CNCDH

COMMISSION NATIONALE
CONSULTATIVE
DES DROITS DE L'HOMME

RÉPUBLIQUE FRANÇAISE

AVIS

AVIS SUR LE SUIVI NUMÉRIQUE DES PERSONNES

28 AVRIL 2020

L'avis sur le suivi numérique des personnes
a été adopté lors de l'Assemblée plénière du 28 avril 2020.
(Adoption 45 voix « pour », 9 abstentions)

TABLE DES MATIÈRES

La France fait face à une crise sanitaire sans précédent sous la Ve République. Afin d'enrayer la propagation du virus et de soulager le personnel soignant rapidement débordé par le nombre de personnes hospitalisées des suites d'une contamination par le Covid-19, le gouvernement a instauré le 17 mars un confinement de l'ensemble de la population. Le confinement a donné lieu à une augmentation des usages d'internet et des technologies numériques et notamment à l'utilisation de nouvelles technologies de surveillance, en particulier de drones chargés de rappeler à l'ordre des personnes se trouvant dans l'espace public. Alors que le confinement sera progressivement levé à partir du 11 mai prochain, comme l'a annoncé le Président de la République lors de son allocution du 13 avril, le gouvernement a annoncé son intention de recourir après cette date, à l'instar d'autres pays comme Singapour, à une application de suivi des interactions sociales des personnes (« contact tracing » ou « proximity tracing »), nommée STOPCOVID. La CNCDH s'inquiète du fait que la gestion de la crise sanitaire puisse donner lieu à l'expérimentation par les pouvoirs publics de nouvelles technologies dont l'impact sur les droits et libertés fondamentaux seraient considérables.

Forte d'une réflexion engagée dans le passé à l'égard des enjeux attachés au développement de ces outils numériques et aux questions relatives aux données personnelles[1], et bien que les détails de l'application STOPCOVID ne soient pas encore totalement connus, la CNCDH a décidé de s'auto-saisir de la question de l'utilisation d'outils numériques de suivi des personnes en raison des risques d'atteintes aux libertés individuelles et collectives, notamment le respect de la vie privée et la protection des données personnelles, et de discriminations.

La règlementation européenne – le Règlement général de protection des données (RGPD) et la directive e-privacy[2] – et la législation française[3] offrent un cadre juridique de référence protecteur des données personnelles : « *les citoyens doivent savoir quelles données sont susceptibles d'être traitées, par qui, dans quel but, à quelles conditions et avec qui ces données peuvent être partagées* » comme l'a rappelé la présidente de la CNIL le 8 avril devant l'Assemblée nationale[4]. Le gouvernement s'est défendu de toute atteinte à la protection des données personnelles, en rappelant son attachement au cadre juridique européen et en insistant sur un certain nombre de garanties[5,]

1. Voir not : CNCDH, *Avis sur la protection de la vie privée à l'ère du numérique,* adopté le 22 mai 2018. , JORF n°0126 du 3 juin 2018 texte n° 63.
2. Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 r*elatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* et la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 c*oncernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.*
3. La loi n° 78-17 du 6 janvier 1978 r*elative à l'informatique, aux fichiers et aux libertés.*
4. Ces droits sont énumérés aux articles 12 et s. du RGPD.
5. Assemblée nationale, Commission des lois, Audition de Cédric O, 9 avril 2020. Sur ce point, voir également la délibération de la Commission nationale de l'informatique et des libertés (CNIL) n° 2020-046 du 24 avril 2020 et l'avis du Conseil national du numérique (CNNum) du 24 avril 2020.

notamment :

- L'acquisition volontaire de l'application ;
- L'anonymat des données ;
- L'absence de données de géolocalisation mais un historique des relations sociales (la technologie BLUETOOTH cible la distance entre les personnes, pas leur emplacement) ;
- La conservation des données dans le téléphone ;
- L'application sera en open source afin que chacun puisse y accéder et l'analyser.

