L'utilisation des données personnelles dans le cadre de la lutte contre l'épidémie de Covid-19, un risque pour les droits et libertés ?

Aurèle Pawlotsky

Electronic version

URL: <http://journals.openedition.org/revdh/9059>

DOI: 10.4000/revdh.9059

ISSN: 2264-119X

Publisher

Centre de recherches et d'études sur les droits fondamentaux

Electronic reference

Aurèle Pawlotsky, « L'utilisation des données personnelles dans le cadre de la lutte contre l'épidémie de Covid-19, un risque pour les droits et libertés ? », *La Revue des droits de l'homme* [Online], Actualités Droits-Libertés, Online since 15 April 2020, connection on 06 November 2020. URL : <http://journals.openedition.org/revdh/9059> ; DOI : <https://doi.org/10.4000/revdh.9059>

This text was automatically generated on 6 November 2020.

Tous droits réservés

L'utilisation des données personnelles dans le cadre de la lutte contre l'épidémie de Covid-19, un risque pour les droits et libertés ?

Aurèle Pawlotsky

- 1 Depuis la proclamation de l'état d'urgence sanitaire¹ le 24 mars 2020, les mesures du gouvernement français visant à lutter contre l'épidémie de Covid-19 font l'objet d'un nombre croissant de critiques : juristes, avocats, associations et élus dénoncent des initiatives attentatoires aux droits et libertés des citoyens, au-delà du simple objectif de ralentissement de la propagation du virus. L'inquiétude de la société civile se fait particulièrement ressentir depuis que le ministre de la Santé Olivier Véran et le secrétaire d'État au numérique Cédric O ont annoncé dans un entretien au Monde le 8 avril qu'ils réfléchissaient au développement d'une application pour smartphone, destinée à « limiter la diffusion du virus en identifiant des chaînes de transmission »². Ils ont par ailleurs précisé que ce projet, dénommé « Stop Covid », serait le premier élément « d'une stratégie globale de déconfinement et un outil numérique parmi d'autres dans la lutte contre l'épidémie »³. Face à la surenchère législative du gouvernement, il apparaît nécessaire de s'interroger sur la compatibilité des mesures tendant à ralentir la progression du Covid-19 avec le respect des droits et libertés fondamentales.
- 2 Le projet s'inscrit dans la lignée de mesures semblables adoptées dans d'autres États. Le traitement des données personnelles revêtirait trois finalités différentes⁴ : cartographier la propagation du virus pour prévoir les zones à risque et les besoins médicaux, faire respecter les mesures prises par les gouvernements, et retrouver les personnes potentiellement exposées dans un objectif de prévention. À ce jour, de nombreux pays ont déjà mis en place de telles procédures, portant des atteintes plus ou

moins importantes aux droits et libertés de leurs citoyens. En Chine par exemple, l'installation d'applications sur les téléphones mobiles est obligatoire et récupère les données des utilisateurs sans leur consentement préalable⁵. À l'inverse, à Singapour, l'application « TraceTogether » mise en place par les autorités est téléchargée volontairement par les citoyens et garantit une anonymisation de ses utilisateurs⁶.

- 3 La volonté affichée du gouvernement français d'avoir recours aux nouvelles technologies pour endiguer l'épidémie de Covid-19 soulève donc de nombreuses questions, notamment concernant le respect du droit à la vie privée des citoyens. Néanmoins, contrairement aux États précédemment évoqués, l'action du gouvernement français en la matière est encadrée par deux textes européens juridiquement contraignants : le règlement général sur la protection des données (RGPD) du 27 avril 2016⁷, transposé par la loi du 20 juin 2018 relative à la protection des données personnelles⁸, et la directive dite « ePrivacy » du 12 juillet 2002⁹. Le cadre posé par ces instruments ouvre la voie à plusieurs possibilités d'utilisation des données personnelles par le gouvernement dans le cadre de la lutte contre l'épidémie de Covid-19 et notamment dans une stratégie de déconfinement (I). De telles mesures auront néanmoins des conséquences néfastes sur les droits et libertés des citoyens – particulièrement concernant le respect de la vie privée – dont il faudra apprécier la nécessité et la proportionnalité (II).

