Les applications pour suivre le Covid à la trace questionnent notre rapport à la cybersurveillance étatique.

«DÉPISTER, AVANT DE TRACER»

Pour Francisco Klauser, «nous devons prendre le temps de la réflexion, penser au-delà de l'application». Lianhao Qu

« GILLES LABARTHE

Numérique » «Pour ou contre» un système de traçage des personnes et de leurs déplacements, dans le cadre de la lutte contre la pandémie? A l'Institut de géographie de l'Université de Neuchâtel, le professeur Francisco Klauser a dirigé plusieurs programmes de recherche sur la problématique de la surveillance, des technologies dites «intelligentes», ou sur les implications du big data. Il souligne à quel point le débat actuel est polarisé, quitte à masquer la complexité des enjeux. Et invite à prendre le temps de bien réfléchir à la place de l'humain face à la technologie. Interview

Quand avez-vous commencé à étudier la surveillance?

Francisco Klauser: Mon intérêt pour la surveillance remonte à plus de 20 ans. Une de mes premières portes d'entrée dans ce domaine avait été d'étudier l'incidence de l'installation en Suisse de caméras de vidéosurveillance en milieu urbain. C'est un type de dispositif qui est relativement visible, physiquement présent, par rapport à d'autres technologies numériques: les gens peuvent voir qu'ils sont filmés. Quelles étaient les implications sociales, spatiales, par exemple en termes d'exclusion? Mes recherches ont ensuite porté sur les différents usages d'autres technologies plus spécifiques, comme les drones. Ou comme les smartphones, qui sont aujourd'hui un outil privilégié pour toutes sortes d'activités. Ils agissent comme des interfaces, aussi pour le contrôle de l'espace. Mais il faut éviter les débats trop polarisés, comme ceux auxquels on assiste aujourd'hui: en soi, ces technologies ne sont ni des «solutions miracle», ni des instruments de contrôle total pour Etat policier.

Le documentaire *Tous surveillés* (voir ci-contre) rappelle cependant que la cybersurveillance a atteint un niveau inégalé en Chine...

J'ai vu ce film... et je dois dire qu'au niveau des technologies utilisées, il ne montre rien de nouveau. Mais c'est une bonne chose qu'il existe. Il nous rappelle que toutes nos activités génèrent des données, et nous devons être sensibilisés à l'usage qui peut en être fait. Cela pose le débat de ce qui est acceptable. Nous devons définir ce que nous voulons comme genre de société. Et ce que nous ne voulons pas.

«La technologie seule ne va pas tout régler»

Francisco Klauser

A propos de risques, il y a une double tendance: d'un côté, avec le cumul de toutes les traces numériques laissées, la quantité de bases de données, et toutes les informations collectées, il faut rester attentifs au pouvoir que représente leur combinaison possible. De l'autre, qu'en est-il de l'automatisation de la surveillance? Les humains seuls ne parviennent plus à gérer une telle masse de données. Aujourd'hui, ce sont des algorithmes qui identifient des comportements à risque, effectuent le suivi et prévoient des réponses automatisées... c'est un autre problème, qui comporte également des risques d'erreur.

En Suisse aussi, nombre de spécialistes martèlent que le triptyque «tester, tracer, mettre en quarantaine» est LA solution pour combattre le Covid-19. A se demander comment on faisait avant l'apparition du smartphone...

Il y a en effet plusieurs manières d'enrayer la propagation de la pandémie. On peut se confiner, isoler, mettre en quarantaine, mettre en place des barrières. C'est ce qui a été fait dans le passé. On peut aussi recourir à la technologie pour trouver des solutions qui permettent plus de flexibilité. C'est la logique actuelle, et elle est assez claire: contenir la pandémie de façon efficace, limiter les interactions avec les personnes contaminées, mais de manière flexible, plutôt que dans un système rigide; ouvrir les frontières, tout en garantissant un niveau suffisant de contrôle.

Aujourd'hui, tout le monde a un smartphone dans sa poche: les applications d'alerte développées en Suisse et en Europe utilisent donc cet outil pour tracer. Accepter de livrer nos données, c'est en somme le prix à payer en échange de notre liberté de mouvement. Et je pense qu'il y a une majorité de gens qui sont aujourd'hui prêts à payer ce prix, pour pouvoir sortir de chez eux ou retourner au travail. Par contre, je ne comprends pas que l'on parle de cette application comme de la «solution miracle», alors même que nous sommes très en retard sur les tests de dépistage. L'application ne sera efficace que si elle est alimentée de suffisamment de données pertinentes, sinon elle ne vaut rien. Nous devons prendre le temps de la réflexion, penser au-delà de l'application. La technologie seule ne va pas tout régler. Ces programmes sont conçus et alimentés par des humains. Ils dépendent des informations qui leur sont fournies, ne fonctionnent pas toujours correctement, font de plus en plus l'objet de tentatives de hacking... et donc, restent fragiles.