La CNCDH met en exergue le caractère transversal des atteintes potentielles aux droits de l'homme pouvant résulter de telles mesures de suivi. Ces atteintes peuvent évidemment concerner le droit à la protection des données personnelles, ce qui appelle une vigilance toute particulière à cet égard. Toutefois, l'éventuelle conformité à la seule réglementation sur la protection des données personnelles n'équivaut pas à un respect des droits et libertés fondamentaux. Des atteintes pourraient être également portées à la protection de la vie privée ainsi qu'aux libertés collectives, être source de discriminations, voire menacer la cohésion sociale. La CNCDH considère que l'intérêt et l'efficacité d'un tel suivi pour endiguer la propagation du virus sont trop incertains en comparaison de la menace disproportionnée qu'ils font peser sur les droits et libertés fondamentaux.

La CNCDH met en garde contre les effets d'une utilisation de ces technologies, aujourd'hui circonscrites à l'identification des interactions sociales à des fins de santé publique, mais susceptibles d'ouvrir à l'avenir sur la poursuite d'autres objectifs, selon des modalités combinant le suivi de contacts et le traçage des personnes[6], et mettant alors gravement en danger les droits et libertés fondamentaux. Ce qui est en jeu ici, ce n'est pas seulement l'utilisation d'un outil de suivi numérique – STOPCOVID – pour endiguer la propagation d'un virus, c'est plus largement l'opportunité et la légitimité de l'utilisation de l'Intelligence artificielle (AI) et des données personnelles à des fins plus larges de surveillance de la population et des contenus, avec un risque d'atteinte transversale aux droits et libertés fondamentaux.

La CNCDH tient enfin à souligner qu'il s'agit de sujets de préoccupation majeure dans une société démocratique, nécessitant une transparence accrue, des garanties suffisantes pour préserver la souveraineté numérique, ainsi que des mesures fortes en faveur de l'éducation et la formation au numérique.

6. A la différence du suivi de contacts des personnes, le traçage des personnes (« tracking ») repose sur des données de géolocalisation.

I - LE TRAÇAGE POUR LIMITER LA PROPAGATION DU COVID-19 : UNE ATTEINTE DISPROPORTIONNÉE AUX DROITS ET LIBERTÉS FONDAMENTAUX

Les principaux éléments mis en avant par le gouvernement pour dissiper les craintes à l'égard de son projet de suivi numérique des personnes, et emporter l'adhésion de la population, suscitent un certain nombre d'interrogations.

Un consentement libre et éclairé sujet à caution

Les données concernant la santé sont des données sensibles, dont le traitement est en principe interdit par l'article 9 RGPD[7]. La mise en place d'une application de suivi de contacts pourrait cependant se fonder sur plusieurs exceptions : notamment le consentement des personnes concernées, ou bien des « motifs d'intérêt public »[8]. Le gouvernement, ainsi que le Président de la République, ont fait valoir à plusieurs reprises que l'utilisation de STOPCOVID reposera sur le volontariat[9]. Reste que pour le RGPD, le consentement de la personne doit répondre à certaines conditions : il doit être libre et éclairé.

Satisfaire à cette double exigence paraît particulièrement compliqué dans le contexte actuel. D'abord, il n'est pas certain que les citoyens soient en mesure de saisir tant les ressorts technologiques, que les implications d'une telle application. De ce point de vue, il est fondamental pour la CNCDH que les utilisateurs disposent d'éléments d'information suffisants, clairs et accessibles sur ce qu'elle permet exactement de faire et ses limites. Pour que le consentement soit parfaitement éclairé, il faudrait encore que chaque personne décidant d'adhérer à l'application soit en capacité de comprendre de telles informations. Cela supposerait donc de renforcer, au-delà de l'application STOPCOVID, l'éducation de tous à ces enjeux, des plus jeunes aux plus âgés et ce, tout au long de la vie[10].

