Cette série de contributions s'efforce de mettre en partage les réflexions, observations, témoignages et questionnements que suscitent, chez chacun d'entre nous, les développements de l'épidémie et les multiples conséquences qu'elle aura aussi bien à court qu'à long terme.

FAUT-IL RECOURIR AU NUMÉRIQUE POUR FACILITER LA SORTIE DU CONFINEMENT ?

6 avril 2020 | Par **Mélanie Heard**, enseignante-chercheuse au Centre de Recherches Interdisciplinaires, CRI et co-coordonnatrice du pôle santé de Terra Nova

Le 16 mars, le Comité européen de la protection des données a publié une déclaration sur l'importance de protéger les données personnelles lors de leur utilisation dans la lutte contre le COVID-19[1]. Le texte rappelle les articles spécifiques du règlement général sur la protection des données (RGPD) qui fournissent les fondements juridiques du traitement des données personnelles dans le contexte des épidémies. Par exemple, l'article 9 autorise le traitement de données à caractère personnel « pour des raisons d'intérêt public dans le domaine de la santé publique, telles que la protection contre les menaces transfrontières graves pour la santé », à condition que ce traitement soit proportionné à l'objectif poursuivi, respecte l'essence du droit à la protection des données et protège les droits et libertés de la personne concernée.

De nombreuses positions ont été exprimées tout récemment pour appeler à un tel usage proportionné et raisonnable, des colonnes de *Nature*[2] à l'éditorial du *Monde*[3], en passant par le *Défenseur des droits*[4].

 $^{[1] \ \} EDPD, \ 16 \ mars \ 2020, \ \underline{https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak \ en}$

^[2] Ienca, M., Vayena, E., « On the Responsible Use of Digital Data to Tackle the COVID-19 Pandemic ». Nat Med (2020). https://doi.org/10.1038/s41591-020-0832-5

^{[3] «} Face au Covid-19, le choix entre santé ou libertés est un faux dilemme », *Le Monde*, 30 mars 2020, https://www.lemonde.fr/idees/article/2020/03/30/face-au-covid-19-le-choix-entre-sante-ou-libertes-est-un-faux-dilemme 6034887 3232.html

^[4] Dans L'Obs, 30 mars 2020; https://www.nouvelobs.com/coronavirus-de-wuhan/20200330.OBS26807/jacques-toubongeolocalisation-je-dis-attention.html

En miroir de ces positions d'alerte face aux risques liberticides de l'usage du numérique, les réseaux de la civic-tech, eux, s'animent d'initiatives multiples pour appréhender le sujet sous un tout autre angle : cette mobilisation, plus proche de l'esprit « sciences citoyennes »[5], investit la vertu d'« empowerment » individuel du numérique : rendre chacun capable de protéger les autres. Il y a donc là un antagonisme des cadres de problématisation qui pose question.

Le 1er avril, le Premier ministre lors de son audition devant la mission d'information de l'Assemblée nationale a confirmé que le traçage des données numériques « pourrait peut-être » figurer comme une « question encore ouverte » à l'agenda stratégique du Gouvernement. Il a utilisé le terme de « tracking » qu'il a désigné comme un outil pour « suivre les déplacements des malades » utilisé « dans certains pays » à l'appui de « l'isolement très strict des malades » et de leurs contacts, statuant que de tels dispositifs n'étaient pas « légalement permis » dans notre pays (1/04, 43'30). Les termes du débat qu'il a esquissé semblent tenir à une distinction sur le caractère obligatoire ou non de tels dispositifs ; il a laissé ouverte, quoiqu'avec une certaine réticence, la piste de dispositifs volontaires. Il a donc nettement privilégié comme point d'entrée dans ce débat l'enjeu des dérives et atteintes pour les libertés. Si cette entrée paraît naturelle s'agissant d'un secteur où la conquête des droits est une ligne de force puissante, les termes de ce débat dans le cas d'espèce méritent d'être clarifiés et plusieurs critères de jugement peuvent nous y aider.