Ainsi des brèches subsistent, pour échapper à un maillage de plus en plus serré...

Pour les programmes de surveillance, il y a des différences extraordinaires selon les contextes. C'est une question de principe. Certains programmes se justifient suivant les situations: c'est le cas aujourd'hui. Après, même les programmes les plus sophistiqués restent fondamentalement limités. Certains ne cessent de tomber en panne. Les programmateurs peuvent se tromper, faire des erreurs... et cela se révèle moins efficace que ce qu'on aurait pu penser. Ce n'est donc pas une surveillance à la «Big Brother» tout-puissant: la réalité est beaucoup plus complexe et il reste des formes de contre-pouvoir. Le fait par exemple de filmer les actions de la police avec son téléphone portable montre qu'on peut aussi résister en s'appropriant ces technologies.

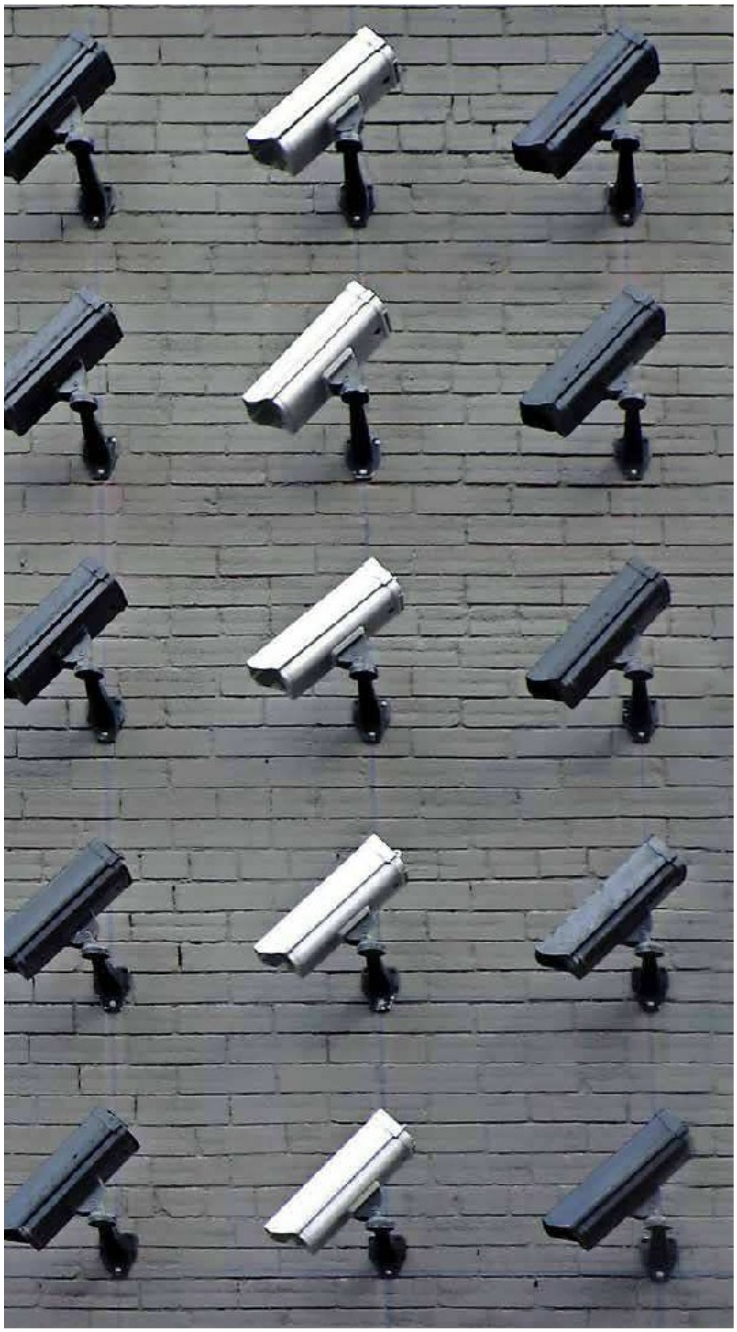
Mais d'un autre côté, qu'est-ce qui arrive après que de nouveaux instruments de surveillance ont été développés et installés pour répondre à un contexte exceptionnel? Nous devons nous poser la question. Car on le sait bien, une fois mis en place, ces nouveaux programmes ont tendance à rester.

Quelle est la situation suisse en matière de surveillance?