Ensuite, la CNCDH s'interroge sur l'authenticité d'un consentement libre dans le contexte actuel. Comme le soulignait la présidente de la CNIL devant les députés, « *le*

7. Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
8. Respectivement, art. 9, 2, a) et g) du RGPD.
9. Assemblée nationale, Commission des lois, Audition de Cédric O, 9 avril 2020.
10. La CNCDH renouvelle cette recommandation depuis de nombreuses années : *Avis sur la lutte contre les discours de haine sur internet*, février 2015 , JORF n°0158 du 10 juillet 2015 texte n°125; *Avis sur la protection de la vie privée à l'ère du numérique*, mai 2018, JORF n°0126 du 3 juin 2018 texte n° 63 ; *Avis relatif à la proposition de loi visant à lutter contre la haine sur internet*, juillet 2019, JORF n°0161 du 13 juillet 2019 texte n°107.

refus de consentir ne doit pas exposer la personne à des conséquences négatives »[11]. Le gouvernement ne paraît manifestement pas conditionner le déconfinement des personnes à l'utilisation de l'application. La CNCDH souligne que cela s'oppose également à ce qu'un employeur impose à son salarié de télécharger et d'utiliser l'application, ou que cettte dernière conditionne l'accès à l'espace public[12]. D'autres facteurs de contrainte sont néanmoins à craindre, tenant notamment aux risques de pression sociale, tant à titre individuel que familial[13] ou professionnel, pouvant s'exercer dans un contexte de crise sanitaire particulièrement aigüe. L'impératif de santé publique, la lutte contre la propagation du Covid-19, la préservation du personnel soignant, sans doute invoqués à l'appui de la mise en place de l'application, constitueront autant de leitmotivs qui pèseront sur le choix des individus, appelés à agir en citoyens responsables[14]. Par ailleurs, la CNCDH craint des risques de stigmatisation et de harcèlement à l'égard de tout individu qui refuserait d'adhérer à ces mesures de suivi[15].

Une autre difficulté tiendrait à la possibilité pour les personnes vulnérables, notamment les mineurs ou les personnes en situation de handicap, d'exprimer leur consentement pour adhérer à cette mesure volontaire.

Un anonymat relatif

Si l'anonymat peut représenter une garantie pour la protection des données personnelles, il n'est que rarement suffisant. Un certain nombre d'études ont en effet montré que l'anonymat des données offre rarement une garantie effective contre les possibilités de ré-identification des personnes, notamment à partir d'un recoupement de plusieurs bases de données[16], ou par la combinaison de données techniques[17]. Le pseudonymat, prévu par le projet d'application STOPCOVID, ne garantit quant à lui qu'une moindre protection des données personnelles. Outre les risques de ré-identification possibles par les acteurs en charge de la mise en œuvre de l'application, ou de détournement par des tiers malveillants, la CNCDH craint que les personnes

11. Assemblée nationale, Commission des lois, Audition de M.-L. Denis, 8 avril 2020. Ce que souligne également, le Comité européen de protection des données (CEPD) : EDPB, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, 21 avril 2020, pt 24. Dans le même sens, voir la Délibération n° 2020-046 de la CNIL.
12. La Délibération n°2020-046 de la CNIL rappelle de telles interdictions.
13. Par exemple, la pression exercée par les parents sur les enfants.
14. Dans son premier bulletin de veille le Comité éthique du numérique relevait que la « p*ortée du consentement sur les proches et autres contacts de la personne concernée, ou encore l'attribution de la responsabilité à la personne plutôt qu'à la collectivité, sont d'importants sujets de préoccupation éthique* » : Comité national pilote d'éthique du numérique, « Réflexions et points d'alerte sur les enjeux d'éthique du numérique en situation de crise sanitaire aiguë », Bulletin de veille n°1, 7 avril.
15. Voir à cet égard certaines pressions exercées sur le personnel soignant par leur voisinage à l'occasion de la crise sanitaire actuelle.
16. R. Chatellier, « Nouvelles frontières des données personnelles », CNIL, 2016.
17. Par exemple, une adresse IP, données antennes, wi-fi.

destinataires d'une notification puissent dans certains cas, par un jeu de déduction, deviner l'identité de la personne contaminée à l'origine de la notification18. Or, la préservation de la confidentialité de ces informations est cruciale pour prévenir toute forme de discrimination[19].