Le premier de ces critères est, comme l'a défini le Premier ministre, le caractère volontaire ou non de l'utilisation des données privées. Sur ce point, on voit bien qu'une application qui serait téléchargée par l'usager dans une démarche optin ne franchit pas la ligne de l'utilisation des données sans consentement de leur propriétaire. La plupart des applications de « tracking » qui sont utilisées aujourd'hui face au COVID, celle de Singapour faisant office de modèle du genre[6], sont de cette nature opt-in. La teneur générale du débat aujourd'hui, autour du caractère nécessairement liberticide de ces dispositifs, ne se justifie donc pas immédiatement.

^{[5] «}Two Million Guinea Pigs and Counting: The Remarkable Rise of Self-Monitoring in The Time of Coronavirus», *Forbes*, 27/03/2020, voir notamment l'appli « http://safepaths.mit.edu/du MIT Media Lab; ou encore l'intiative CoEpi (https://www.coepi.org/)

^[6] https://www.tracetogether.gov.sg/

D'autres critères de jugement doivent entrer en ligne de compte : le degré auquel ces données sont identifiantes en tout premier lieu bien sûr, mais aussi le fait que les données résident dans le téléphone de l'usager ou non, paramètre qui engage des alternatives décisives quant aux garanties nécessaires pour prévenir les dérives, sécuriser l'accès de tiers aux données, border le caractère temporaire de leur disponibilité, et prévoir leur destruction. Là encore, le modèle singapourien offre aux usagers des garanties conséquentes puisqu'il n'y a pas, grâce à l'usage du bluetooth et en l'absence de géolocalisation par GPS, de centralisation des données recueillies entre appareils[7].

Un autre critère de classification des enjeux peut résider dans la finalité du recueil de ces données, avec deux grandes finalités possibles, distinctes mais non nécessairement exclusives l'une de l'autre.

La première finalité est scientifique, engageant l'intérêt collectif à disposer de données populationnelles utiles à la gestion de l'épidémie. Cette finalité peut requérir des données agrégées, pour connaître par exemple en temps réel les concentrations de populations et donc les besoins potentiels en termes d'offre de soins ; dans ce cas, il n'y a pas besoin de données corrélées au statut des utilisateurs par rapport au Covid. Mais la même finalité de surveillance épidémiologique[8] au niveau collectif peut utiliser des données numériques associées cette fois au statut Covid, pour suivre les dynamiques de propagation de l'épidémie dans l'ensemble de la population et ainsi identifier, localiser et quantifier, dans la perspective du déconfinement, un phénomène de rebond.

L'autre finalité de l'usage de données numériques est centrée sur l'échelle plus réduite des individus et des chaînes de transmission interindividuelles. L'objectif est alors de fournir aux individus une information sur leur niveau d'exposition personnelle au risque pour les amener à adapter leurs comportements. Les comportements préventifs qu'il s'agit de favoriser, dans un but à la fois individuel et collectif, sont décisifs : l'isolement des malades dès les premiers symptômes, et surtout la quarantaine de leurs contacts dès qu'est suspectée une rencontre prolongée à moins d'un mètre dans les 14 jours précédents.

^[7] Voir Mathis Cohen et Simon Matet, « Quelle réponse numérique à la crise du Covid-19? », Terra Nova, 4 avril 2020.

^[8] En santé publique, la surveillance épidémiologique concerne la description des phénomènes au niveau collectif ; elle désigne la collecte systématique et continue de données sur un phénomène de santé, leur analyse, interprétation et diffusion dans une perspective d'aide à la décision ; Langmuir, A. D. « The Surveillance of Communicable Diseases of National Importance », New England journal of medicine, 268 : 182- 192 (1963).

Ces mesures – isolement des malades, quarantaine de leurs contacts - sont les piliers de toute intervention de santé publique en situation d'épidémie. Elles sont adossées à des méthodes de « traçage des contacts »[9] : l'autorité sanitaire conduit un interrogatoire circonstancié des cas sur leurs interactions des derniers jours, notifie par téléphone tous les contacts ainsi repérés, et suit ces contacts durant leur mise en quarantaine (monitoring des symptômes). Le dispositif est banal, couramment mis en œuvre pour les maladies à déclaration obligatoire, de la rougeole aux infections à méningocoque en passant par les toxi-infections alimentaires collectives ou le saturnisme [10].

