



Surveillance numérique pour combattre la COVID-19 : Le droit à la vie privée et le droit à l'information en péril au Sénégal

AUTEUR: Ndiaga Gueye | PAYS: Sénégal

INTRODUCTION

Pour lutter contre la COVID-19 de nombreux pays ont recours aux technologies numériques de surveillance des populations.

En effet, suite à la progression exponentielle du nombre de personnes porteuses de cette maladie, ayant comme conséquence une crise sanitaire mondiale, un nombre de plus en plus important de pays dans le monde prend des mesures liées aux technologies digitales pour mettre sous surveillance leur propre population en vue de stopper la propagation du virus.

Pour atteindre cet objectif, selon le contexte propre à chaque pays, des moyens juridiques et des modalités techniques variées sont mises en œuvre, soit pour vérifier le respect des mesures de quarantaine de certaines personnes infectées ne nécessitant pas de soins intensifs, soit pour découvrir le trajet de personnes ayant été en contact avec une personne diagnostiquée positive au coronavirus.

Parmi les technologies de surveillance numérique utilisée actuellement dans plusieurs pays dans le monde, il y a le « contact tracing » appelé aussi « backtracking » ou traçage numérique.

Pour mieux comprendre cette technologie du traçage numérique, une présentation en sera faite dans un premier temps mais aussi les dispositions juridiques sur lesquelles peuvent s'appuyer les autorités sénégalaises pour justifier son utilisation pour retracer les cas contacts des personnes infectées à la COVID-19. Dans un second temps, une analyse de l'impact de l'utilisation du traçage numérique sur le droit à la vie privée et le droit à la protection des données à caractère personnel sera effectuée tout en relevant l'opacité gouvernementale sur cette question.

Enfin, dans une troisième partie, des recommandations sont formulées afin d'assurer une réponse du gouvernement du Sénégal à la COVID-19 en utilisant la surveillance numérique dans le respect des droits humains en ligne et hors ligne.

TRAÇAGE NUMÉRIQUE

Le traçage numérique consiste à collecter et traiter les données des appels téléphoniques et de géolocalisation des téléphones mobiles pour retracer les mouvements des individus testés positifs à la COVID-19.

Lorsque qu'une personne se déplace dans le cadre de ses activités quotidiennes, le signal émis par son téléphone mobile passe d'une antenne-relais à une autre. En s'appuyant sur le bordage de ce terminal les opérateurs sont en mesure de visualiser et suivre les déplacements de leurs clients.

Ainsi donc, pour repérer les personnes susceptibles d'avoir été exposées à un porteur du virus, les opérateurs de téléphonie mobile utilisent en effet des informations collectées grâce aux données personnelles de leurs clients et à la géolocalisation de leurs téléphones portables. Ils sont ainsi tracés et mis sous surveillance au quotidien.

Aussi, il est possible, non seulement d'identifier les personnes qui doivent être mises en quarantaine de toute urgence, car elles ont été en contact avec des individus porteurs du virus, mais aussi de détecter les zones à risque dans un pays où le virus pourrait se propager.

CADRE LÉGAL DE SURVEILLANCE NUMÉRIQUE

Pour utiliser un tel dispositif de traçage numérique au Sénégal, le ministère de la Santé transmet les informations sur les personnes testées positives au ministère de l'Intérieur qui s'appuie sur les opérateurs de téléphonie mobile pour identifier et localiser tous les cas suspects.

Les fondements juridiques ne font pas défaut au Sénégal pour justifier la mise en œuvre d'une telle stratégie numérique d'identification des personnes ayant été au contact de personnes infectées.

L'article 1er de la loi n° 2016-33 du 14 décembre 2016¹ relative aux Services de renseignement, votée dans le cadre de la lutte antiterroriste, dispose :

Les services de renseignement ont pour mission commune la recherche, le recueil, l'exploitation et la mise à la disposition des autorités de décision des renseignements relatifs aux menaces contre la sécurité et les intérêts fondamentaux de la Nation. Les besoins spécifiques et les priorités en matière de renseignement sont précisés dans un plan national de renseignement.

Cette disposition permet au gouvernement du Sénégal de surveiller la population pour notamment faire face aux menaces contre la sécurité et les intérêts fondamentaux de la Nation en mettant en œuvre l'article 10 de la loi sur le renseignement :

Les services spéciaux de renseignement peuvent, lorsqu'ils disposent d'indices relatifs à l'une des menaces prévues à l'article 2 et en l'absence de tout autre moyen, recourir à des procédés techniques, intrusifs, de surveillance ou de localisation pour recueillir les renseignements utiles à la neutralisation de la menace.