Des effets sur la cohésion sociale

La CNCDH s'inquiète également de l'impact d'une telle mesure de suivi sur le comportement des personnes : les résultats communiqués par l'application pourraient induire des réactions de suspicion à l'égard des autres (qui m'a contaminé ?) ou susciter de la stigmatisation et de l'exclusion à l'égard des personnes suspectées d'être l'agent contaminant. En modifiant notre rapport aux autres et au monde, en suscitant des réactions d'anxiété, ou de stigmatisation et de discriminations à l'égard de certaines catégories de personnes, cette mesure représenterait une menace tant pour le respect de la vie privée, entendue largement au sens de la jurisprudence de la Cour européenne des droits de l'homme[20], que pour les valeurs républicaines de dignité, de liberté, d'égalité et de fraternité et plus généralement pour préserver la cohésion sociale.

Une temporalité indéterminée

L'examen de la proportionnalité de l'application, tant du point de vue du RGPD – sa durée ne devrait pas excéder celle nécessaire à la réalisation de l'objectif poursuivi – que du point de vue de l'atteinte au respect de la vie privée, implique également de s'interroger sur la durée de la mise en place de l'application. A cet égard, la CNCDH relève qu'il n'existe à l'heure actuelle aucune précision à ce sujet. Puisque le virus pourrait circuler encore longtemps au sein de la population, plusieurs vagues de contamination pouvant survenir, l'application pourrait être maintenue longtemps, bien au-delà de la fin de l'état d'urgence sanitaire ou réactivée lors d'autres crises. Ce faisant, l'application serait davantage exposée à des risques de piratage, laissant craindre des atteintes répétées à la protection des données personnelles.

18. Par exemple, une personne, pour éviter la contamination, ne sort de chez elle que pour faire ses courses à l'épicerie du quartier, tout en s'efforçant de se tenir à distance des personnes qu'elle croise. Si elle reçoit une notification de son téléphone, elle en déduira que la personne contaminée n'est autre que l'épicier. Exemple empruntée à N. X. Bonnetain et autres, « Le traçage anonyme, dangereux oxymore : analyse de risques à destination des non-spécialistes », 21 avril 2020. Disponible à : https://risques-tracage.fr/. D'après ces chercheurs, il serait possible d'envisager des solutions techniques et organisationnelles permettant de réduire un tel risque.
19. A. Courmont, « Coronoptiques : dépister la population, rendre visible le virus », LINC, 10 avril 2020.
20. Au fil de sa jurisprudence, la Cour européenne a fait évolué sa compréhension de la notion, en passant d'une conception restrictive, cantonnée dans la défense à l'encontre des ingérences étatiques (secret de la correspondance, inviolabilité du domicile, etc.) à une conception plus large « non susceptible d'une définition exhaustive, qui recouvre l'intégrité physique et morale de la personne » et susceptible « d'englober de multiples aspects de l'identité physique et sociale d'un individu » (CEDH, 4 décembre 2008, *S. et Marper c. RU*, req. n° 30562/04 et 30566/04, § 66).

Des effets incertains

La CNCDH s'interroge sur le caractère nécessaire et approprié d'une application de suivi dans la lutte contre l'épidémie dès lors qu'elle porterait atteinte aux droits et libertés fondamentaux. Elle relève qu'il n'existe pas à l'heure actuelle de consensus à l'égard de son efficacité. Pour sa part, la CNIL appelle à la vigilance et souligne que l'application ne peut être déployée que si son utilité est suffisamment avérée et si elle est intégrée dans une stratégie sanitaire globale[21]. D'après certains experts, le taux de participation à l'application requis pour assurer son efficacité est de 60% minimum[22]. Or, il se heurte notamment à un obstacle majeur : la fracture numérique. D'après le baromètre numérique 2019 publié par l'Arcep, 77% de la population française est équipée d'un smartphone[23] : 18 millions de Français sont ainsi exclus du périmètre de ces applications, parmi lesquels des personnes âgées (44% des 70 ans et plus sont équipés) ou des personnes aux revenus moins élevés. Par ailleurs, des problèmes de compatibilité pourraient se poser, notamment, entre les systèmes d'exploitation IOS et Android.

