Position paper

l21 Avril 2020

Adressé à M. Thierry Breton, Commissaire européen pour le marché intérieur, en charge du numérique, de l'industrie et des services, la défense, l'espace, l'audiovisuel et du tourisme

LA PROTECTION DES DONNÉES ET LA CRISE SANITAIRE

CONTEXTE

1. Dans le contexte de crise sanitaire liée au Coronavirus, les Institutions européennes s'interrogent sur les mesures à mettre en œuvre afin de limiter la propagation des virus et sur les conditions dans lesquelles les données personnelles, notamment en matière de santé, peuvent être utilisées.

2. Dans des situations de pandémie, la possibilité de collecter, en dehors de toute prise en charge médicale, des données concernant des personnes afin de déterminer si elles présentent des symptômes de virus, ou des données relatives à des déplacements et évènements, ne saurait être envisagée sans que soit garantie la pleine application des droits et libertés fondamentaux qui garantissent le droit au respect de la vie privée des citoyens.

ÉTAT DES LIEUX

3. Plusieurs réflexions sont déjà menées autour de l'utilisation des données personnelles et de localisation lorsqu'il ne s'agit pas de décisions déjà entérinées et dans certains cas drastiques.

4. Ainsi, en Israël, depuis le 16 mars, le service de renseignement intérieur, le Shin Bet, d'ordinaire focalisé sur les « activités anti-terroristes », peut désormais, sans autorisation préalable de la justice, traquer les données de localisation des téléphones portables des citoyens. En pratique, le Shin Bet peut obtenir la localisation des personnes infectées sur une période de 14 jours ayant précédé leur diagnostic et « *identifier les trajets et les personnes avec qui elles sont entrées en contact* ».

L'objectif consiste à prévenir par [illegible]nnes ayant été en contact avec des personnes malades et de leur der[illegible]acer en quarantaine. Le quotidien de gauche *Ha'Aretz* n'a pas hésité à dénoncer les « *mesures les plus draconiennes de l'histoire israélienne pour traquer à grande échelle les déplacements de citoyens respectueux des lois* ». Le cas d'Israël se rapproche de ceux de la Chine et de la Corée du Sud, deux pays dans lesquels les personnes en quarantaine sont suivies à la trace via une application sur leur téléphone portable.

Les États-Unis, quant à eux, s'apprêtent à lancer un plan de partage de données anonymisées avec les géants de la Tech (Google, Apple, Facebook…) dans le but de disposer d'un système de suivi des contacts à l'aide de données de localisation et de technologies de reconnaissance faciale.

5. En Europe, la situation est fort heureusement un peu différente. En Lombardie, région la plus touchée d'Italie par l'épidémie, les opérateurs téléphoniques ont fourni aux autorités les données concernant le passage d'un téléphone portable d'une borne téléphonique à une autre. Ces données sont anonymisées et permettent de savoir quel pourcentage de la population respecte strictement le confinement. D'après les informations récoltées par la Région, seulement 60 % de sa population resterait à la maison. En Belgique, après le feu vert du ministère de la Santé, les opérateurs fournissent à la plateforme Dalberg Data Insights des « cartes de mobilité » anonymisées et basées sur des agrégats géographiques, comme le code postal, qui, croisées avec les données épidémiologiques des autorités, pourront leur permettre de prédire la propagation vers tel ou tel endroit. En Allemagne, le gouvernement s'apprête à lancer une application mobile, inspirée de Singapour, pour faciliter le suivi individuel des cas et l'identification des chaînes de contamination au coronavirus, dans le cadre de la stratégie de sortie progressive du confinement. Ce suivi repose sur la technologie Bluetooth. La France a quant à elle demandé à un Comité de scientifique d'étudier la possibilité de mettre en place un traçage de la population.

6. En revanche, et on peut le regretter, le Comité Européen de la Protection des données (CEPD) vient tout juste de rappeler les règles applicables dans l'Union Européenne. Cependant, et dans le même temps, la Commission européenne réclame des données d'opérateurs téléphoniques pour évaluer l'effet des mesures de confinement…

Ce paradoxe est difficilement compréhensible, notamment pour des citoyens de plus en plus désorientés par les tergiversations des gouvernements de certains États

membres. Surtout, et sans surprise, le recours à la reconnaissance faciale, dont la technologie se développe rapidement dans le monde, est de plus en plus envisagé, alors même qu'elle peut conduire à de nombreux détournements. La reconnaissance faciale n'est pas infaillible et a toujours besoin, en cas de sanctions potentielles, de l'intervention d'un humain, et notamment d'un juge.

