unapl
UNION NATIONALE DES PROFESSIONS LIBÉRALES
PROFESSIONS LIBÉRALES, LES MÉTIERS DE LA VIE.
La lettre europe
@unapl_officiel
www.unapl.fr

N° 34 Mai 2020

NUMERO SPECIAL COVID- 19.

A l'heure où la France semble mettre un coup d'arrêt à la mise en place de l'application de traçage des contacts, StopCovid, il n'est pas inintéressant de faire un petit tour d'horizon tant théorique que pratique sur les applications de suivi numérique de l'épidémie au sein de l'UE et de divers Etats-Membres.

Alors que certains Etats ont déjà décidé de mesures de déconfinement et que d'autres s'apprêtent à le faire, certains estiment que ces applications de traçage numérique et l'exploitation des données de géolocalisation des citoyens pourraient se révéler très efficaces, du moins combinées avec d'autres mesures s'insérant dans le cadre d'une stratégie nationale plus globale.

La Corée du Sud, Singapour, Hong- Kong ont montré l'efficacité de telles méthodes, tout en réveillant des craintes légitimes et justifiées quant au risque d'utilisation abusive de ces données. Comment être efficace sans fouler aux pieds nos valeurs de respect de la vie privée et des libertés individuelles ? L'Europe fait figure d'exception dans le monde avec ses lois sur la privauté des données personnelles (règlement européen de protection des données ou RGPD[1] et directive e- Privacy[2]).

Une autre voie est-elle possible, conforme à la réglementation européenne ?

Ce que dit le droit européen en matière de données de localisation :

Si le traitement de données anonymisées de géolocalisation est autorisé par le droit européen, le traitement de données de localisation individualisées représente une étape supplémentaire qui requiert normalement, sauf circonstances exceptionnelles – dont l'épidémie fait partie !-, le consentement de la personne.

Le RGPD et la directive e- Privacy permettent, en premier lieu, de traiter **des données anonymisées de géolocalisation, c'est- à- dire suffisamment agrégées pour ne pas permettre d'identifier un individu particulier**.

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
[2] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

Ainsi, en **Belgique**, en **Allemagne**, en **Autriche**, en **France**, en **Italie** ou encore en **Espagne**, les opérateurs mobiles[3] ont accepté de communiquer les données de géolocalisation anonymisées de leurs abonnés aux gouvernements. Celles-ci permettent d'évaluer les **déplacements de population suite aux mesures de confinement ou encore d'affiner les études épidémiologiques,** autant d'informations essentielles pour que les autorités sanitaires dimensionnent en conséquence l'offre de soins dans les territoires**.** Elles ne ciblent toutefois **pas les individus**, mais fournissent des **données agrégées par zone géographique**, par exemple par commune. Dans des zones urbaines comme celles de Madrid ou Milan, les opérateurs téléphoniques ont ainsi fourni des "*heat maps*", des cartes permettant d'évaluer l'efficacité des mesures de confinement par quartiers.

Cependant, si elles sont utiles, ces données agrégées ne permettent pas, par définition, de faire de la **prévention personnalisée, c'est- à dire de prévenir quelqu'un qu'il a été en contact avec une personne porteuse du virus** et qu'il est donc à risque. Entrer dans cette dernière logique suppose **un traitement des données de localisation individualisées. Le RGPD et la directive e- Privacy autorisent celui- ci, sous certaines conditions, dès lors que l'utilisateur y consent.**

Pour être exact, le RGPD et la directive e- Privacy vont jusqu'à prévoir l'utilisation des données personnelles sans consentement lorsque des situations exceptionnelles l'exigent, en particulier la nécessité de sauvegarder les **intérêts vitaux** d'une personne, comme **en cas d'épidémie, dans les situations de catastrophe naturelle ou d'origine humaine, etc.**

Alors même que, dans le contexte actuel de crise du Covid- 19, le RGPD et la directive e- Privacy autoriseraient le recueil et le traitement de données personnelles sans le consentement des personnes, il est à remarquer que la base du volontariat semble la ligne rouge à ne pas dépasser dans tous les pays de l'Union.

Une ligne rouge que les Etats ne sont pas prêts à dépasser : les applications de traçage numérique resteront sur la base du volontariat.

Alors même que l'exemple de l'application TraceTogether à Singapour a révélé que ce type d'application n'est efficace qu'à condition d'être téléchargé par la majorité de la population, les Etats répugnent à le rendre obligatoire. La confiance des citoyens, qui sera notamment fonction de l'explicitation de la finalité poursuivie, sera donc essentielle pour permettre un large recours à celui-ci.