¹ <http://www.jo.gouv.sn/spip.php?article10999>

Même si une crise sanitaire n'est pas mentionnée explicitement, une menace contre les intérêts fondamentaux de la Nation peut justifier aux yeux du gouvernement du Sénégal le recours aux dispositifs techniques prévus par la disposition ci-dessus.

Cette disposition qui autorise la surveillance, est renforcée par l'article 90-11 et suivants de la loi n° 2016-30 du 08 novembre 2016 portant Code de procédure pénale² qui autorise le juge d'instruction ou l'officier de police judiciaire sur délégation judiciaire ou sur autorisation et sous le contrôle du procureur de la République à adresser des réquisitions aux opérateurs de télécommunications et aux fournisseurs de service ou de réseaux de télécommunications aux fins de communication de toutes informations utiles à l'enquête.

L'article 20 de la loi n°2018-28 du 12 décembre 2018 portant Code des Communications électroniques³ va également dans le sens d'une légalisation de la surveillance numérique :

Conformément aux dispositions des articles 90-11 et suivants du code de procédure pénale, les opérateurs et fournisseurs de services sur demande des autorités judiciaires :

- Communiquent les données informatiques spécifiées en leur possession ou leur contrôle qui sont stockées dans un système informatique ou un support de stockage informatique ;
- Communiquent les données en leur possession ou sous leur contrôle relatives à leurs abonnés ;
- Répondent aux réquisitions aux fins de communication de toutes informations utiles à la manifestation de la vérité stockées dans le ou les systèmes informatiques qu'ils administrent.

Les opérateurs de communications électroniques et les fournisseurs de services ou de réseaux de communications électroniques sont tenus de mettre les informations requises à la disposition des autorités susmentionnées.

Cette collecte de données personnelles par la mise en œuvre de ce cadre légal serait de surcroît conforme à la loi n° 2008-12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel.⁴

En effet, les données de santé que révélerait une telle surveillance numérique des populations peuvent bien être traitées, d'abord pour le motif suivant : «le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou est

2 <https://www.sec.gouv.sn/sites/default/files/loisetdecrets/Loi%20n%C2%B0%202016-30%20du%2008%20novembre%202016%20modifiant%20la%20Loi%20n%C2%B0%2065-61%20du%2021%20juillet%201965%20portant%20Code%20de%20proc%C3%A8dure%20p%C3%A9nale.pdf>

3 <http://www.numerique.gouv.sn/mediatheque/documentation/loi-n%C2%B02018-28-du-12-d%C3%A9cembre-2018-portant-code-des-communications>

4 <https://www.cdp.sn/content/loi-n%C2%B0-2008-12-du-25-janvier-2008-portant-sur-la-protection-des-donn%C3%A9es-%C3%A0-caract%C3%A8re>

effectué par une autorité publique ou est assigné par une autorité publique au responsable du traitement ou à un tiers, auquel les données sont communiquées», article 41, alinéa 9. Ensuite, elles doivent être «nécessaires à la promotion et à la protection de la santé publique y compris le dépistage», article 43, alinéa 5. Et enfin, «lorsqu'il est nécessaire aux fins de médecine préventive, de diagnostics médicaux, de l'administration de soins ou de traitements soit à la personne concernée, soit de son parent ou lorsque les services de santé agissent dans l'intérêt de la personne concernée. Les données sont traitées sous la surveillance d'un professionnel des soins de santé qui est soumis au secret professionnel», article 43, alinéa 8.

Ainsi donc, tous les éléments juridiques sont déjà mis en place pour permettre au gouvernement du Sénégal d'utiliser ces pouvoirs de surveillance pour identifier les personnes ayant été en contact avec les personnes porteuses du virus.

OPACITÉ GOUVERNEMENTALE

Toutefois, l'Association des Utilisateurs des Technologies de l'Information et de la Communication (ASUTIC) n'a, à ce jour, aucune information officielle du gouvernement du Sénégal permettant d'affirmer l'utilisation de ces pouvoirs démesurés de surveillance des populations, conférés par l'Assemblée nationale depuis 2016, dans le cadre de la lutte contre la COVID-19.

Néanmoins, depuis le début de l'épidémie au Sénégal le 02 mars 2020, les autorités du ministère de la Santé communiquent sur le nombre de cas contacts qu'elles sont en train de suivre.

Aussi, l'annonce par le ministère de la Santé du Sénégal du nombre de cas contacts suivis, qui étaient de 1875 au 15 avril 2020⁵, révèle que la stratégie de traçage numérique a été adoptée par les autorités, en sus, du suivi de contacts traditionnel basé sur l'interrogatoire de la personne infectée.