L'UNION EUROPÉENNE ET LE TRAITEMENT DES DONNÉES

7. Pour rappel, deux textes législatifs sont applicables dans la situation actuelle, même si le second est souvent oublié ou ignoré :

- le Règlement Général de Protection des Données (RGPD) prévoit des mécanismes de collecte et de traitements des données personnelles par les autorités de santé publique applicables dans le cas d'épidémies, sans qu'il soit nécessaire de recueillir le consentement de la personne concernée ;

- le traitement des données de localisation collectées par les opérateurs de communications électroniques est régi quant à lui par la directive e-privacy. La révision de cette directive est malheureusement actuellement en suspens.

8. EN CONSÉQUENCE, DANS L'UNION EUROPÉENNE, LE TRAITEMENT DES DONNÉES REPOSE NOTAMMENT SUR DES PRINCIPES DE NÉCESSITÉ, DE PROPORTIONNALITÉ, DE TRANSPARENCE ET DE CONFIDENTIALITÉ.

9. La demande formulée par la Commission auprès d'opérateurs téléphoniques de plusieurs pays afin « *qu'ils fournissent des données agrégées sur leurs abonnés mobiles pour mieux comprendre et anticiper l'évolution de la pandémie* » peut dès lors s'interpréter comme un réflexe de facilité face à une réalité qui frappe de plein fouet le monde entier.

Dans le même temps, la Commission explique bien par la voix de son Commissaire qu'elle souhaite « *donner aux chercheurs européens du Centre Commun de recherche, qui sera le destinataire des données, les moyens d'aider les autorités locales à dimensionner correctement l'offre de soins en vérifiant, grâce aux données mobiles, si les consignes de confinement sont appliquées* ».

Cette position nous paraît problématique alors même que la préservation des droits et libertés fondamentaux pourrait être assurée grâce à des outils moins intrusifs et tout aussi compatibles avec l'objectif d'efficacité de la lutte contre la pandémie.

POSITION DE L'*INSTITUTE FOR DIGITAL FUNDAMENTAL RIGHTS* (iDFrights)

10. L'iDFrights appelle à la vigilance en matière de protection de la vie privée et insiste sur le fait qu'une application mobile de suivi des déplacements pourrait faciliter la collecte d'informations personnelles et, par voie de conséquence, qu'elle doit être parfaitement encadrée. Dans cette optique, nous serions tous géolocalisés et identifiés d'autorité par nos États une fois les données collectées.

Mettre en œuvre des mesures adaptées à la situation telles que la limitation des déplacements et réunions, ne signifie pas prendre des mesures susceptibles de porter atteinte au respect de la vie privée des personnes concernées par la collecte de données de santé, si elles devaient aller au-delà même de la gestion de la crise liée au virus.

L'iDFrights considère que tous les moyens de géolocalisation ne se valent pas. Le suivi des flux de population via les données anonymisées d'un opérateur télécoms pose moins de questions que le pistage d'un citoyen, même consentant, pendant la période d'incubation d'une maladie via son smartphone personnel. Et il va sans dire que l'obligation pour une personne d'activer une telle application pour sortir du confinement serait totalement inacceptable et contraire aux textes européens du RGPD et de la directive *e-privacy*.

L'iDFrights souhaite la mise en place d'une vigilance continue et une évaluation périodique des dispositifs de protection. Il est essentiel de maintenir « l'humain » au centre de toute décision. Notamment, l'Institut insiste sur la préservation d'une intervention humaine à chaque étape du processus de l'analyse des données permettant un consentement éclairé du citoyen.

D'une façon générale, la gravité inédite de cette crise sanitaire peut légitimer l'utilisation, l'agrégation des données, voire la géolocalisation, le bornage, l'offuscation ou tout autre moyen similaire, sous la condition expresse de la vigilance exercée par une autorité de contrôle permanente, créée ou mandatée à cet usage. Dans ces cas, il est incontournable d'exiger la destruction des informations ainsi recueillies dès la fin de la crise sanitaire.