En outre, l'application serait fondée sur des données scientifiques relatives au Covid-19 encore insuffisantes, sachant que le « *modèle de transmission du virus reste très incertain* »[24]. En conséquence de cette incertitude, couplée à une fiabilité toute relative des tests, l'application ne manquerait pas de signaler des « faux positifs » : des personnes penseront à tort avoir été en contact avec des personnes malades. À l'inverse, une personne en contact avec le virus ne serait pas nécessairement avertie par l'application en cas de « faux négatif »[25]. La technologie BLUETOOTH elle-même, fondée sur la distance entre terminaux, ne représente pas un indicateur fiable de

21. Délibération n°2020-046 de la CNIL.
22. D'après une étude parue dans la revue *Science* parue le 31 mars, une telle application est efficace si 60% de la population l'utilise et qu'une campagne de dépistage y est associée (« Quelles données, pour quel suivi ? », Benoît Georges, 1er avril 2020).
23. Se pose la question de la compatibilité de l'application avec les différents systèmes d'exploitation mobile.
24. Le PDG d'Inria – l'établissement public qui supervise le développement de l'application STOPCOVID – précise bien que « *toutes les applications de « proximity tracing » reposent ainsi sur des fonctions de risque, définies, avec les chercheurs en épidémiologie, sur la base de l'état de l'art. Cette connaissance est encore très lacunaire et est susceptible de changer très rapidement, en fonction des retours d'expérience* » : B. Sportisse, « Contact tracing : quelques éléments pour mieux comprendre les enjeux », 18 avril 2020, disponible à : https://www.inria.fr/fr/contact-tracing-bruno-sportisse-pdg-dinria-donne-quelques-elements-pour-mieux-comprendre-les-enjeux
25. Selon le professeur Vincent Thibault, chef de service du laboratoire de virologie au CHU de Rennes, « *sur 100 patients testés négatifs, il est probable que 30 % d'entre eux soient infectés par le virus* ». D. Sergent, « Covid-19, la fiabilité des tests en question », *La Croix*, 29 mars 2020.

contagion[26]. Les erreurs qui pourraient en résulter auront des incidences sur les personnes concernées, sur leur liberté d'aller et venir ou encore sur leur santé.

Enfin, la CNCDH s'interroge sur les conséquences qu'il faudrait tirer d'une notification selon laquelle l'utilisateur a croisé une personne diagnostiquée positive au Covid-19. À s'en tenir à la logique du volontariat actuellement mise en avant par le gouvernement, il appartiendrait à la personne de se faire dépister et, éventuellement, de s'astreindre à un strict confinement. La CNCDH s'inquiète d'une reprise en main du système par les autorités publiques, qui pourraient être tentées de vouloir identifier les personnes à risque et, sur le fondement des dispositions du code de la santé publique, les contraindre à une mise en quarantaine[27]. Un autre motif de préoccupation pour la Commission renvoie à la nature des conséquences d'une notification positive pour un utilisateur ayant été en contact avec une personne contaminée : devrait-il se soumettre à un dépistage obligatoire au risque de faire l'objet de poursuites judiciaires pour atteinte à la vie d'autrui ?

Encore faudrait-il qu'un nombre suffisant de tests soient disponibles et en mesure d'être utilisés. Il faut également ajouter que les porteurs asymptomatiques du virus ne seraient pas, par définition, identifiés comme tels par l'application.

