14 avril 2020

Utiliser les données pour lutter contre la pandémie

Questions et réponses sur l’utilisation de données

La lutte contre la propagation du coronavirus est un défi de taille. Un des problèmes réside dans le fait que les personnes infectées peuvent transmettre le virus à d’autres avant de se rendre compte qu’elles l’ont contracté. L’actuel confinement adopté par le Conseil fédéral est aussi et surtout une réponse au fait que tout un chacun peut potentiellement transmettre le virus ou en être infecté. Les mesures prises jusqu’ici veulent, avec le respect des règles de distanciation sociale, permettre de briser les chaînes d’infection en agrandissant l’espace de sécurité entre les personnes.

Comment exploiter des données pour combattre la pandémie ?

Pour endiguer la propagation du virus, il serait notamment très utile de pouvoir retracer les contacts personnels des patients lorsqu’ils ne présentaient pas encore de symptômes. Averties, les personnes concernées pourraient adapter leur comportement en conséquence. L’on peut également visualiser si les règles de distanciation sociale sont respectées et, en théorie, déterminer le lieu approximatif où se trouve une personne infectée. Des gouvernements et entreprises du monde entier réfléchissent à la manière d’exploiter à ces fins les données des opérateurs de téléphonie mobile ou les données des utilisateurs générées par des applications sur les smartphones. Les approches diffèrent, avec ou sans référence à la personne, selon les règles prévalant en matière de protection des données et la conception des droits de la personnalité dans un pays donné.

Il faut distinguer entre a) les données que génèrent les utilisateurs du réseau de téléphonie mobile et qu’ils mettent à la disposition de la Confédération et b) les applications spéciales installées sur les terminaux des usagers pour évaluer dans quelle mesure ils sont personnellement touchés. Sous c) il faut, par souci d’exhaustivité, mentionner que certains pays asiatiques recourent à des applications qui, par leur atteinte grave et massive aux droits de la personnalité, n’entrent pas en ligne de compte ni pour la Suisse ni en Europe.

A) Utilisation de données de téléphonie mobile existantes, générées par les utilisateurs

↓ **À quelle fin l’Office fédéral de la santé publique (OFSP) a-t-il pu récemment accéder aux données visualisées de Swisscom ?**

À la demande de l’OFSP, Swisscom lui fournit des analyses sur la mobilité et sur l’affluence dans l’espace public. Les données servant pour les analyses et visualisations sont anonymisées et agrégées. Elles ne permettent ainsi aucune identification des individus. Grâce aux analyses, l’OFSP peut vérifier si l’interdiction de rassemblement dans les lieux publics, sur les sentiers et dans les parcs est respectée.
Les analyses fournissent également des indications concernant l’impact général des mesures sur la mobilité des personnes. Il a ainsi été possible de déterminer si les mesures prises devaient être adaptées.

↓ **Comment fonctionne la plateforme Mobility Insights (MIP) de Swisscom ?**

La plateforme Mobility Insights est un produit déjà utilisé par Swisscom. Au moyen de statistiques de groupes anonymisées, les clients commerciaux peuvent obtenir, par exemple, des informations sur les flux de trafic à des heures précises. Générées sur le réseau mobile, les données en question sont aussitôt anonymisées conformément à la loi sur la protection des données et éditées sous forme agrégée pour l’analyse. Il est ainsi possible de créer des « cartes thermiques » qui montrent la présence de cartes SIM dans un lieu public (unité de base : quadrants de 100 x 100m, mesure à partir de plus de 20 cartes SIM). En lien avec l’utilisation de la plateforme MIP par l’OFSP, Swisscom a publié un document FAQ très complet (en allemand) expliquant le fonctionnement et les bases.

↓ **L'utilisation, par l'OFSP, des données de localisation issues du réseau de téléphonie mobile est-elle conforme au droit de la protection des données ?**

L'OFSP ne reçoit pas de données de localisation de Swisscom. Swisscom a permis à l'OFSP d'accéder uniquement à des analyses utilisant des données agrégées et anonymisées, avec un décalage dans le temps. Ces analyses ont été présentées à l'OFSP sous une forme éditée et visualisée pour l'usage prévu. Au sein de l'OFSP, une seule personne a reçu le droit de les consulter. Le préposé fédéral à la protection des données et à la transparence (PFPDT) a récemment classé le processus comme conforme au droit de la protection des données. Depuis, Swisscom a préparé pour le public un fichier FAQ détaillé sur l'utilisation de la plate-forme MIP par l'OFSP et le traitement des données concernées. En outre, chaque détenteur d'une carte SIM peut demander à l'opérateur, en ligne ou par téléphone, de bloquer celle-ci pour l'évaluation des données de localisation ou de mobilité (opt-out).

