi cybersécurité et protection des données personnelles - Gouvernement de la République de Guinée, Mai 2016

Commentaire par l'équipe du Bureau Afrique d'Internet Sans Frontières - Contenu mis à disposition d'ABLOGUI sous licence Creative Commons ***CC BY-NC-SA***

Après les lois du 8 novembre 2005 relatives à la règlementation générale des radiocommunications, et celle du 13 août 2015 dite nouvelle loi des télécommunications, le Gouvernement de la République de Guinée s'apprête à légiférer une nouvelle fois sur les télécommunications.

Avec la présentation et la discussion prochaine du projet de loi relative à la cybercriminalité et à la protection des données personnelles, le gouvernement guinéen explique vouloir se doter d'instruments législatifs et réglementaires pour lutter contre la cybercriminalité, créer un cadre pour assurer la protection des données personnelles, des droits et des libertés des citoyens guinéens, et se mettre en conformité avec ses engagements internationaux et régionaux.

Le gouvernement guinéen reconnait que les Technologies de l'Information et de la Communication "permettent de réduire les contraintes horaires, les frontières physiques, permettent de développer et d'entretenir des relations d'affaires, et accroitre la productivité et le rendement des industries et des services" ; mais il estime également que le cyberdéveloppement "entraine cependant de nombreux et complexes défis pour les Etats", et que le cyberespace permet de "créer un espace immatériel qui n'a pas de frontières au sein duquel ou à travers lequel peuvent être commis de graves et multiples actes répréhensibles".

Pour Internet Sans Frontières, si la lutte contre la cybercriminalité est nécessaire pour créer un cyberespace sécurisé pour les citoyens qui y naviguent, celle-ci doit se faire dans le strict respect des principes de proportionnalité, de nécessité et de légalité.

En outre, avec l'arrivée massive des entreprises du numérique en Afrique, Internet Sans Frontières ne peut que se réjouir que les Etats africains légifèrent sur la protection des données personnelles et la vie privée de leurs citoyens. Cependant, les enjeux de la protection des données personnelles et de la vie privée des citoyens appellent des dispositifs législatifs innovants, qui vont au-delà de celles prévues par les modèles actuels et obsolètes que sont les lignes directrices proposées par l'OCDE en 1980 et mises à jour en 2010, ou encore la loi française informatique et libertés de 1978, que beaucoup jugent peu aptes à relever les nouveaux défis du numérique.

I. Une loi non conforme aux exigences démocratiques

Dans toute démocratie, les libertés des citoyens peuvent être restreintes par l'Etat, à condition que ces restrictions soient strictement proportionnelle et nécessaire au but légitime poursuivi, et qu'elles aient reçu l'aval d'une personnalité relevant de l'autorité judiciaire. Cette exigence est renforcée pour les lois pénales, qui doivent en outre être précises et prévisibles. En l'espèce, le projet de loi présenté par le gouvernement guinéen présente des insuffisances sérieuses sur ces point fondamentaux.

A. Entorses aux principes généraux du droit pénal

1. Principe de légalité des délits et des peines

Le projet de loi présenté par le Gouvernement de Guinée créé de nouvelles infractions relatives à la cybercriminalité, mais dans des termes parfois vagues, qui laissent place à une trop grande interprétation. Une imprécision et un manque de clarté qui peuvent être préjudiciable au justiciable et aux citoyens en matière pénale.

Plusieurs dispositions semblent ne pas respecter ce principe, et demandent à être rédigées avec des termes précis, dont les définitions auront été rappelées dans le Titre I relatif aux dispositions générales :

- Article 17 : cette disposition réprime la “détention frauduleuse d’un équipement de télécommunications à connecter sur un réseau ouvert au public ou un réseau privé”. La généralité du terme “équipement de télécommunications” peut laisser craindre que l’utilisation de logiciels de type VPN (Réseau Privé Virtuel), utilisé par ceux qui souhaitent légalement protéger leurs données de navigation et leur identité en ligne, pourrait être concernée ;

- L’Article 31 réprime “la production, la diffusion, la mise à disposition d’autrui de données de nature à troubler l’ordre ou la sécurité publics, ou à porter atteinte à la dignité humaine par le biais d’un système informatique”. Ici encore, la généralité des termes peuvent laisser place aux interprétations les plus folles. L’histoire récente de la République a démontré que peuvent prendre les rennes du pouvoir des appareils qui ont une conception de l’ordre public différente de celle entendue dans les traités et conventions que le pays à signés et ratifiés ;

- Il en est de même pour l’article 41 selon lequel “quiconque commet ou tente de commettre un acte de terrorisme visant des données, logiciels et/ou programmes informatiques pourrait être assimilé à un crime” : l’utilisation du conditionnel laisse une place trop importante à l’interprétation. En outre, le terme acte de terrorisme et les infractions concernées méritent d’être précisemment et strictement définis par le Gouvernement, comme il le fait par exemple à l’article 58, relatif aux atteintes à la propriété intellectuelle.