Pour procéder au traçage numérique, le ministère de la Santé du Sénégal transmet d'abord, la liste contenant les informations sur les personnes testées positives au ministère de l'Intérieur du Sénégal, à savoir, nom et prénom, numéro de téléphone mobile et adresse du domicile, ensuite ce dernier s'appuie sur les opérateurs de téléphonie mobile pour leur identification et leur localisation.

Aussi, se pose la question de la mise en place d'un tel dispositif de collecte et de traitement des données personnelles de géolocalisation à des fins de santé publique sans risquer un impact disproportionné sur les droits humains en ligne, en particulier, sur le droit à la vie privée et la protection des données à caractère personnel.

La Commission de Protection des Données Personnelles (CDP), qui est l'autorité au Sénégal en charge de l'application de la loi n° 2008-12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel, a publié un communiqué le 24 avril 2020 dans lequel elle rappelle que : « la situation

⁵ <https://twitter.com/MinisteredelaS1/status/1250535918324387845>

actuelle d'urgence sanitaire, la protection des libertés individuelles et des droits fondamentaux, notamment la vie privée demeure applicable, et ne peut être suspendue. Cependant, des mesures dérogatoires respectueuses de la loi 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel ou d'autres dispositions législatives ou réglementaires applicables peuvent être envisagées».

Dans son communiqué, la CDP n'a en fait que rappeler la légalité de la surveillance numérique au Sénégal. Elle n'a, à aucun moment, donné des informations sur les dispositifs et les techniques d'identification et de suivi des personnes infectées mises en œuvre par le gouvernement du Sénégal sur lesquelles elle a été consultée par les autorités.

La CDP a tout au plus souligné «que les solutions les moins intrusives pour la vie privée des personnes doivent toujours être privilégiées. Aussi, la Commission préconise que la dimension éthique soit systématiquement prise en charge par tous les acteurs engagés dans le processus de lutte contre le Covid-19».

Cette opacité gouvernementale sur les systèmes de surveillance numérique utilisés doit nous pousser à être particulièrement vigilants pour limiter le potentiel intrusif de ces dispositifs pour préserver l'équilibre entre les droits individuels et l'intérêt général.

LES MENACES SUR LES DROITS HUMAINS EN LIGNE

Le manque de transparence du gouvernement du Sénégal sur les dispositifs techniques d'identification et de suivi des personnes infectées constitue une atteinte au droit à l'information, un des 13 principes de la Déclaration africaine des droits et libertés de l'internet⁶.

Le principe 4 de la Déclaration africaine des droits et libertés de l'internet relatif au droit à l'information stipule :

Tout individu a le droit d'accéder à l'information sur l'internet. L'internet doit être disponible de façon continue pour faciliter la libre circulation de l'information. Toute information, y compris celle générée par des activités de recherche scientifique et sociale, produite avec le soutien des fonds publics, doit être gratuitement accessible à tous.

En outre, il met en péril le droit à la vie privée et à la protection des données à caractère personnel de la Déclaration Africaine.

En effet, le principe 8 dispose :

Toute personne a droit à la vie privée en ligne, notamment le droit de contrôler la façon dont ses données personnelles sont collectées, utilisées, divulguées, conservées et éliminées. Toute personne a le droit de

⁶ <https://africaninternetrights.org/fr/declaration>

communiquer anonymement sur l'Internet, et d'utiliser la technologie appropriée pour assurer une communication sécurisée, privée et anonyme.

Le droit à la vie privée sur internet ne peut être soumis à aucune restriction, sauf celles prévues par la loi, pour un objectif légitime, qui sont nécessaires et proportionnées dans une société démocratique, conformément aux normes internationales en matière de droits de l'homme.

Les données collectées et traitées par l'utilisation de ces technologies de surveillance numérique sont des données de santé classées comme des données sensibles. Leur traitement est en principe interdit par la loi sur la protection des données personnelles au Sénégal.

Cependant, leur utilisation peut être légale pour motifs d'intérêt public avec le consentement des personnes concernées.

Répondre à cette double exigence légale est difficile dans le contexte africain, notamment au Sénégal en raison du manque de culture numérique de la population. En effet, le taux d'analphabétisme est élevé (55%)⁷.

Par conséquent, il est sûr et évident que les citoyens ne seront pas en mesure de comprendre les principes de fonctionnement de ces technologies et les conséquences de leur utilisation sur leurs données personnelles et leur vie privée. Ainsi, ils ne pourront pas donner un consentement éclairé.