La Suisse n'est pas la Chine, ni une dictature, ni un pays fortement centralisé, comme la France ou la Grande-Bretagne, qui ont développé de vastes programmes informatiques axés sur l'accumulation des données personnelles. La surveillance policière reste beaucoup plus modeste qu'ailleurs. En tant que pays décentralisé, la Suisse a des processus de décision qui peuvent relever du niveau cantonal, voire communal, et les décisions sont prises presque séparément. Nous avons quand même une tradition assez importante de protection de la sphère privée, comme d'autres pays, l'Allemagne par exemple. Et je dois dire que je suis personnellement très fier de la décision prise en Suisse, et par des responsables de l'EPFL-EPFZ, de se distancier du projet de recherche européen et de préférer un mode de gestion décentralisé des données. Cela ne résoudra pas tout, mais cela va déjà dans le bon sens. »

> Lire aussi en pages 19

Derrière ce débat très polarisé, un enjeu majeur: la place de l'humain face à la technologie



SWISS PT

» **NOM**
PT signifie *proximity tracing*, pour «traçage de proximité».

» **CRÉATION**
Sur mandat de l'OFSP, l'appli a été développée par l'EFPL, l'EPFZ et la société suisse Ubique.

» **PRINCIPE**
Grâce au Bluetooth, l'appli détecte si deux smartphones se trouvent à moins de 2 mètres pendant plus de 15 minutes. Si l'utilisateur est testé positif, les utilisateurs ayant été à proximité de lui sont notifiés.

» **CALENDRIER**
Après une phase pilote, l'appli sera disponible en juin.

» **UTILISATION**
Gratuite et sur base volontaire.

» **DURÉE**
«Une fois la crise du coronavirus passée, ce système sera supprimé», promet l'OFSP.

UN MARCHÉ DE LA SURVEILLANCE EN PLEINE SANTÉ

Images satellite, par caméras ou drones; outils de surveillance d'internet, de géolocalisation, de reconnaissance faciale; QR codes… Réalisé en 2019, le film documentaire *Tous surveillés. 7 milliards de suspects* montre le cocktail de technologies liberticide déployé en Chine, à des fins de contrôle et de répression – sur la minorité musulmane ouïgoure, notamment. A cela s'ajoute la désormais célèbre application gouvernementale de traçage des concitoyens, obligatoire sur tous les smartphones: elle distribue des «bons» et des «mauvais» points, selon les comportements de chacun. Les mal notés se retrouvent «punis», mais une autre sanction les attend encore: l'opprobre, puis l'isolement social…

Une situation extrême, certes. Or, après l'invocation de la lutte contre le terrorisme, la pandémie du coronavirus représente aujourd'hui un nouvel argument de vente pour les concepteurs et développeurs de systèmes de traçabilité, inspirés de près ou de loin par le «modèle» chinois. Plusieurs pays d'Asie ont déjà mis en place des applications «anti-Covid-19» sur une base obligatoire, ou volontaire (comme à Singapour). Certaines se sont révélées à l'usage beaucoup plus intrusives que ce qui était initialement annoncé. Aux Etats-Unis, l'application Care19 est vantée comme la solution pour sauver des vies. D'autres projets similaires sont en cours en Europe, où 1,4 milliard d'euros sont injectés chaque année dans la recherche en matière de sécurité. Presque la moitié des mandats sont attribués à des entreprises privées. Quelle est leur part de responsabilité? Qui les contrôle en retour? **GIL**

› *Tous surveillés. 7 milliards de suspects*, de Sylvain Louvet, à voir sur Arte.tv jusqu'au 19 juin.

FAUT-IL INSTALLER L'APPLI SWISS PT?

OUI **Jean-Philippe Walter, commissaire à la protection des données du Conseil de l'Europe.**

«Mon adhésion est liée au respect de garanties fortes et au fait que cette application ne peut être considérée comme un outil de surveillance individuelle dans les mains de l'Etat. La protection des données est pleinement compatible et conciliable avec d'autres droits fondamentaux et intérêts publics pertinents. Elle n'est ainsi pas conçue pour s'opposer au recours à la technologie. Il est cependant essentiel de veiller à ce que les garanties soient mises en œuvre lors de l'adoption de mesures extraordinaires destinées à protéger la santé publique. Ces mesures doivent être nécessaires et proportionnées à la finalité légitime poursuivie et refléter un juste équilibre entre tous les intérêts concernés et les droits et libertés en jeu. Il faut au préalable en évaluer la nécessité et les risques.