I/- L'utilisation des données personnelles, une technique encadrée par le droit européen

- 4 À l'occasion de son audition par la Commission des lois de l'Assemblée nationale le 8 avril dernier, la présidente de la Commission Nationale de l'Informatique et des Libertés (CNIL) Marie-Laure Denis déclarait : « Il n'y a pas à se demander s'il faut s'affranchir du cadre, ou prendre des libertés avec celui-ci, parce que le cadre juridique que l'Europe et la France se sont donné comporte en lui-même, en son propre sein, les solutions permettant de répondre à la situation »¹⁰. Un traitement des données personnelles des Français par le gouvernement serait donc envisageable à droit constant dans un but de protection de la santé publique. Il importe cependant de distinguer les différentes solutions dont pourrait se prévaloir le gouvernement pour atteindre ses objectifs tout en respectant les règles de droit applicables en la matière. Deux modes de collecte des données personnelles sont envisageables, chacune faisant l'objet d'un régime différencié.
- 5 La première forme d'utilisation des données personnelles consiste en un traitement collectif des informations relatives à la localisation des individus, pour cartographier et surveiller les flux globaux de population. Cette technique est la moins attentatoire aux droits et libertés, car elle permet d'avoir recours à des données anonymisées et agréées, qui ne donnent en principe pas la possibilité aux autorités d'identifier des informations individuelles et privées. Ces données, anonymisées et suffisamment agréées, ne sont pas soumises au respect des principes du RGPD¹¹. Elles doivent cependant respecter les règles de la directive ePrivacy¹². Le gouvernement français a en réalité déjà eu recours à cette technique il y a quelques semaines avec l'aide de la société Orange, qui lui a fourni les données de toutes les personnes connectées sur son réseau mobile. Cela avait permis de savoir que 1,2 million de Parisiens avaient quitté la capitale la veille du confinement¹³.

- 6 La deuxième manière pour le gouvernement d'utiliser les données personnelles des Français dans un objectif de lutte contre la pandémie serait de réaliser un suivi individualisé des personnes exposées au virus. Ces derniers jours, le gouvernement a semblé se prononcer en faveur d'une telle technique, annonçant notamment que des réflexions étaient en cours sur le lancement de l'application « Stop Covid »¹⁴. Le régime du traitement individuel des données personnelles est régi par le RGPD qui définit des principes et limites pour leur utilisation. Les informations relatives à la santé des personnes sont qualifiées de « données sensibles » par l'article 9 du RGPD qui proscribit par principe leur utilisation. L'article 9 § 2 liste néanmoins une série d'exceptions permettant l'utilisation de ces données dans certains cas. Deux de ces exceptions pourraient fonder juridiquement la mise en place d'une application de suivi individualisé. D'une part, le consentement explicite donné par la personne faisant l'objet du traitement de ses données personnelles peut permettre au gouvernement d'y avoir recours¹⁵. Concrètement, il s'agirait d'une application mobile téléchargée volontairement par les citoyens, qui consentiraient à l'utilisation de leurs données personnelles dans un objectif de lutte contre le Covid-19. D'autre part, la présence de « motifs d'intérêt public importants » constitue également une exception à l'impossibilité de traiter des données sensibles. S'il ne fait aucun doute que ces motifs d'intérêt public sont en l'espèce avérés, un tel traitement des données de santé sans consentement des individus devrait faire l'objet d'une loi particulière pour justifier que le traitement est « proportionné à l'objectif poursuivi ».
- 7 Dans ces deux dernières hypothèses relatives au traitement individualisé des données personnelles, les autorités devront respecter les principes généraux du RGPD. Le Règlement impose notamment la transparence des procédures, une limitation du traitement des données en fonction de finalités déterminées, explicites et légitimes, une limitation de la durée de conservation, ou encore la minimisation des données collectées¹⁶.
- 8 Les récentes prises de position de membres du gouvernement ont mis en avant une forte probabilité que soit mis en place, sur le modèle de Singapour, un suivi individualisé des personnes exposées au virus fondé sur le volontariat. Afin de réduire les atteintes potentielles à la vie privée, le gouvernement envisage le recours à la technologie « Bluetooth » qui permet une réduction des données collectées. Cette éventualité, parfois dénommée « contact tracing », « tracking » ou « backtracking », soulève cependant un certain nombre de problématiques en termes de respect des droits et libertés.