2. Instauration d’un système de surveillance en violation des droits humains

A la suite des révélations d’Edward Snowden sur le vaste programme de surveillance mis en œuvre par l’agence de renseignement américaine NSA, les organisations de la société civile, dans le sillage des travaux de l’ONU, ont adopté en 2013 Les Principes Internationaux sur

l'Application des Droits Humains à la Surveillance des Communications[1]. Ces 13 principes reprennent ce que les Conventions internationales relative aux droits de l'homme, signée et ratifiée par tous les pays de la planète, exigent des gouvernements à l'ère du numérique.

Selon ces principes, les systèmes de surveillance des communications électroniques mis en place par les Etats doivent notamment :

- Être nécessaires : La Surveillance des Communications doit être le seul moyen d'atteindre un objectif légitime, ou, en cas de multiples moyens, être celui qui porte le moins atteinte aux droits de l'homme ;

- Être placées sous la responsabilité de l'autorité judiciaire : Les décisions de mise en œuvre de système de Surveillance des Communications doivent être prises par une autorité judiciaire compétente, impartiale et indépendante. Cette autorité doit : être distincte et indépendante des autorités qui dirigent la Surveillance des Communications, et disposer des ressources adéquates aux effets de l'exercice des fonctions qui lui ont été assignées ;

- Respecter les exigences d'un procès équitable

En l'espèce, le projet de loi présenté par le Gouvernement de la République de Guinée permet à une « *autorité compétente* » de requérir que les personnes morales ou physiques qui offrent un accès internet mettent en place une surveillance des activités de leurs abonnés, sans que le texte ne précise la place qu'occupe l'autorité judiciaire dans le déclenchement de la procédure de mise sous surveillance.

De même, les dispositions relatives aux mesures de perquisition des systèmes informatiques (articles 94 et suivants) ne précisent pas la place de l'autorité judiciaire impartiale et indépendante dans la décision de déclenchement desdites mesures. Le renvoi à l'article 96 au code de procédure pénale ne constitue une protection suffisante contre les atteintes possibles aux libertés individuelles et droits fondamentaux des citoyens visés.

[1] Lire les 13 principes https://fr.necessaryandproportionate.org/fr/node/2612

B. Une loi qui légitime la censure en ligne

Internet Sans Frontières s'inquiète de ce que certaines dispositions de la loi peuvent ouvrir la voie à des cas de censure. Admettre que de telles dispositions fassent leur entrée dans le corpus juridique guinée serait porter la pire atteinte à la liberté fondamentale d'expression, et serait contraire à tous les engagements régionaux et internationaux pris la République de Guinée.

En prévoyant que sera puni de six mois d'emprisonnement et d'une amende allant de 40M à 120M de Francs Guinéens l'émission d'injure, d'une expression outrageante, tout terme de mépris ou toute invective qui ne renferme l'imputation d'aucun fait, l'article 29 du projet de loi prévoit non seulement une peine disproportionnée au regard de l'infraction dont il est question, mais laisse ouverte la possibilité que les termes « injure » « expression outrageante » ou encore « mépris », « invective » soient interprétés de manière extensive pour englober toute opinion qui ne plairait pas à la victime alléguée ou à l'autorités chargée de réprimer l'infraction.

Les articles 70 et 71 imposent aux opérateurs de télécommunications, et aux entreprises du numérique, d'être des agents de la censure, en les obligeant à prévoir des dispositifs permettant de filtrer le contenu accessible aux utilisateurs d'Internet, sous peine d'amende, voire d'emprisonnement. Ce type de disposition n'a pas sa place dans une société ouverte et démocratique.

C. Une loi qui criminalise les lanceurs d'alerte

En réprimant la trahison et l'espionnage, c'est-a-dire le fait pour un national ou un étranger de posséder et livrer des informations marquées du sceau du secret à une puissance étrangère, les articles 37 et 38 du projet de loi s'apparentent à une forme de prémunition contre les lanceurs d'alerte, sans pour autant que ne soit prévue des dispositions visant à assurer une protection juridique de ceux-ci.

Le rôle de ces derniers dans l'exigence de transparence, de bonne gouvernance qui doivent prévaloir dans toute démocratie saine devrait assurer à ceux-ci une protection juridique. C'est

ce que défend également David Kaye, Rapporteur spécial de l'ONU pour la la liberté d'expression, dans son dernier rapport datant d'octobre 2015[2] : se fondant notamment sur l'article 19 de de la Déclaration Universelle des Droits de l'Homme, que la République de Guinée a signée et ratifée, Mr Kaye affirme : *"Les États peuvent restreindre l'accès à l'information dans des domaines spécifiques et des circonstances strictement définies, mais la divulgation des informations relatives aux droits de l'homme ou de violations du droit humanitaire ne devrait jamais être la base des sanctions de toute nature,"* .