Mais le point spécifique ici est naturellement le grand nombre de cas et d'enquêtes de traçage à conduire. L'état des équipes dédiées à cette tâche dans les ARS début mars ne laisse guère de doutes sur le caractère impraticable d'une telle tâche avec des méthodes traditionnelles. Or on sait que la réactivité du dispositif est justement une condition absolue de son efficacité; la rapidité avec laquelle on peut, dès les premiers symptômes d'un individu, alerter toutes ses relations des derniers jours, est LA variable qui détermine l'efficacité du dispositif, comme le démontre une modélisation de l'Oxford Big Data Institute récemment publiée dans *Science*[11]. Selon les auteurs, le recours à l'outil numérique trouve par conséquent ici sa justification la plus élémentaire : permettre une efficacité en temps réel radicalement inaccessible sans lui.

Précisons que, dans cet ordre de finalité, le point crucial réside dans les décisions qui sont prises quant aux moyens d'obtenir des individus l'adoption des comportements requis. L'alternative est claire : soit l'isolement des cas et la mise en quarantaine des contacts est volontaire, soit elle est obligatoire. C'est un débat extrêmement classique du droit de la santé publique, largement commenté dans le sillage de l'épidémie de SRAS de 2003[12].

^[9] https://www.who.int/features/qa/contact-tracing/en/

^[10] voir le site de Santé publique France : https://www.santepubliquefrance.fr/maladies-a-declaration-obligatoire/definition-objectifs-criteres-acteurs-de-la-declaration-obligatoire. Pour la rougeole, on pourra détailler ici : https://solidarites-sante.gouv.fr/fichiers/bo/2018/18-11/ste 20180011 0000 0053.pdf

Il est intéressant de noter que la systématisation de procédures similaires de notification des partenaires est désormais l'objectif dans le cas du VIH et des infections sexuellement transmissibles, avec une action dédiée dans la Stratégie nationale de santé sexuellle de mars 2017 (action n°28), soutenue par les recommandations du Conseil national du sida datant de février 2018 qui soulignent l'efficacité des pratiques de ce type dans d'autres pays : https://cns.sante.fr/actualites/notification-formalisee-aux-partenaires-nouvel-avis-cns/

^[11] Ferretti, Luca, et al. « Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing ». Science, mars 2020. science.sciencemag.org, doi:10.1126/science.abb6936.

^[12] Lawrence O. Gostin et al., « Quarantine: Voluntary or Not? »:, *The Journal of Law, Medicine & Ethics*, 24 juin 2016, https://journals.sagepub.com/doi/10.1111/j.1748-720X.2004.tb00196.x.; Institute for bioethics et Mark Rothstein, « Quarantine and Isolation. Lessons from SARS », s. d.

Aujourd'hui en France, l'adoption de ces comportements est recommandée aux individus, mais la loi du 23 mars 2020 a clairement identifié, en se référant explicitement à l'article 1 du règlement sanitaire international (RSI), la possibilité que ces comportements individuels fassent l'objet de mesures obligatoires [13].

C'est le caractère obligatoire ou non de ces mesures qui porte la charge de l'atteinte aux libertés dans ce dispositif. Le recours, pour soutenir les comportements requis, au traitement de données numériques est une composante secondaire du dispositif. Si les mesures sont obligatoires, le traitement des données peut au surplus être lui-même obligatoire et intervenir comme moyen de contrôle coercitif pour sanctionner d'éventuels manquements. Mais il n'y aurait pas de sens à faire peser sur cet aspect subsidiaire du dispositif la charge du débat sur son caractère plus ou moins attentatoire aux libertés. C'est sur le caractère coercitif de l'isolement et de la quarantaine que reposent les choix difficiles à faire pour proportionner l'atteinte aux libertés avec l'efficacité de santé publique recherchée. Le traitement des données personnelles vient en second rang dans l'ordre de la décision. Cela ne veut pas dire qu'il soit de moindre importance pour les droits ; simplement le raisonnement doit le traiter comme une déclinaison, non comme une mesure en soi.