La nécessité d'un débat démocratique

La question de la proportionnalité des risques apportés par cette nouvelle technologie au regard de l'objectif de lutte contre l'épidémie constitue un enjeu essentiel dans un régime démocratique. Même si cela n'est pas exigé par le RGPD, l'application, autant sur le principe que sur ses modalités de mise en œuvre (communication du cahier des charges, suivi des mises à jour pour éviter des dérives dans le temps, ou encore des conditions de la désactivation de l'application à la fin de la crise), devraient donner lieu à un projet de loi afin d'impliquer la représentation nationale dans son processus d'adoption, éventuellement pour le refuser. La CNCDH s'inquiète d'ailleurs, de manière générale, de voir que la crise actuelle donne lieu à une marginalisation du Parlement. Après avoir envisagé dans un premier temps de ne pas

26. Sur ce point, voir not. Office parlementaire d'évaluation des choix scientifiques et technologiques, *Point sur les technologies de l'information utilisées pour limiter la propagation de l'épidémie de COVID-19*, 11 avril 2020 : « *On notera également que la proximité avec des personnes malades n'est qu'un déterminant très approximatif de la probabilité d'avoir été infecté, étant donné que le port du masque et l'adoption des gestes barrière peuvent prévenir une infection, malgré une proximité avec un cas avéré. A l'inverse, une « distance d'effet » paramétrée à un mètre ignore le risque des contaminations résultant d'une toux importante par une personne ne portant pas de masque. De plus, le contexte est ignoré : le risque de contagion dans un environnement fermé est plus élevé que dans un environnement ouvert, or, le traçage de la proximité relative par BLUETOOTH ne permet pas la contextualisation, contrairement aux traçages GPS* ». Sans compter que la précision du BLUETOOTH varie selon le type de téléphone. Sur ces différents éléments, voir aussi l'avis du CNNum, p. 16.

27. Pour rappel, l'article L. 3131-1 du CSP, tel que modifié par la loi du 23 mars 2020, habilite le ministre de la Santé et les préfets à prendre des mesures restrictives des libertés après la fin de l'état d'urgence sanitaire, « a*fin d'assurer la disparition durable de la situation de crise sanitaire* ».

soumettre cette question au vote de ce dernier, le gouvernement s'est heureusement ravisé. Pour autant, le débat démocratique ne saurait être suffisant en l'absence d'un contrôle indépendant de la mise en œuvre des mesures de suivi[28].

Quand bien même le gouvernement opterait pour une application adossée à un objectif légitime de santé publique, pour un temps limité, en garantissant un niveau de sécurité suffisant pour toutes les données collectées, sous le contrôle d'organismes indépendants, elle ne saurait se passer d'une stratégie de déconfinement plus large, associée à une massification des tests et au port de masques, s'inscrivant dans une politique de santé publique d'envergure[29]. À plus long terme, cette première utilisation pourrait ouvrir la voie à d'autres types d'utilisations d'outils numériques de suivi susceptibles d'engendrer des conséquences plus graves pour les droits et libertés fondamentaux. La CNCDH souhaiterait à cet égard exposer un certain nombre de préoccupations.

II - DES MOTIFS DE PRÉOCCUPATION PLUS LARGES À L'ÉGARD DU CONTACT TRACING

Effet cliquet

Le recours à un outil numérique dans le contexte actuel bénéficie incontestablement de l'effet légitimant attaché à la protection de la santé publique. Indépendamment des atteintes au respect de la vie privée que l'application envisagée par le gouvernement est susceptible d'occasionner, sans doute serait-elle accueillie favorablement par une grande partie de la population soucieuse d'en finir au plus vite avec l'épidémie. La CNCDH craint que cette acceptabilité sociale ne puisse favoriser à l'avenir, par un effet d'accoutumance, l'usage de ce même type de technologie pour d'autres fins : suivi médical hors Covid-19, contrôle de certaines catégories de personnes (étrangers, manifestants, personnes en MICAS etc.).