Cette évaluation me semble avoir été faite à satisfaction par nos autorités et l'application offrir des garanties élevées et suffisantes. Le déploiement se fera lorsque le parlement aura adopté une loi qui en fixera le cadre et les conditions. Au préalable, le Conseil fédéral procédera à une phase de test qui permettra de vérifier l'efficacité du dispositif et de corriger des erreurs. La finalité est clairement définie et l'information du public transparente. L'application fonctionne sur un système décentralisé, contribuant à limiter le risque d'accès non autorisé. Les données restent dans nos téléphones et les personnes l'utilisant ne sont pas identifiées. Le système alertera de manière anonyme les utilisateurs exposés à la maladie lors d'un contact prolongé avec une personne positive. Il ne communique jamais avec les autorités. Seule la personne concernée est alertée et prend contact avec l'autorité sanitaire. L'installation et l'utilisation se font sur une base volontaire. Elle sera désactivée une fois la pandémie conjurée et les données effacées. Enfin, je compte sur le préposé fédéral à la protection des données pour surveiller le respect des exigences légales.»

NON **Sébastien Fanti, avocat, préposé valaisan à la protection des données et à la transparence.**

«Liminairement, je tiens à affirmer, avec force, que je suis favorable au traçage de l'actuelle pandémie, tout en observant que la pertinence de cette démarche digitale suscite encore de nombreux questionnements, le traçage manuel demeurant, d'un avis unanime, absolument nécessaire. La posture adoptée ci-après n'est donc pas l'expression d'un rigorisme introversif en termes de protection des données, mais un exercice démocratique à l'heure où l'information officielle confine, parfois, à la propagande, alors que la transparence devrait être une vertu cardinale du droit d'urgence.

Le solutionnisme technologique est une croyance selon laquelle les problèmes pourraient être résolus de manière simple et rapide grâce aux nouvelles technologies. Cette approche est pourtant problématique, car toutes les technologies, aussi efficaces soient-elles, n'apportent pas de réels avantages. En l'occurrence, l'application Swss PT divise les experts en sécurité informatique. Rarement un projet n'aura généré un débat aussi vif dans notre pays. Des collègues de l'EPFL publient des prises de position diamétralement opposées. Bref, les garants de notre sécurité ne sont pas d'accord. Lorsque l'analyse des risques génère des résultats aussi fondamentalement antinomiques, le principe de précaution doit prévaloir. Rappelez-vous du dossier électronique du patient, censément sécurisé. Ce d'autant que nous dépendons partiellement de Google et d'Apple pour que le processus choisi prospère. Et que la technologie utilisée, soit le Bluetooth, est imparfaite. Elle va générer des faux positifs. Ainsi vous risquez fort de devoir vous autoconfiner inutilement, ce qui va générer une perte de revenu ou de chiffre d'affaires. Cette application crée donc des attentes inconsidérées. Ne sommes-nous pas capables, dans notre pays, de développer un processus de traçabilité fiable et neutre technologiquement?» » **TR**

L'Europe en ordre dispersé

Entre la France et l'Allemagne, les deux locomotives européennes du développement d'applications de traçage, c'est l'incompréhension. Deux visions s'affrontent.

Le moins que l'on puisse écrire est que les applications de traçage de la propagation du Covid-19 font débat. Et pas seulement en Suisse. Chez nos voisins européens également la pratique divise, entre flou quant aux modalités techniques et risques d'une dérive en matière de surveillance. La question de la centralisation des données creuse notamment un profond fossé entre la France et l'Allemagne. Avec son application baptisée StopCovid, la France mise en effet sur une centralisation des données. Avec ce système, un utilisateur de l'application diagnostiqué positif au coronavirus sera invité à «donner son consentement afin que son historique de crypto-identifiants rencontrés soit envoyé sur un serveur d'une autorité de santé sans divulguer ses propres crypto-identifiants». Dans un premier temps Berlin défendait la même approche, mais les Allemands ont fini par retourner leur veste, optant pour une solution décentralisée. Un revirement crucial qui apporte de l'eau au moulin des ardents défenseurs de la protection des données personnelles. Outre-Rhin, la peur d'un grand fichier étatique à la «Big Brother» l'a finalement emporté. La Suisse s'est également distanciée de cette approche centralisée, avec les mêmes craintes.

En France, c'est l'incompréhension. Vu de Paris, le système centralisé offre l'avantage de donner une vision d'ensemble de l'évolution du virus dans le pays. La perspective d'une application unique dans tous les pays européens aurait en outre permis de mutualiser les informations. C'était sans compter la levée de boucliers de scientifiques et de militants contre les potentielles dérives de ce système. Reste qu'au-delà des dérives potentielles et des garanties étatiques quant à la protection des données, c'est l'utilité même d'une application de traçage qui fait débat. Selon une étude de l'Université de Cambridge, au Royaume-Uni, l'utilisation de logiciels induit quantité de problèmes pratiques. Notamment ceux des faux positifs ou l'inefficacité d'une application si elle n'est pas massivement adoptée par la population. On estime qu'il faudrait que 80% des possesseurs de smartphones jouent le jeu. Un pari loin d'être gagné. » **OW**