DS AVOCATS

FLASH INFO - CORONAVIRUS

9 avril 2020

#RGPD - Applications de traçage des citoyens en période de pandémie : la solution est-elle européenne ?

A l'ère où des services web ou des objets connectés inondent nos vies, les éditeurs aiment susurrer à nos oreilles la « chanson douce » selon laquelle, ces technologies viendraient nécessairement améliorer notre vie au quotidien dans le respect de notre vie privée. En échange du partage de nos données personnelles, nous pouvons en un clic (trop souvent compulsif), bénéficier de toutes sortes de services d'information ou de tâches traités par un assistant personnel mis à disposition de l'utilisateur. Au son de la voix ou des petits doigts de l'utilisateur-maître pianotant sur son matériel à l'obsolescence programmée, le programme-esclave exécute les ordres dictés en traitant les données concernées et souvent, malheureusement, bien plus que nécessaire.

Confinés et privés de nos libertés, quelles solutions les outils technologiques apportent-ils en cette période de crise sanitaire sans précédent ? La question du traitement des données personnelles par un dispositif technologique peut légitimement se poser dans un contexte où, au 23ème jour de confinement, nos libertés de mouvement (certains ajouteraient même, d'expression) ont considérablement été affectées pour des raisons évidentes de sécurité.

1. Des applications de tracking variées

Force est de constater que le marché est capable de proposer des applications permettant de suivre les individus dans leurs déplacements et ce, pour bon nombre d'activités (trajet, sport, rencontres, etc.). Depuis le début de la crise du COVID 19, certaines applications dédiées ont pu être rapidement développées. Elles ont pour vocation de traiter des informations sur les personnes contaminées et d'identifier le risque de contamination de celles avec qui le malade entre en contact.

Cependant, si l'initiative est louable, elle ne peut se faire au détriment du corpus de règles existant sur le territoire français et européen permettant d'assurer aux citoyens une exploitation de leurs données personnelles respectant leur vie privée et leurs libertés.

A l'étranger, Singapour a utilisé une technologie s'appuyant sur le Bluetooth qui enregistre l'historique des rencontres du propriétaire pendant 21 jours. Les données sont chiffrées et stockées localement sur le mobile. Si la personne suivie est contagieuse, il devient très facile d'avertir les utilisateurs dont il a croisé la route.

D'autres technologies permettent également de suivre les citoyens, avec différents degrés d'invasion de leur vie privée : le bornage téléphonique, la géolocalisation via des applications GPS, la vérification de l'utilisation faite des cartes bancaires et de transport, la vidéosurveillance (potentiellement couplée avec la reconnaissance faciale).

2. Stop Covid, l'application de tracking annoncée par la France :

En France, le ministre de l'Intérieur a annoncé le lancement d'une application sur smartphone, Stop Covid, traitant les données de géolocalisation des utilisateurs pour suivre l'évolution de la crise sanitaire liée à la pandémie Covid-19.

Le député Mounir Mahjoubi explique que l'application serait utilisée pour trois finalités :

- « l'observation des pratiques collectives de mobilité et de confinement » ;
- « l'identification des sujets contact en retraçant le parcours récent des personnes testées positives » et
- « le contrôle des confinements individuels ».

Si le traçage des citoyens, pour répondre à ces finalités, est envisageable au regard du droit français, cette question doit être analysée en prenant en compte les différents textes applicables.

Au-delà du Règlement général sur la protection des données n°2016/679 dit « RGPD » et de la loi n°78-16 dite « Informatique et Libertés » modifiée, la directive 2002/58/CE dite « vie privée et communications électroniques » trouve à s'appliquer.

Au vu du contexte actuel, dans quelles conditions le développement d'une application de tracking pourrait-elle être compatible avec le droit français ?

3. Le traitement de données anonymisées :

Privilégier le traitement de données anonymisées par ce type d'application est l'option que le Comité européen à la protection des données (CEPD) recommande dans une Déclaration du 19 mars 2020. Cette approche est sans aucun doute la plus protectrice de la vie privée et des libertés fondamentales.

Le gouvernement utilise déjà des données anonymisées collectées par Orange via des antennes-relais, pour « *l'observation des pratiques collectives* ». Ces données n'étant pas des données personnelles, sortent du champ d'application du RGPD. Rappelons toutefois que cette anonymisation doit être irréversible, durable et répondre aux exigences techniques imposées par le CEPD. Ainsi, les données ne doivent pas pouvoir être ré-identifiées, notamment par croisement avec d'autres jeux de données.