Il conviendrait donc en l'espèce que le projet de loi guinéen circonscrive mieux les circonstances et les domaines dans lesquels une trahison ou un acte d'espionnage peuvent être identifiés, et prévoit un dispositif de protection des lanceurs d'alerte.

II. Une protection des données personnelles et de la vie privée peu adaptées aux enjeux actuels et futurs du numérique

La deuxième partie du projet de loi est consacrée à la protection des données à caractère personnel. S'il faut féliciter la décision du Gouvernement Guinéen de légiférer sur cette question essentielle à l'ère du numérique, Internet Sans Frontières ne peut que constater que les dispositions proposées à la discussion ne répondent pas aux enjeux et défis actuels.

A. Un projet de loi attendu

Le modèle économique des entreprises du numérique dépend de leur capacité à capter et à exploiter les données personnelles de leurs utilisateurs. Les capitalisations boursières faramineuses de sociétés comme Facebook, Google, ou encore Twitter, ne trompent pas : les données personnelles de l'utilisateur représentent l'or noir du 21è siècle.

[2]New UN report on sources and whistlblowers
http://ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=16635&LangID=E

Il était donc urgent que la République de Guinée se dote d'un dispositif pour encadrer la collecte, le traitement et l'exploitation des données personnelles des citoyens guinéens. L'instauration d'un correspondant à la protection des données personnelles à l'article 14, et la création d'une autorité en charge de la protection des données à caractère personnel représentent des étapes essentielles prises par le Gouvernement, et qu'Internet Sans Frontières ne peut que saluer.

Mais le projet de loi s'inspire de modèles qui ont prouvé leur insuffisance face aux nouveaux enjeux et défis posés par l'exploitation des données personnelles des utilisateurs d'Internet.

B. Un dispositif législatif obsolète face aux nouveaux enjeux

Face à l'insuffisance des dispositifs législatifs en vigueur pour assurer la protection de la vie privée et des données personnelles des utilisateurs européens des services offerts par les entreprises opérant sur le cyberespace, l'Union européenne vient d'adopter un règlement dont peuvent s'inspirer les législateurs africains, et guinéens plus précisément.

Les nouveaux enjeux et défis posés par l'économie numérique sur la vie privée des utilisateurs exigent des législateurs anticipation et innovation dans la rédaction des textes, pour imposer aux entreprises du numérique de placer au cœur de leur activité la protection des données personnelles de leurs internautes. Le régime de déclaration, et la légalité de la finalité du traitement, tel que prévu par le projet de loi guinéen, ne suffisent pas pour suffisamment protéger la vie privée numérique des citoyens guinéens.

Des concepts comme « *Privacy by default* », qui impose au responsable de traitement l'application des mesures afin d'assurer que, par défaut, seules seront traitées les données à caractère personnel nécessaires à chaque finalité spécifique du traitement, ou encore le principe d'extraterritorialité de l'application des normes, qui soumet les entreprises proposant des services sur le marché d'un espace territorial spécifique aux règles en vigueur dans ledit territoire, peu importe que ces entreprises ont leur siège social dans un espace tiers, font partie d'un arsenal dont les législateurs guinéens auraient pu s'inspirer pour adopter des normes adaptées aux enjeux actuels et futurs.

Internet Sans Frontières ne peut donc qu'encourager le Gouvernement guinéen à réfléchir de manière plus approfondie au dispositif de protection des données personnelles des utilisateurs guinéens de services proposés par les entreprises opérant dans le cyberespace.

Enfin, l'efficacité des lois relatives à la protection de la vie privée et des données personnelles dépend de la capacité à inclure les acteurs du marché, et les acteurs représentant les utilisateurs dans le processus de création de la norme. Internet Sans Frontières constate que cela n'a pas été le cas en l'espèce en République de Guinée.

Conclusion

Le projet de loi présenté par le Gouvernement de la république de Guinée pour lutter contre la cybercriminalité et assurer la protection des données personnelles est une avancée notable dans la prise en compte des enjeux posés par la nouvelle société de l'information et la pénétration des TIC dans le quotidien de millions de citoyens guinéens.

Mais ce texte souffre de nombreuses insuffisances dans la prise en compte des exigences démocratiques en ce qui concerne la lutte contre la cybercriminalité, et dans la capacité d'anticipation des enjeux et défis, actuels et futurs, posés par la collecte, le traitement, et l'exploitation des données à caractère personnel à l'ère du numérique.