En vue de son déconfinement, commencé le lundi 20 avril, **la Norvège** a lancé dès le 16 avril sa propre application mobile de traçage, Smittestopp, qui **informe ses utilisateurs d'un possible contact (plus de 15 mn à moins de 2 m) avec une personne infectée, sans révéler l'identité de cette dernière. L'installation de l'application est volontaire. À rebours des orientations prises par l'Union européenne, elle fonctionne grâce à la géolocalisation, et non à la technologie Bluetooth,** afin de permettre également aux autorités sanitaires de mieux observer la propagation de l'épidémie et mesurer l'efficacité des restrictions. **Les données, anonymisées, sont centralisées et automatiquement détruites au bout de 30 jours.**

En République Tchèque, en vue du déconfinement, le gouvernement développe des **méthodes inspirées de celles mises en œuvre à Singapour ou en Corée du Sud, comprenant notamment l'utilisation, sur une base volontaire,** d'applications numériques qui permettent aux opérateurs de

[3] Orange a ainsi développé un outil de modélisation des flux de population à partir de données de géolocalisation anonymisées qu'il met au service de l'Inserm.

téléphonie mobile et de cartes de paiement de fournir des données en vue du **traçage des contacts des personnes infectées, afin de les informer des risques de contamination**. Le projet, qui comprend aussi des tests massifs, a été testé en Moravie du Sud.

L'Italie a annoncé être prête à tester dans plusieurs régions une **application de traçage de contacts, « Immuni »**, développée par la start-up Bending Spoons, en vue d'accélérer la sortie du confinement. En cas de succès dans les régions testées, l'application serait rendue disponible dans toute l'Italie. La proposition de la start-up milanaise, qui participe à l'initiative PEPP-PT[4], a été retenue par une commission spéciale parmi les centaines de propositions parvenues en réponse à l'appel lancé en mars par le ministre italien de l'Innovation aux développeurs informatiques. L'application utilise la **technologie Bluetooth** ; **si l'un des utilisateurs est testé positif, ses contacts seront prévenus par l'application et invités à se mettre en quarantaine et à se faire tester, le tout sur la base d'un strict anonymat. L'utilisation de l'application sera volontaire**, conformément aux recommandations de l'autorité italienne de protection des données, du CEPD[5] et de l'exécutif européen.

En France, l'application "***Stop-Covid***" permettant d'alerter les individus ayant été en contact avec un malade du Covid-19, qui devait être opérationnelle à partir du 11 mai, est au point mort, le gouvernement préférant ne pas prendre le risque de certaines dérives possibles, en particulier en termes de libertés individuelles.

Pour rappel, cette application devait fonctionner également **sur la base du volontariat**, en exploitant les données de géolocalisation des smartphones.

- L'application StopCovid ne devrait stocker que des « crypto-identifiants éphémères ». Ainsi, lorsque l'Etat enverra un message à une personne via l'application pour la prévenir d'une possible exposition au virus, il ne pourra obtenir ni identifiant du téléphone contacté, ni le nom du patient à l'origine de l'alerte.
- Elle était prévue de fonctionner sans géolocalisation.
- Contrairement à son équivalent polonais, StopCovid ne devait pas servir à vérifier le respect du confinement.
- Contrairement aux approches israéliennes, StopCovid ne devait pas permettre de retracer les déplacements passés.

Les autorités indépendantes de contrôle de la protection des données rappellent les exigences nécessaires.

Si les autorités indépendantes de contrôle de la protection des données des Etats -membres se sont inquiétées de décisions précipitées en la matière, en particulier en Allemagne et en Italie, elles invitent généralement les décideurs politiques à la prudence.

Ces instances ont en effet pour mission de contrôler l'action des Etats et autres puissances publiques, en particulier en temps de crise, pour prévenir les potentiels abus au nom de l'urgence, et jouer un **rôle de contre-pouvoir**.

Ainsi, dans un souci de démocratie et de protection des libertés fondamentales, les autorités de protection des données insistent pour un usage mesuré des données personnelles : *cet **usage doit être limité dans le temps et doit être réalisé de manière transparente**.*

[4] Consortium universitaire européen pan- European Privacy Preserving Proximity Tracing qui a vu le jour suite à la pandémie.
[5] Comité européen de la protection des données.

D'autant que les **données à caractère médical ou biométrique, particulièrement concernées par le suivi numérique,** constituent des données dites "**à caractère sensible**".

- **Le Comité européen de la protection des données (CEPD), qui se compose des autorités nationales et du contrôleur européen de la protection des données**, a publié le 21 avril des lignes directrices sur l'utilisation de la géolocalisation et des outils de traçage des contacts dans le contexte de l'épidémie de Covid-19.

  L'usage de ces outils, qui doivent être intégrés dans une stratégie sanitaire globale, doit être strictement **nécessaire et proportionnel**.

  Le comité rappelle la nécessité d'une **anonymisation « robuste »** des données de géolocalisation utilisées **et recommande la transparence sur les méthodes d'anonymisation employées.**

  En ce qui concerne le traçage des contacts, le comité rappelle sa préférence pour une **solution européenne, ou à tout le moins pour des applications interopérables**.

  L'usage du Bluetooth correspond mieux au principe de spécificité et de minimisation des données collectées que la géolocalisation.

  La surveillance des contacts entre individus constituant une « grave intrusion dans la vie privée», **l'utilisation de ces applications doit être volontaire, sans que le refus ou l'incapacité de les utiliser n'engendre de conséquence négative.**

  Le comité ne se prononce pas sur le choix d'un stockage centralisé ou décentralisé des données.

  Les autorités de santé doivent être responsables du traitement des données.

