COVID TRACKING : jusqu'où serons-nous collectivement prêts à abdiquer la protection de nos données personnelles?

Guillaume DESGENS-PASANAU, magistrat, professeur associé au Cnam, ancien directeur juridique de la CNIL

Publié le 21 avril 2020 – Mis à jour le 27 avril 2020

Alors que nous traversons la plus grave crise sanitaire de l'histoire moderne, il nous appartient collectivement de veiller à ne pas porter une atteinte irréversible à nos libertés fondamentales et individuelles.

@pexels

Le confinement subi depuis plusieurs semaines par 67 millions de français est certainement la plus grande opération de contrôle de la population organisée dans notre pays en temps de paix, dans un contexte où la loi organique d'urgence l'ayant instauré a légitimement suscité, sur le plan juridique, des inquiétudes liées à la faiblesse du contrôle juridictionnel et de constitutionnalité qu'il aurait justifié.

Dans le but de cartographier la propagation du virus, identifier les personnes à risque et faire respecter les mesures prises par le gouvernement pour endiguer sa propagation, de nombreux projets de surveillance des personnes sont désormais à l'étude. Ils reposent principalement sur des techniques de traçage des téléphones portables par géolocalisation ou utilisation de la technologie bluetooth (« contact tracing »).

Des initiatives ont déjà été prises. La société Orange a par exemple transmis aux pouvoirs publics les analyses issues de sa solution "FluxVision" selon lesquelles 17% des habitants du Grand Paris auraient quitté la région parisienne entre le 13 et le 20 mars. Le projet « StopCovid », piloté par l'INRIA et qui s'intègre dans le cadre du projet de recherche européen Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) vise quant à lui à alerter toute personne ayant été en contact avec un porteur du virus grâce à l'historique de ses interactions sociales.

Sans méconnaitre l'intérêt possible (mais pas toujours certain) de l'utilisation de ces technologies pour endiguer l'épidémie durant la phase de déconfinement, ces initiatives devront impérativement s'accompagner d'une réflexion attentive sur les enjeux induits en termes de protection de la vie privée.

« Nous sommes en guerre »

Plutôt que d'invoquer sans cesse l'existence d'une période inédite - justifiant ainsi des réponses extraordinaires - nous serions collectivement bien inspirés de prendre le temps d'un regard rétrospectif sur l'évolution des législations de protection des données au cours des 20 dernières années.

La « guerre » contre la crise sanitaire succède en réalité à près de 20 années de « guerre » contre le terrorisme engagée depuis les attentats du 11 septembre 2001. Cette volonté de renforcer la sécurité publique s'est

traduite en France par un nombre toujours croissant de législations spéciales, venant déroger aux principes fondamentaux du droit commun de la protection des données, lequel a été tout récemment renforcé au niveau européen à l'occasion de la mise en œuvre du règlement européen général sur la protection des données (RGPD).

Un exemple marquant est celui de la vidéosurveillance, désormais appelée « vidéoprotection », et plus récemment des techniques de reconnaissance faciale dont le développement s'est progressivement élargi dans l'espace public, au gré de lois évoquant tout d'abord la prévention d'actes de terrorisme, puis la protection des lieux particulièrement exposés à des risques d'agression, puis la prévention des risques naturels et désormais la simple constatation d'infractions aux règles de la circulation routière.

L'évolution des textes encadrant la vidéosurveillance est symptomatique de ce processus irréversible appelé "effet de cliquet" : une fois qu'une technologie de surveillance est mise en œuvre, son développement devient inéluctable et s'inscrit dans des usages de plus en plus banalisés à mesure qu'ils sont socialement acceptés. La multiplication de ces usages engendre un risque de mésusage des données, appelé risque de détournement de finalité. En 2020, ce sont près de 2000 caméras qui sont implantées sur les carrefours parisiens. Non plus seulement pour lutter contre une attaque terroriste, mais désormais selon les textes pour vérifier "l'obligation du port d'un casque homologué d'une motocyclette". Dans le même temps, les statistiques sur la violence routière dans Paris ont explosé, ce qui pose la question de l'efficacité réelle de cette technologie.

Allons-nous irrémédiablement poursuivre sur cette même pente en raison de la crise que nous traversons ?

Protéger nos données n'est pas qu'une coquetterie.

Alors que les morts se comptent par dizaines de milliers et que la crise économique gronde, l'histoire récente nous enseigne qu'il ne faut pour autant pas renoncer à préserver nos libertés individuelles.

L'absence de protection des données relatives à la santé des individus pourrait conduire à un grave risque de stigmatisation.C'est ainsi qu'à la fin des années 90, seule l'intervention de la CNIL a permis de mettre en œuvre un dispositif de surveillance épidémiologique des personnes séropositives tout en garantissant leur anonymat et l'absence d'exclusion sociale. Aujourd'hui encore, c'est le RGPD qui protège les salariés en interdisant aux employeurs de procéder par eux-mêmes à la collecte d'informations relatives à la recherche d'éventuels symptômes du virus, ceci étant réservé aux seules autorités sanitaires.