B) Collecte de données à l'aide d'applications spécifiques

↓ **Les recueils de données des multinationales technologiques peuvent-elles servir pour lutter contre la pandémie ?**

L'affluence sur un lieu peut être visualisée sur l'application Googlemaps, par exemple. Apple aussi possède un accès complet aux données de position des smartphones. Bien que la situation exceptionnelle permette sans doute à la Confédération d'ordonner la remise de ce genre de données, les experts estiment que leur fiabilité et valeur informative est insuffisante. Les valeurs de référence sur lesquelles elles reposent ne sont pas bien connues. Dans le contexte actuel de lutte contre la pandémie, ce genre d'approche n'est guère la meilleure option. Il y a d'autres moyens techniques permettant de mieux atteindre l'objectif d'une recherche de contacts efficace, à savoir identifier et informer de façon ciblée des cas suspects et leurs contacts.

↓ **Comment peut-on utiliser les smartphones pour lutter contre la pandémie ?**

Des diverses applications pour smartphones en cours de développement, certaines sont déjà utilisées en Asie. L'idée des applications dites de recherche de contacts est de suivre les contacts et d'isoler les cas suspects. La conception de la protection des données varie alors selon les pays.

↓ **Qu'est-ce que le projet en logiciels PEPP-PT ?**

PEPP-PT est l'acronyme de Pan-European Privacy-Preserving Proximity Tracing et le nom de l'organisme sans but lucratif européen fondé récemment. Ce projet est mené par une équipe d'environ 130 employés de 17 instituts, organisations et sociétés d'Europe. L'École polytechnique fédérale de Lausanne (EPFL) y joue également un rôle de premier plan. En plus de jouir de l'attention de l'OFSP, le projet est soutenu par d'autres experts et instituts de recherche de renom à l'étranger, ce qui devrait accroître l'acceptation par les autorités internationales.

L'initiative entend fournir tout le fondement technologique ainsi qu'une version de base d'une application de recherche de contacts. À partir de là, les pays et le secteur privé peuvent développer leurs propres applications. L'interopérabilité des différentes solutions sera garantie par le fondement commun mentionné.

↓ **Comment fonctionne une application PEPP-PT ?**

Une application PEPP-PT s'appuie sur la technologie de transmission Bluetooth Low Energy (LE). Lorsqu'une personne installe l'application et active Bluetooth sur son smartphone, le téléphone envoie à intervalles réguliers un signal anonyme et scanne le réseau à la recherche de signaux identiques. Deux smartphones se trouvant à portée l'un de l'autre échangent les signaux et les enregistrent sous forme chiffrée. Un algorithme vérifie ensuite si la durée et la longueur du contact suffisent à provoquer une infection. Toute personne infectée peut, de son gré, saisir cette information via l'application et son smartphone la transmet à tous ses contacts durant la période d'incubation. L'information étant anonymisée, aucun destinataire ne peut identifier lequel de ses contacts était infecté. Sur cette base, le système avertit les personnes à risque et conseille de se mettre en quarantaine ainsi que de procéder à un test de diagnostic.

L'idée est d'avertir rétroactivement les contacts pendant la période d'incubation critique, lorsque les symptômes ne sont pas encore perceptibles. Cela est très utile pour un contrôle efficace de la pandémie et ne nécessite ni données personnelles ni suivi géographique des utilisateurs. Les smartphones fonctionnent un peu comme un phare sur une côte brumeuse : émettre un signal pour devenir visible. Les navires qui s'approchent captent le signal et y réagissent sans vraiment connaître l'émetteur.

↓ **Comment juger PEPP-PT au regard de la protection des données ?**

Les experts tant européens que suisses ne voient pas de conflit général entre la protection des données et l'utilisation décrite ici des données pour la lutte contre la pandémie. Cela suppose toutefois que les principes du droit de la protection des données soient appliqués correctement. Le préposé fédéral à la protection des données et à la transparence (PFPDT) salue les différentes mesures du projet : participation facultative, renonciation aux données de géolocalisation et utilisation d'identifiants temporaires. Selon le PFPDT, ces mesures démontrent que des aspects clés de la protection des données ont été pris en compte. Pour une évaluation finale selon les critères de la loi sur la protection des données, le PFPDT attend de voir la version définitive de l'application.

↓ **Quelles difficultés techniques peut-on rencontre en utilisant des applications de recherche de contacts ?**

Un des défis sera d'éviter les fausses alertes. Il peut arriver que, par mégarde (ou sciemment), une personne se dise infectée et inquiète ainsi inutilement les autres utilisateurs de l'application. Une solution possible est d'accepter uniquement les messages vérifiés, par exemple émis au nom d'un médecin. Ce problème n'est cependant pas technique, mais relève du processus et de la volonté des utilisateurs de faire bon usage de l'application. En outre, il faudra un nombre critique d'utilisateurs pour que le système fonctionne efficacement.