Il paraît clair aujourd'hui que la question du régime d'isolement des cas et de quarantaine de leurs contacts est une variable qui s'imposera comme cruciale dans les scénarios de sortie du confinement. La modélisation parue le 31 mars dans *Science* confirme, s'il en était besoin, que ces mesures qui seules permettent de casser les chaînes de transmission, sont cruciales. En ciblant les situations d'exposition cas/contacts, elles sont une alternative désirable à la lourdeur catastrophique du confinement universel. Elles n'ont de sens qu'adossées à un système de traçage des contacts extrêmement réactif, permettant aux individus d'adapter leurs comportements en temps réel à l'information sur leur niveau de risque.

La question des moyens pertinents pour que des individus adoptent les comportements de prévention requis est naturellement un poncif de l'action de santé publique.

^[13] Loi n° 2020-290 du 23 mars 2020 d'urgence pour faire face à l'épidémie de covid-19, Article 2 : « Art. L. 3131-15.-Dans les circonscriptions territoriales où l'état d'urgence sanitaire est déclaré, le Premier ministre peut, par décret réglementaire pris sur le rapport du ministre chargé de la santé, aux seules fins de garantir la santé publique : (...) « 2° Interdire aux personnes de sortir de leur domicile, sous réserve des déplacements strictement indispensables aux besoins familiaux ou de santé ;

^{« 3°} Ordonner des mesures ayant pour objet la mise en quarantaine, au sens de l'article 1er du règlement sanitaire international de 2005, des personnes susceptibles d'être affectées »

On voit bien que la compliance des individus à l'égard de ces mesures devient LA variable clé, en l'espèce, pour contrôler la diffusion de l'épidémie. Si tel est l'horizon des choix qui s'annoncent, on verra donc se réouvrir le débat sur la question de savoir s'il faut se fier à des recommandations, à l'empowerment et au counseling pour convaincre les individus de s'isoler, ou bien si c'est au contraire l'obligation assortie d'un contrôle et d'une menace de sanctions qui permet d'être efficace. Gageons qu'on verra resurgir les arguments sur la contre-productivité de l'obligation, si largement théorisés face au VIH, avec l'hypothèse qu'une menace de coercition détourne les individus du dépistage. Il faudra également statuer sur les conditions de cet isolement, inéquitables selon les revenus, et sur les moyens de protéger les autres membres du foyer avec des décisions difficiles sur l'opportunité de créer des lieux intermédiaires dédiés à l'isolement des cas peu symptomatiques[14]. Dans tous les cas, le recours au numérique devra être envisagé ici pour ce qu'il est désormais de façon reconnue en santé publique : un levier précieux du changement des comportements individuels[15].

Dans ce cadre, la question du recours au numérique ne pourra donc être que subordonnée à l'analyse des conditions d'efficacité des mesures qu'il viendra soutenir. Elle ne peut se poser qu'après plusieurs étapes de raisonnement préalable, à savoir :

- quelle est l'efficacité attendue de la triade : isolement des cas / traçage de leurs contacts / mise en quarantaine de ces contacts ?
- quelles hypothèses de compliance retient-on pour établir cette efficacité, en distinguant la compliance permise par le volontariat versus par l'obligation, et en nuançant selon que l'on offre des lieux d'isolement intermédiaires ou qu'on privilégie le domicile?
- quelle réactivité peut-on attendre du système de traçage des contacts, selon qu'il est manuel ou bien adossé au traitement de données numériques ?
- quel impact le traitement des données numériques est-il susceptible d'avoir sur la capacité des individus à adopter les comportements requis ?

Ce n'est que si la question de l'efficacité des mesures envisagées est clairement renseignée à ces différentes étapes que pourra se poser la question de la proportionnalité, en regard de cette efficacité, de l'atteinte aux libertés qu'un traitement des données numériques pourrait représenter.

^[14] Franck Nouchi, « Coronavirus : l'urgence absolue de créer des structures de prise en charge des patients peu symptomatiques », *Le Monde*, 27 mars 2020

^[15] Voir par exemple Commission Européenne, *Livre vert sur la santé mobile*, Bruxelles (2014); Haute autorité de santé, Rapport de prospective 2019, https://www.has-sante.fr/upload/docs/application/pdf/2019-07/rapport_analyse_prospective_20191.pdf

Et l'on voit bien que l'adhésion volontaire, comme envisagée actuellement, à une application qui collecte les interactions bluetooth entre téléphones, tout en permettant un gain d'efficacité patent pour le traçage des contacts, n'est certainement pas la partie du dispositif qui concentre le plus d'enjeux dans l'atteinte aux libertés.