Plus largement, la constitution de fichiers visant à profiler les individus sur la base de leur comportement peut conduire à de graves risques de discrimination sur le plan économique. La question des "listes noires" défraye ainsi régulièrement l'actualité, comme par exemple tout récemment au sujet d'un fichier national des incidents de paiement dans le secteur du logement locatif, dont la mise en œuvre a été interrompue suite à l'action de la CNIL. **A l'heure de la mise en œuvre d'outils de détection ou de surveillance d'individus atteints du COVID, quelles seraient les conséquences de la délivrance éventuelle de "certificats d'immunité" ou de la création de listes de personnes immunisées ?**Que deviendra celui qui, ne disposant pas d'un tel certificat, se verrait demain interdire l'accès à des commerces ou services de première nécessité ?

N'oublions pas également que la technologie ne constitue jamais une solution miracle. Ainsi, les données de localisation issues des téléphones reposent sur des infrastructures techniques dont la précision et la fiabilité sont très variables. Leur efficacité en termes de lutte contre la pandémie est de ce point de vue à relativiser et ne risque pas de remplacer nos « gestes barrières ». Comme pour toute technologie innovante, par exemple en matière de biométrie, il faut scrupuleusement évaluer le risque de « faux positif », c'est-à-dire le risque que la machine se trompe ! **Le contrôle par la machine ne doit pas remplacer le contrôle par l'humain.**

Ne pas céder à la tentation de législations d'exception

La réglementation européenne, qu'il s'agisse du RGPD ou de la directive « e-privacy », autorise la mise en œuvre d'outils technologiques de lutte contre la pandémie tout en préservant nos libertés fondamentales. La géolocalisation des individus est par exemple possible, à la condition de respecter certains principes fondamentaux, en particulier l'anonymisation des données.

Il importe par conséquent, à court mais aussi à plus long terme, de ne pas déroger à ces règles, en exhortant nos législateurs à ne pas céder à la tentation d'adopter des législations dérogatoires qui viendraient ainsi détricoter les principes construits en France et en Europe depuis près de 45 ans, et qui, à coup sûr, perdureraient au-delà de la crise sanitaire.

Activer d’urgence les mécanismes de contrôle institutionnel

Les contrepouvoirs institutionnels doivent pleinement jouer leur rôle dans l’analyse des dispositifs à venir de surveillance massive de la population.

Alors que les pouvoirs publics insistent sur l'effort de transparence qu'ils entendent engager pour informer le public sur l'évolution du virus, la même transparence doit être attendue des autorités indépendantes de contrôle et en particulier de la CNIL, laquelle est restée jusqu'à présent très frileuse. Son rôle ne doit pas se limiter à accompagner les acteurs institutionnels en leur rappelant poliment le cadre juridique applicable.

Il incombe à la CNIL de se positionner plus clairement et communiquer publiquement sur les lignes rouges à définir concernant l'action à venir des pouvoirs publics et des opérateurs privés. **Concernant l'utilisation de données de géolocalisation, l'anonymisation systématique et irréversible des données sur les individus devrait être consacrée comme l’unique solution acceptable sur le plan des libertés individuelles.**Cette position a d’ailleurs été adoptée dès la mi-mars par le Comité européen à la protection des données (CEPD).

Par ailleurs, dans le cadre des pouvoirs élargis de contrôle et de sanction dont elle dispose depuis l’entrée en vigueur du RGPD, la CNIL devrait rendre régulièrement compte au public, pour chaque projet, des vérifications qu’elle engage concernant les dispositifs de surveillance à venir, par exemple afin d’évaluer chaque dispositif d’anonymisation utilisé et garantir l'absence de risque de ré-identification des personnes concernées.

Au-delà, il appartiendra également à l'autorité judiciaire de jouer pleinement son rôle dans le contrôle de la légalité et de la proportionnalité des dispositifs envisagés.

Engager un véritable débat de société

Il ne suffit pas de rappeler que notre droit pose des règles de protection de nos données. Encore faut-il que la société veuille bien s’en emparer.

Dans le contexte où les individus se sont de plus en plus accommodés à l'usage des technologies, au point de ne plus en percevoir parfois les risques (comme en matière d'exposition de soi sur les réseaux sociaux), la crise sanitaire est une occasion unique de relancer un grand débat de société sur l’équilibre à construire entre technologie, sécurité et liberté.

Ce débat devrait impliquer au premier chef la représentation nationale, la société civile et les corps intermédiaires. La perspective d'un débat au parlement français fin avril concernant le traçage des données mobiles initialement annoncé sans vote était de ce point de vue tout à fait navrant.

N’en déplaise à certains, la dimension européenne ne devra pas être oubliée. Elle est même essentielle : à l'heure où Google et Apple annoncent s'associer pour rationaliser l’exploitation des données issues de nos téléphones portables et ainsi mieux nous protéger, se pose crûment la question de notre souveraineté numérique. Notre modèle européen de protection des données est l'un des plus protecteur au monde. Il serait grand temps de le faire prévaloir, et de se réarmer sur le plan industriel en investissant massivement dans la conception d’outils numériques made in Europe et « privacy by design ».

| Droit | Innovation | Informatique | Numérique | Sécurité | Société

UE "Métier du délégué à la protection des données"

UE "Droit des nouvelles technologies, de l'information et de la communication : perfectionnement"

Certificat de spécialisation "Délégué à la protection des données (DPO/CIL)"

L'auteur

Guillaume Desgens-Pasanau, magistrat, professeur associé et responsable national du certificat de spécialisation Délégué à la protection des données.
Découvrez son blog consacré à l'actualité en matière de protection des données.

+ tous ses articles

http://blog.cnam.fr/technologie/covid-tracking-jusqu-ou-serons-nous-collectivement-prets-a-abdiquer-la-protection-de-n