Le recours à une application permettrait d'exploiter des données personnelles supplémentaires, qui devront, à leur tour être anonymisées pour sortir du champ d'application du RGPD et de la loi Informatique et Libertés.

4. La mise en place d'un suivi individualisé des personnes :

La mise en place d'un suivi individualisé des personnes est nécessaire pour mettre en œuvre « *l'identification des sujets* » et « *le contrôle des confinements individuels* ».

Si le suivi individualisé est fait sur la base du volontariat, le responsable du traitement (c'est-à-dire, celui qui détermine les finalités du traitement et ses moyens qui, ici, reste encore à déterminer) sera dans l'obligation de recueillir le consentement des personnes concernées. Ce consentement doit être libre et éclairé. En pratique, le respect de telles règles risque d'être délicat à mettre en œuvre. En effet, si un employeur n'est pas en position de recueillir le consentement de ses employés en raison du « déséquilibre des rapports de force » (G29, WP259 rév.01), on pourrait douter de la validité du consentement qui serait recueilli par un ministère (par ex. le ministère de l'Intérieur) auprès d'un citoyen dans le traitement de ses données dans le cadre d'une crise sanitaire.

L'application Stop Covid qu'évoque ces derniers jours le gouvernement français comme solution à préconiser et qui est en cours de développement, se fonderait sur le volontariat, et ainsi le consentement de l'individu.

Quoiqu'il en soit, le refus d'un citoyen de consentir au traçage ne devrait pas être retenu contre lui. Ainsi, un citoyen qui refuserait d'être tracé ne devrait pas voir sa période de confinement prolongée par rapport à celle d'un citoyen dans les mêmes conditions de santé qui aurait, quant à lui, accepté d'être tracé.

Si le suivi individualisé est imposé aux citoyens, le traitement de données devra être autorisé par une loi, qui ne pourra s'affranchir des principes imposés par les textes. L'article 15 de la Directive « vie privée et communication électronique » autorise de limiter la portée de certains droits et obligations (notamment s'agissant des données relatives au trafic), pour assurer « la sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique ».

Ainsi, dans le cadre d'un suivi individualisé imposé, ce traitement devra notamment respecter les principes de proportionnalité, de limite dans le temps et d'information des citoyens.

Qu'il s'appuie sur le consentement de l'individu ou qu'il soit imposé par la loi, le caractère temporaire du dispositif est essentiel. En effet, poursuivre le traçage au-delà de la durée de l'état sanitaire d'urgence serait une atteinte grave aux libertés fondamentales. De même, le dispositif devra limiter autant que possible le caractère intrusif. Lors des traitements mis en œuvre, la fréquence de la collecte des données devra être appropriée. Ce point devrait faire l'objet d'une vigilance particulière de la part de la CNIL qui, rappelons-le, a récemment mis en demeure EDF et ENGIE pour n'avoir pas correctement recueilli le consentement des utilisateurs sur la fréquence de la collecte.

Un tel traitement serait soumis à contrôle par la Cour de justice de l'Union européenne et par la Cour européenne des droits de l'Homme, comme le rappelle le CEPD dans sa Déclaration du 19 mars 2020. Il devra également respecter des mesures de sécurité et stocker les données de manière à en garantir leur sécurité ce qui, selon la CNIL conduirait les fournisseurs à proposer des solutions de stockage en local sur le smartphone plutôt qu'une conservation sur un serveur centralisé (qui plus est, sur des serveurs partagés dans le cloud).

5. Vers une réponse européenne ?

Dans un communiqué du 6 avril, le CEPD appelle au développement d'une application européenne de tracking, utilisant la technologie Bluetooth, rappelant toutefois, qu'un tel dispositif de pistage massif devra être respectueux des règles en matière de protection des données et de privacy by design.

Par cet appel du 6 avril, sans aucun doute salutaire, le CEPD défend le recours à la technologie au service de la sécurité des citoyens européen.

*

Espérons que les mesures mises en place respecteront les droits et libertés des individus sur leurs données personnelles. Une atteinte à ces droits et libertés, au-delà de ce qui est strictement nécessaire, entacherait l'image de l'Europe, championne de la protection des données personnelles.

Antoine Gravereaux,
Associé
gravereaux@dsavocats.com

Ines Jousset
Collaboratrice
jousset@dsavocats.com

Pour plus d'information, notre équipe se tient mobilisée pour répondre à vos questions :

Catherine Verneret,
Associée
verneret@dsavocats.com

Bertrand Potot
Associé
potot@dsavocats.com

Sylvain Staub,
Associé
staub@dsavocats.com

Antoine Gravereaux,
Associé
gravereaux@dsavocats.com