↓ **Quelles applications de recherche de contacts sont développées actuellement en Suisse ?**

Plusieurs solutions sont en cours de développement en Suisse. Elles suivent la même approche que PEPP-PT, donc avec une protection adéquate de la vie privée des citoyens. Les applications de recherche de contacts peuvent établir un relevé automatique des rencontres sans les sauvegarder dans la mémoire interne, avec des données personnelles sensibles. Relevons ici NextStep de la société Ubique, qui développe aussi l'application CFF : une version test est déjà disponible pour les smartphones Android, mais pas encore pour les iPhones. Ubique participe également au projet PEPP-PT. Voici une vidéo du développeur qui explique bien le fonctionnement de l'application. Un récent marathon de programmation, organisé sous le patronage du Département fédéral de l'intérieur et du Département de l'économie, a donné naissance à plusieurs prototypes conformes à la protection des données comme Virus Tracker ou We Trace, parmi d'autres, qui doivent maintenant aboutir à des produits concrets et commercialisables.

C) Autres méthodes de collecte de données, impensables en Suisse

↓ **Comment certains pays d'Asie de l'Est utilisent-ils les nouvelles technologies pour lutter contre la pandémie ?**

Pour briser les chaînes d'infection, certains pays d'Asie de l'Est utilisent déjà des applications. À ce stade, ils le font avec une conception de la protection des données différente de celle prévalant en Europe. Ainsi, l'utilisation des applications est en partie obligatoire. On sait de la Chine que ces systèmes renseignent non seulement sur l'état de santé, mais relaient des données allant jusqu'au numéro de la carte d'identité. Les groupes de population sont enregistrés selon un système de feux de circulation (vert, jaune, rouge) et réintégrés en conséquence au processus de travail. La géolocalisation et des plateformes en ligne existantes font en outre toute la transparence sur les « foyers d'infection » géographiques. Contrairement aux débats menés jusqu'ici en Europe, les systèmes dans le contexte asiatique servent non seulement à retracer les chaînes d'infection et à avertir les individus d'une infection potentielle, mais aussi à établir un contrôle social et à conditionner un changement de comportement. Ce qui peut être utile dans le but de lutter contre la

pandémie est exclu dans la conception suisse et européenne de la protection des données. Ces atteintes graves aux droits de la personne en faveur d'un contrôle étatique remettent fondamentalement en question la compatibilité avec la conception libérale de l'État.

↓ **Comment ces applications sont-elles constituées du point de vue technologique ?**

La principale différence par rapport aux solutions discutées en Europe est que l'État s'accorde des droits d'accès très étendus aux systèmes et données existants. Cela signifie, par exemple, que des données provenant de diverses applications quotidiennes sont agrégées sans consentement exprès. On ne parle donc plus vraiment d'application de recherche de contacts, mais plutôt de système de surveillance totale aux vastes ramifications.

En Chine, la recherche de contacts s'effectue surtout via un système intégré aux applications WeChat et AliPay, très populaires et répandues : les utilisateurs complètent un formulaire avec leurs coordonnées et signalent les symptômes comme la fièvre ou la toux. Les données sont analysées et la personne reçoit un code couleur : vert si elle est en bonne santé, jaune si elle a été en contact avec des personnes infectées, rouge si elle est infectée. Appelé « Health Code », ce code QR médical fonctionne comme un laissez-passer dans l'espace public, où seuls les porteurs d'un code vert peuvent se déplacer librement. À cela s'ajoute la surveillance déjà très poussée des espaces publics, que la Chine utilise également dans sa lutte contre la pandémie.

Autant de mesures fort invasives et non transposables à une démocratie. Pourtant, même des États démocratiques comme la Corée du Sud se servent des données de caméras de sécurité, cartes de crédit, téléphones portables ou systèmes de navigation des voitures pour la recherche de contacts.

↓ **Comment évaluer les processus en Asie de l'Est du point de vue de la protection des données ?**

Selon la conception du droit en Suisse et en Europe, les applications obligatoires et contraignantes qui, de surcroît, récoltent des données hautement sensibles et complètes, posent problème. Elles peuvent engendrer des incitations néfastes (« oubli » du téléphone portable à la maison) et des risques pour la sécurité. On parle ainsi déjà de marchés noirs révélant les déplacements exacts des personnes (même en temps réel), permettant de graves atteintes à la vie privée. Les préoccupations face aux approches très invasives en Chine ou en Corée du Sud ne sont pas uniquement liées à la protection des données, mais aussi de nature constitutionnelle. En Suisse, l'usage de ces instruments est hors de question.

↓ **Quelles méthodes moins invasives utilise-t-on en Asie ?**

D'autres pays asiatiques implémentent des mesures d'un autre genre, misant sur la transparence. Via des applications smartphones, les personnes infectées sont en contact direct avec les autorités et le système GPS sur les téléphones portables permet de les localiser. Les autorités s'appuient en général sur les données exhaustives des citoyens fournies via différents canaux. Des informations détaillées sur les personnes infectées sont alors aussi publiées, y compris les lieux où elles se sont rendues en dernier. En même temps, les applications indiquent si l'on s'approche d'une personne infectée ou du lieu où elle se trouvait. Bien qu'elles soient moins invasives qu'en Asie de l'Est, ces applications révèlent également beaucoup de données personnelles.