Cette crainte est d'autant plus vive que, par le passé, les pouvoirs publics ont pu étendre le champ et les modalités d'utilisation d'une technique à partir du moment où elle a pu être mobilisée dans un premier temps, à titre exceptionnel, pour des fins légitimes[30] : le gouvernement pourrait être tenté d'utiliser la technologie en place pour identifier les interactions sociales d'une personne, dans le cadre d'un contrôle

28. Voir en ce sens l'avis du CNNum, p. 14.
29. En ce sens, la Délibération n° 2020-046 de la CNIL appelle également à « *une vigilance particulière contre la tentation de 'solutionnisme technologique'* ».
30. Cf l'extension des motifs d'utilisation des tests génétiques, des techniques de surveillance, etc.

judiciaire ou d'une mesure individuelle de contrôle administratif (MICAS), au risque de porter gravement atteinte aux droits et libertés fondamentaux. Cette normalisation des mesures d'exception, déjà critiquée dans le passé par la CNCDH[31], pourrait profiter à de futurs gouvernements prompts à sacrifier les droits fondamentaux au nom de l'impératif de sécurité publique. La CNCDH appelle donc les pouvoirs publics à mettre en perspective les effets à long terme induits par le recours au suivi de contacts des personnes, avec ses effets très incertains à court terme sur la propagation du virus.

Et après : des risques d'atteintes transversales aux droits et libertés fondamentaux

Les mesures de suivi individuel ou collectif, afin de limiter la propagation d'une épidémie, pourraient induire des risques de discriminations/stigmatisations en ciblant : certaines zones territoriales, certaines populations, certaines personnes identifiées comme porteuses du virus.

Alors que le gouvernement paraît aujourd'hui présenter un système ayant une portée limitée sur les libertés fondamentales, la CNCDH s'inquiète que cette initiative puisse donner lieu dans le futur à la tentation de se tourner à nouveau vers une solution technologique, ayant déjà fait ses preuves, pour la gestion d'autres domaines que la santé publique : le maintien de l'ordre, la gestion des flux migratoires, etc. Ce n'est plus seulement la protection des données qui serait en cause, mais de nombreux droits et libertés fondamentaux : la liberté d'aller et venir, la liberté de manifester, de se réunir, etc. La Commission redoute plus généralement l'incidence sur les libertés d'un dispositif de surveillance renforcé par l'utilisation d'outils numériques : le sentiment d'être surveillé en permanence risque d'entraver l'exercice effectif des libertés individuelles et collectives.

Les droits économiques et sociaux sont également susceptibles d'être impactés : directement si l'on conditionne par exemple un certain nombre de prestations sociales à l'utilisation d'une appli de suivi ; indirectement en considérant que les outils numériques pourront suppléer des ressources humaines et matérielles amoindries pour des raisons budgétaires.

Souveraineté numérique

Depuis le début de la crise sanitaire, les opérateurs privés multiplient leurs propositions de collaboration à destination des Ètats. En France, selon la Présidente

31. Notamment s'agissant des pouvoirs de police prévus par la loi relative à l'état d'urgence de 1955 qui ont été repris, avec quelques aménagements, dans la loi du 30 octobre 2017 *renforçant la sécurité intérieure et la lutte contre le terrorisme* : CNCDH, *Avis sur le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme,* juillet 2017.

de la CNIL, Orange partage des données de localisation anonymisées avec plusieurs partenaires, dont l'INSERM, afin que les épidémiologistes modélisent la propagation de la maladie[32]. C'est également Orange qui a partagé avec les pouvoirs publics son étude, menée à partir des données de géolocalisation des téléphones de ses abonnés, selon laquelle 17 % des habitants de la métropole du Grand Paris ont quitté leur région entre le 13 et le 20 mars[33]. Si l'implication d'opérateurs privés dans le suivi de la population ne pose a priori pas de problème au regard du respect de la vie privée, puisque les données sont globales (non individualisées) et anonymes, cela pourrait avoir pour effet d'engendrer une défiance d'une partie de la population à l'égard des autorités publiques et des outils numériques.