11. L'iDFrights, s'agissant de la souveraineté d'un continent dans son entier, insiste sur la nécessité de donner les moyens aux associations et entreprises européennes de privilégier leurs recherches et de promouvoir leurs actions, afin de créer, entre le modèle américain et le modèle asiatique, une troisième voie : la voie européenne déjà

engagée par une série de textes dont le RGPD de 2018. Leur expérience doit être valorisée car elles sont parfaitement à même de proposer des axes de réflexion pour allier sauvetage des vies humaines et acquis de l'Union. Puisque dans l'état actuel des traités, les politiques de santé relèvent exclusivement de la responsabilité des États membres, les entreprises européennes savent donc très bien intégrer, dans leurs projets, les éléments sociétaux qui sont la marque de fabrique des pays membres et travailler ensemble

12. L'iDFrights s'inquiète du fait que le RGDP ne s'applique qu'en Europe. En effet, les données générées et collectées l'étant sur des plateformes n'ayant pas de base en Europe, la gestion de leurs traitements échappera automatiquement aux autorités européennes. C'est la raison pour laquelle il est recommandé :

- de donner les moyens à des plateformes européennes d'émerger et de prospérer,
- de veiller à l'encadrement des technologies et d'Internet concernant l'usage des données massives,
- et d'ouvrir une nouvelle réflexion quant aux enjeux éthiques posés par « *le big data* »

13. L'iDFrights craint les erreurs potentielles de la reconnaissance faciale qui peuvent l'emporter sur les avantages en termes de sécurité. Il ressort en effet de plusieurs études que les logiciels de reconnaissance faciale peuvent présenter un préjugé racial ou ethnique. L'Institut n'est donc pas favorable à l'utilisation généralisée de cette technologie qui soulève des problèmes en matière de protection des droits et libertés fondamentaux. Et ceci est d'autant plus grave que, combinées à d'autres données, les données obtenues peuvent être utilisées pour tirer des conclusions sur l'identité des personnes concernées.

14. L'IDFrights soutiendra toutes les options européennes qui seront basées sur un système qui assurera un strict respect du RGPD et notamment l'initiative sur laquelle travaillent la Commission Européenne, la France et l'Allemagne qui coopèrent d'ailleurs, et semblent privilégier un système dit de « contact-tracent ». Cette technologie utiliserait les ondes de type Bluetooth. Leur émission, à partir du smartphone, permettrait d'identifier les contacts éventuels d'une personne infectée (qui se signalera comme telle volontairement par son accès à l'application grâce à un code qu'elle recevra) avec une personne non infectée, cette dernière recevant

l'information par alerte, ce qui lui permettra de se faire tester immédiatement, et ainsi de limiter la chaîne de propagation du virus.

La mise au point de cette application que les français appellent « stop Covid 19 » ne nécessite pas de s'identifier. Pas besoin non plus de centralisation des données, nous assure-t-on.

Pour autant, cette application (qui n'est pas encore au point technologiquement) devra être supprimée dès la fin de l'épidémie, et les autorités de contrôle devront s'en assurer.

CONCLUSION

15. Le propre des grandes crises est qu'elles obligent à préparer un nouvel avenir, et non pas à restaurer le passé. Celle que nous impose le COVID 19 est sans précédent depuis 1945 - au moins - pour l'hémisphère nord. Ses conséquences sont déjà sanitaires et économiques. Mais ne doutons pas qu'elles frapperont aussi l'ordre politique des nations, en les poussant parfois vers de dangereuses réponses autoritaires. Lors de la Seconde Guerre mondiale, le camp des pays libres a travaillé sur « l'après », bien avant le silence des armes. C'est donc dès à présent qu'il faut se saisir des outils numériques pour aider à lutter contre la propagation de la pandémie qui reviendra peut-être d'année en année.

Mais c'est aussi dès à présent qu'il faut se doter d'autorités de contrôle de l'utilisation massive de données personnelles et les doter de vrais pouvoirs. À l'échelle des pays membres, il faut rassembler et renforcer ces pouvoirs.

Au plan des Institutions Européennes il faut hisser une autorité de contrôle à la hauteur quasi constitutionnelle de l'enjeu : un Conseil des Droits et Libertés Numériques réunissant et consolidant pour cette tâche immense, permanente, les petites structures existantes, telles le « contrôleur des données ». Ce Conseil viendra en appui des structures nationales. Les pays membres de l'Union sont trop faibles individuellement pour encadrer et réguler seuls les usages de ces nouveaux outils numériques. Les industries capitalistes qui les exploitent transgressent parfois - c'est déjà le cas depuis une décennie au moins - les règles, lois, et parfois les souverainetés mêmes des États. L'Histoire, c'est sûr, regardera si nous avons été capables de faire face aux puissantes dérives si souvent observées à l'encontre des libertés individuelles, et demain collectives. Et si la pandémie a rassemblé courageusement l'unité des peuples et des États ou est parvenue à tout infecter.