Ce qui concentre en revanche des enjeux majeurs pour l'efficacité du dispositif, c'est l'ampleur de cette adhésion volontaire (opt-in) pour utiliser l'application. Plus encore que les éventuelles fonctionnalités qui pourraient être associées (informations médicales, aide au diagnostic ou au suivi, voire offre de services, soutiens ou solidarités locales), c'est probablement la clarté du processus décisionnel qui en sera une variable essentielle ; seuls des citoyens conscients des gains d'efficacité qu'elle permet seront susceptibles de télécharger volontairement une telle application dans leur smartphone. Il est permis de penser que la position du gouvernement, y compris devant la mission d'information de l'Assemblée nationale, abordant cet enjeu du numérique sous l'angle des usages liberticides qui en sont faits dans certains pays, soit, pour le coup, contre-productive.

Il est possible, à l'inverse, de proposer un processus décisionnel raisonnable qui statue successivement sur l'utilité du traitement numérique des données en appui des mesures de santé publique nécessaires, puis sur son utilité pour pallier les insuffisances d'un traitement manuel des données.

De ce point de départ découlent assez naturellement les réquisits qui doivent peser sur un usage raisonnable de ces données : adhésion en *opt-in* à une application, données résidentes dans le téléphone, sécurisation du protocole choisi par un tiers de confiance garant de son caractère temporaire (avec destruction des données), de sa disponibilité en open-source, en lien avec les organismes de recherche, et assorti d'un contrôle démocratique.

Ce contrôle démocratique peut prendre plusieurs formes, et ce sont ces choix précis qu'il faut débattre ; un contrôle *ex post* n'est pas suffisant, il faut des procédures d'examen *ex ante*. L'implication du Parlement paraît consensuelle, mais un tiers de confiance *ad hoc* paraît souhaitable également.

Si le dispositif global de santé publique inclut des mesures coercitives suspendant l'exercice de certaines libertés, alors un bon modèle de contrôle démocratique peut être recherché du côté de la Commission nationale de contrôle des techniques de renseignement, dont la mission est bien le contrôle de proportionnalité a priori, en situation dérogatoire au droit commun[16]. La nature de l'expertise à mobiliser mérite examen, et doit probablement combiner l'expertise technique à une expertise juridique capable d'évaluer la proportionnalité des moyens et des fins. Enfin, l'inclusion de la société civile dans ce dispositif de contrôle démocratique serait une réelle avancée : elle aurait une double vertu à la fois éthique – de légitimation démocratique des décisions prises, et une probable vertu épistémique – en améliorant la pertinence des dispositions par une meilleure prise en compte des caractéristiques pratiques de leur mise en œuvre sur le terrain.

Les bonnes pratiques en la matière sont bien balisées, y compris pour l'inclusion des « parties prenantes ». Le secteur de l'humanitaire, qui a désormais largement recours au traitement de données individuelles pour guider les interventions d'aide, notamment en situation de catastrophes naturelles, a parfaitement thématisé les « usages raisonnables » de ces données et défini les garde-fous nécessaires à chaque type d'usages. Ces travaux, notamment au Secrétariat général des Nations-unies (Bureau de la coordination des affaires humanitaires, UN-OCHA)[17], ont le mérite de rappeler que le critère de légitimité de l'usage du numérique est d'une simplicité radicale : en situation d'urgence, la production d'informations en temps réel est utile à la fois aux individus, pour qui l'adaptation au risque est vitale, et aux autorités, qui sont d'autant plus efficaces qu'elles ciblent les besoins.

^[16] https://www.cnctr.fr/2_presentation.html

 $[\]hbox{[17]} \, \underline{\text{https://centre.humdata.org/data-policy/:}} \, \text{voir notamment les guidelines détaillées de mars}$

^{2019 : &}lt;a href="https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf">https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf Voir aussi le concept de « data ethics » détaillé dans la note : https://centre.humdata.org/wp-content/uploads/2020/02/guidance_note_ethics.pdf