La technologie retenue par le gouvernement pour son application de suivi numérique des personnes est le BLUETOOTH. Or, laisser le BLUETOOTH activé présente différents risques de sécurité et de détournement. Il est ainsi possible d'identifier les terminaux (téléphones portables, objets connectés, etc.) à proximité, et donc ceux qui utilisent, ou n'utilisent pas l'application. La CNCDH s'inquiète également du nombre limité de systèmes d'exploitation mobile alors que ceux-ci sont en mesure de conditionner l'accès à certaines fonctionnalités du terminal.

Si l'utilisation des technologies de l'IA peut avoir un intérêt incontestable dans la recherche médicale, à partir de l'exploitation des données de santé anonymisées et agrégées, le recours au numérique ne saurait représenter l'élément central d'une stratégie de protection de la santé publique et, dans l'immédiat, d'une stratégie de déconfinement. L'utilisation des outils numériques ne peut pas se substituer à une politique de santé publique ambitieuse (des investissements dans la recherche médicale, un service public hospitalier respectueux du personnel soignant et des patients[34], etc.), mise à mal ces dernières années par des restrictions budgétaires régulières. Au regard du risque élevé d'atteintes à une pluralité de droits et libertés fondamentaux, mais encore de leur absence d'efficacité avérée pour endiguer la propagation de l'épidémie, la CNCDH recommande au gouvernement de ne pas recourir aux mesures de suivi numérique des personnes. Compte tenu de ces risques, la Commission sera particulièrement vigilante à l'égard de l'utilisation des systèmes d'intelligence artificielle à des fins de surveillance des personnes et des contenus[35].

32. Assemblée nationale, Audition de Marie-Laure Denis du 8 avril 2020.
33. M. Untersinger, « Confinement : plus d'un million de Franciliens ont quitté la région parisienne en une semaine », *Le Monde,* 26 mars
34. Voir l'a*vis de la CNCDH, Agir contre les maltraitances dans le système de santé : une nécessité pour respecter les droits fondamentaux*, adopté le 22 mai 2018.
35. Un groupe de travail mène actuellement une réflexion relative à l'impact de l'IA sur les droits et libertés fondamentaux, dans la continuité de l'avis rendu par la CNCDH sur le *projet de loi relatif aux contenus haineux* de juillet 2019.

CNCDH
COMMISSION NATIONALE CONSULTATIVE DES DROITS DE L'HOMME
RÉPUBLIQUE FRANÇAISE

Créée en 1947 sous l'impulsion de René Cassin, **la Commission nationale consultative des droits de l'homme (CNCDH) est l'Institution nationale de promotion et de protection des droits de l'homme française, accréditée de statut A par les Nations unies.**

L'action de la CNCDH s'inscrit dans une quadruple mission :
- Conseiller les pouvoirs publics en matière de droits de l'homme ;
- Contrôler l'effectivité des engagements de la France en matière de droits de l'homme et de droit international humanitaire ;
- Assurer un suivi de la mise en oeuvre par la France des recommandations formulées par les comités de suivi internationaux et régionaux ;

Sensibiliser et éduquer aux droits de l'homme.

L'indépendance de la CNCDH est consacrée par la loi. Son fonctionnement s'appuie sur le principe du pluralisme des idées. Ainsi, seule institution assurant un dialogue continue entre la société civile et les experts français en matière de droits de l'homme, elle est composée de 64 personnalités qualifiées et représentants d'organisations non gouvernementales issues de la société civile.

La CNCDH est le rapporteur national indépendant sur la lutte contre toutes les formes de racisme depuis 1990, sur la lutte contre la traite et l'exploitation des êtres humains depuis 2014, sur la mise en oeuvre des Principes directeurs des Nations unies sur les entreprises et les droits de l'homme depuis 2017, et sur la lutte contre la haine anti-LGBT depuis avril 2018.

20 Avenue Ségur - TSA 40 720 - 75334 PARIS Cedex 07
Tel : 01.42.75.77.09
Mail : cncdh@cncdh.fr
www.cncdh.fr

@CNCDH
@cncdh.france