  Une notification d'infection par un utilisateur dans l'application doit se faire uniquement **sur la base d'une autorisation donnée par un professionnel de santé ou assimilé,** et non sur la base d'une simple présomption d'infection.

  Les algorithmes ne doivent fonctionner que sous stricte supervision humaine, et les codes sources utilisés rendus publics.

  Une **étude d'impact** concernant la protection des données doit être menée avant de mettre en œuvre ces applications.

  - **En France, la CNIL**, a pu rappeler notamment que **les conditions d'expression du consentement libre et éclairé devront être parfaitement claires et explicites.**

    Concernant le **principe de minimisation des données** (collecte uniquement des données strictement nécessaires), la CNIL a rappelé **l'importance de privilégier un identifiant plutôt que des données nominatives** ; les solutions doivent aussi privilégier le **chiffrement de l'historique des connexions.**

    A la différence du Comité européen de la protection des données, la CNIL s'est prononcée plutôt en faveur d'un stockage des données sur un téléphone, plutôt que de les envoyer systématiquement dans une base centralisée.

A noter :
Dans un avis en date du 24 avril, **le Conseil national du numérique** s'était prononcé favorablement à l'application "*Stop-Covid*" à condition que celle- ci s'insère dans une **stratégie exceptionnelle de santé plus globale qui relève de l'ordre public sanitaire et donc de l'intérêt général**. **La limitation dans le temps du système**, qui doit rester une réponse exceptionnelle à une crise qui l'est aussi, est un aspect essentiel.
Celle- ci doit être utilisée pour **informer, aider et responsabiliser, plutôt que pour contrôler, stigmatiser ou réprimer les individus.**
Le Conseil recommande en particulier qu'une **seule application spécifiée par l'État** soit mise en œuvre, **libre de tout soupçon d'intérêt économique sous-jacent.**
Le Conseil recommande de créer **un comité de contrôle** s'assurant de la bonne mise en oeuvre du système et garantissant le respect des valeurs qui le fondent tout au long de son usage.

Une boîte à outil, publiée par la Commission européenne le 16 avril dernier, en vue d'encadrer les applications de suivi de l'épidémie.

Le commissaire au Marché intérieur, Thierry Breton, a, d'ores et déjà, exclu tout recours à un usage obligatoire de ces applications et souhaite confier le traitement de ces données aux autorités de santé uniquement. Conçue avec le réseau d'autorités de santé eHealth, la boîte à outils, publiée formule les recommandations suivantes :

- installation d'applications nationales de traçage **sur une base volontaire** ;

- traitement des données personnelles dans le **respect du RGPD et de la directive eprivacy** ;

- **responsabilité de l'autorité nationale de santé** ;

- **désactivation des applications une fois la crise passée** ;

- **anonymisation des données** (l'identifiant ne doit pas désigner l'utilisateur) ;

- - **géolocalisation déconseillée**

- **applications interopérables entre elles dans l'UE** ;

- **lutte contre les applications tierces dangereuses**.

Pour consulter la boîte à outils de la Commission européenne : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52020XC0417(08)

Le Conseil de l'Europe alerte sur les risques sociétaux et juridiques des applications numériques de traçage liées à la prévention de la pandémie.

La présidente du Comité du Conseil de l'Europe sur la protection des données, et le commissaire du Conseil de l'Europe à la protection des données ont publié le 28 avril une déclaration conjointe relative aux effets secondaires possibles de ces applications. Ils préconisent la mise en place de garanties juridiques et techniques afin de limiter les risques d'atteintes aux données personnelles et à la vie privée.

Cette déclaration synthétise de façon très pédagogique et très claire les précautions élémentaires à respecter dans la mise en œuvre de ces applications. Celles- ci doivent garantir notamment **qu'aucune identification directe des personnes ne soit possible** et que toute nouvelle identification soit empêchée.

La finalité du traitement des données, identifier les personnes potentiellement exposées au virus, **doit être clairement spécifiée** et doit exclure strictement tout traitement ultérieur des données à des fins non liées (par exemple, à des fins commerciales ou répressives).

Les données relatives à la santé constituent une catégorie spéciale de données qui ne peuvent être traitées qu'avec des garanties appropriées qui complètent les autres exigences en matière de protection des données, comme le prévoit l'article 6 de la Convention 108+.

Compte tenu de la nature particulière des données de localisation et du fait que la proximité entre les personnes peut être obtenue sans les localiser, **le suivi numérique des contacts doit se faire sur la base d'enregistrements des connexions entre les dispositifs et non sur la base de données de localisation (données GPS par exemple).**

Même dans la situation actuelle, les personnes conservent le droit de ne pas être soumises à une décision les affectant de manière significative, fondée uniquement sur un traitement automatisé de données, sans que leur avis soit pris en considération.

La pandémie COVID-19 ne connaissant pas de frontières, l'interopérabilité entre les systèmes doit être assurée pour permettre un échange des informations disponibles au-delà des frontières nationales, à condition que les garanties nécessaires soient assurées.

Pour lire la déclaration : https://rm.coe.int/covid19-joint-statement-2-28-april-2-fr/16809e3fd6