II/- Le recours au « contact tracing », une solution inquiétante

- 9 De nombreuses voix se sont exprimées contre l'utilisation du « contact tracing ». Cette technique consisterait à créer une application mobile qui repèrerait par « Bluetooth » toute personne également détentrice de l'application et située dans un certain périmètre. En cas de contamination d'un individu par le virus, toutes les personnes l'ayant croisée seraient ainsi prévenues du risque pour leur santé, et pourraient faire l'objet de mesures spécifiques¹⁷. Cette option est pour le moment considérée par le gouvernement comme étant la moins attentatoire au respect de la vie privée, et donc la plus souhaitable. Des sociétés multinationales envisagent également d'avoir recours à

ces outils : le 10 avril, les entreprises Apple et Google ont annoncé un partenariat visant à mettre en œuvre des technologies de « contact tracing » à destination des utilisateurs de leurs smartphones, reposant sur le volontariat¹⁸. Le suivi individualisé par traitement de données personnelles, même s'il repose sur le consentement préalable, pose cependant un certain nombre de questions relatives à la protection des droits et libertés.

- 10 De nombreux acteurs de la société civile et élus considèrent en ce sens que la condition du consentement préalable des individus à l'utilisation de leurs données personnelles ne suffirait pas à rendre acceptables de telles mesures. Sacha Houlié, député LREM, a ainsi dénoncé une forme de « servitude volontaire »¹⁹. Surtout, l'Observatoire des libertés et du numérique a souligné que « la notion de consentement libre, au cœur des règles de la protection des données, est incompatible avec la pression patronale ou sociale qui pourrait exister avec une telle application »²⁰. Comment le consentement des individus pourrait-il en effet être libre et éclairé, dans un climat social de culpabilisation et devoir de « responsabilité collective » pour lutter contre l'épidémie de Covid-19 ?
- 11 Un grand nombre d'acteurs de la société civile s'inquiètent également de voir l'utilisation de ces outils de surveillance se banaliser dans le cadre de la lutte contre l'épidémie de Covid-19, et être reconduite à la fin de l'état d'urgence sanitaire. On le sait, les mesures présentées comme « exceptionnelles » en temps de crise sont souvent légitimées et généralisées par la suite. L'exemple des mesures prises dans le cadre de l'état d'urgence entre 2015 et 2017 en fournit une illustration²¹.
- 12 À ces réticences, s'ajoutent d'autres interrogations, notamment concernant le caractère « nécessaire et proportionné » des mesures envisagées vis-à-vis des atteintes à la vie privée qu'elles impliqueraient, mais également concernant la sécurisation des données ou le recours à des acteurs privés pour mettre en place les outils. Or, l'efficacité de l'utilisation des données personnelles dans un objectif de lutte contre la pandémie n'étant pas clairement établie²², est-il bien raisonnable d'y avoir recours au prix d'une très forte restriction des libertés et droits fondamentaux des individus ? Dans une déclaration conjointe de plusieurs dizaines d'organisations de la société civile publiée sur le site web d'Amnesty International²³, un certain nombre de recommandations ont été formulées à l'attention des gouvernements en cas de recours aux technologies de surveillance numérique. Ces ONG demandent notamment aux autorités nationales de n'utiliser les données personnelles de leurs citoyens que pour répondre à des objectifs légitimes de santé publique, de façon limitée dans le temps, en garantissant un niveau de sécurité suffisant pour toutes les données collectées, sous le contrôle d'organismes indépendants.
- 13 Le lanceur d'alerte Edward Snowden, ancien employé de la Central Intelligence Agency (CIA) et de la National Security Agency (NSA) aux États-Unis, est en ce sens revenu dans une interview pour Vice²⁴ sur l'utilisation des données personnelles par les États dans le cadre de la lutte contre l'épidémie de Covid-19. Selon lui, « ce qui est construit en ce moment, c'est l'architecture de l'oppression »²⁵. Comment pourrions-nous en effet nous assurer que les données recueillies à cette occasion ne seront pas utilisées à d'autres fins que celles publiquement annoncées par le gouvernement, ou qu'elles ne seront pas conservées à l'issue de l'état d'urgence sanitaire ?