De plus, rien dans l'utilisation de ces technologies ne garantit l'anonymat, il y a donc toujours une possibilité d'être identifié. La non-protection des données personnelles des personnes permet de connaître la personne infectée par la COVID-19.

Ce sera une violation du droit à la vie privée, ce qui pourrait être une source de stigmatisation ou même de discrimination sociale. C'est un danger pour la cohésion sociale.

Le niveau de vigilance doit être élevé car le gouvernement du Sénégal n'informe jamais la population quant à la façon dont il utilise concrètement ce cadre légal de surveillance, une totale opacité est entretenue.

Par conséquent, il nous faut être très attentif à l'utilisation de ces dispositifs de dépistage afin d'éviter le risque d'entrer dans une nouvelle ère de surveillance numérique invasive des Sénégalais.

Le gouvernement du Sénégal doit s'engager à faire immédiatement la transparence sur toutes les mesures de surveillance numérique de la population mises en œuvre ou qu'il compte mettre en œuvre pour lutter contre la propagation de la COVID-19.

Ainsi, elles seraient dûment examinées par les citoyens pour limiter les risques d'abus qui découleraient des pouvoirs exorbitants que lui confère ce cadre légal en attendant que les lois votées depuis 2016 au Sénégal, attentatoires aux droits numériques⁸, soient battues en brèche.

7 www.ansd.sn/ressources/RGPHAE-2013/ressources/doc/pdf/3.pdf

8 <https://droitsnumeriques.sn/etat-des-lieux>



Surveillance Numérique

Dans les principes fondamentaux de la société de l'information au Sénégal, celui de sécurité vise à garantir les droits fondamentaux des personnes et les droits sur les biens :

Le principe de sécurité vise à établir la confiance de l'ensemble des acteurs dans l'organisation et le fonctionnement des infrastructures et des systèmes de la société de l'information. Il garantit les droits fondamentaux des personnes et les droits sur les biens et sauvegarde l'ordre public ainsi que les valeurs fondamentales de la société de l'information dans un environnement transparent et prévisible qui reflète la situation réelle du pays.

La sécurité est un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives.

L'État a le devoir d'assurer la sécurité en veillant, sur l'ensemble du territoire de la République, à la défense des institutions et des intérêts nationaux, au respect des lois, au maintien de la paix et de l'ordre public, à la protection des personnes et des biens.

Il associe à la politique de sécurité dans la société de l'information, les collectivités locales, les acteurs du secteur public comme privé et les organisations de la société civile, confrontés aux manifestations de la cybercriminalité sous toutes ses formes⁹.

En d'autres termes, il ne peut être mis en place au Sénégal au nom de la sécurité un dispositif numérique qui remette en cause le respect du droit à la vie privée y compris la confidentialité des communications et la protection de leurs droits et libertés à l'égard de tout traitement de données à caractère personnel.

Sur le fondement de cette exigence légale, ASUTIC, a procédé à la signature de la déclaration conjointe de la société civile¹⁰, qui rappelle aux gouvernements

⁹ Article 6 de la Loi n° 2008-10 du 25 janvier 2008 portant loi d'orientation sur la Société de l'Information.
<http://www.jo.gouv.sn/spip.php?article6661>

¹⁰ <https://www.hrw.org/fr/news/2020/04/02/covid-19-declaration-conjointe-de-la-societe-civile>

que le recours aux technologies de surveillance numérique pour combattre la pandémie doit se faire dans le respect des droits humains.

RECOMMANDATIONS

Au regard de tout ce qui précède, ASUTIC formule les recommandations suivantes au gouvernement du Sénégal dans l'utilisation de la surveillance numérique pour lutter contre la propagation de la COVID-19 dans le pays :

- Faire la transparence sur toutes les mesures de surveillance numérique de la population mises en œuvre ou qu'il compte mettre en œuvre pour lutter contre la propagation de la COVID-19, par le respect du droit à l'information consacré par la constitution du Sénégal;
- De se garder de penser que le numérique est la solution principale à la propagation du virus ;
- Recourir aux technologies de surveillance numérique dans le respect des droits humains, en particulier, le droit à la vie privée et à la protection des données à caractère personnel ;
- S'inspirer dans la lutte contre la COVID-19 du succès de pays démocratiques plutôt que de faire du copier-coller de mesures en provenance de pays totalitaires ayant des sociétés complètement différentes de la nôtre ;
- D'associer à la politique de sécurité sanitaire de lutte contre la COVID-19 dans la société de l'information, les organisations de la société civile.