*

Les Lettres « Actualités Droits-Libertés » (ADL) du CREDOF (pour s'y abonner) sont accessibles sur le site de la Revue des Droits de l'Homme (RevDH) – Contact

NOTES

1. Loi 2020-290 du 23 mars 2020 d'urgence pour faire face à l'épidémie de covid-19
2. Martin Untersinger, Chloé Hecketsweiler, François Béguin et Olivier Faye, « L'application StopCovid retracera l'historique des relations sociales : les pistes du gouvernement pour le traçage numérique des malades », *Le Monde*, 8 avril 2020.
3. *Ibid.*
4. Audition commission des lois Assemblée nationale, Propos liminaires de Madame Marie-Laure Denis, Présidente de la CNIL, 8 avril 2020.
5. Paul Mozur, Raymond Zhong et Aaron Krolik, « In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags » *New York Times*.
6. Vincent Gibert, « Comment Singapour a aplati ses courbes du coronavirus : ils racontent », *Le Huffpost*, 2 avril 2020.
7. Règlement (UE) 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. Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.
9. Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), dite directive ePrivacy.
10. *Ibid.*
11. Article 11 du RGPD.
12. Article 9 de la directive ePrivacy.
13. Martin Untersinger, « Confinement : plus d'un million de Franciliens ont quitté la région parisienne en une semaine », *Le Monde*, 26 mars 2020.
14. Martin Untersinger, Chloé Hecketsweiler, François Béguin et Olivier Faye, « L'application StopCovid retracera l'historique des relations sociales : les pistes du gouvernement pour le traçage numérique des malades », *Le Monde*, 8 avril 2020.
15. Article 9 §2 (a) du RGPD.
16. Article 5 du RGPD.
17. Comme ce fut le cas dans d'autres États ayant mis en œuvre des technologies de « contact tracing » pour lutter contre l'épidémie de Covid-19, un tel suivi pourrait avoir des conséquences attentatoires aux droits et libertés : injonction de se faire dépister, obligation de rester confiné et d'apporter la preuve du respect de cette obligation aux autorités, interdiction de travailler ou d'être scolarisé, etc.
18. Apple, « Apple and Google partner on COVID-19 contact tracing technology », 10 avril 2020. Les sociétés Apple et Google travaillent au développement d'une option directement intégrée aux systèmes d'exploitation iOS et Android, utilisant la technologie Bluetooth pour cartographier les interactions sociales et ainsi prévenir les individus potentiellement exposés au virus.

19. Sacha Houlié, « Tracking, géolocalisation, pourquoi je suis contre », Le Journal du Dimanche, 7 avril 2020
 20. « La crise sanitaire ne justifie pas d'imposer les technologies de surveillance », Communiqué de l'Observatoire des libertés et du numérique (OLN), Paris, le 8 avril 2020.
 21. Jean-Louis Halpérin, Stéphanie Hennette Vauchez, Éric Millard (dir.), L'état d'urgence : de l'exception à la banalisation, Presses universitaires de Nanterre, 2017 ; S. Hennette-Vauchez (dir.), *Ce qui reste(ra) toujours de l'urgence*, Paris, Institut Universitaire Varenne, Coll. Colloques et Essais, Paris, 2018.
 22. Daniel Hoffman, « Tracking sur smartphone : Apple et Google s'allient pour le suivi des données », La Tribune, 11 avril 2020. Ryan Calo, chercheur à l'université de Washington et affilié au Centre pour internet et la société de Stanford, s'est interrogé sur l'efficacité de ces techniques : « S'ils pensent que le suivi numérique des contacts va permettre aux gens d'arrêter la distanciation sociale, je suis sceptique ».
 23. « Déclaration conjointe de la société civile. Le recours aux technologies de surveillance numérique pour combattre la pandémie doit se faire dans le respect des droits humains », Amnesty International, 2 avril 2020
 24. YouTube, Vice, « Shelter in Place with Shane Smith & Edward Snowden », 10 avril 2020.
 25. *Ibid.*
-

ABSTRACTS

Les circonstances exceptionnelles de la lutte contre l'épidémie de Covid-19 sont utilisées par le gouvernement pour justifier l'expérimentation de nouvelles technologies de surveillance. La présente lettre identifie comment le droit positif encadre les différentes possibilités de recours aux données personnelles dans un objectif sanitaire, et dans quelle mesure ces dernières pourraient avoir pour conséquence de graves atteintes aux droits et libertés.

AUTHOR

AURÈLE PAWLITSKY

Etudiant du M2 Droits de l'Homme