

# ARTICLE

## LA CHASSE AUX DONNÉES, NOTAMMENT DE GÉOLOCALISATION, EN TEMPS DE CRISE SANITAIRE ET LA QUESTION DU RESPECT DE LA VIE PRIVÉE ET DES DONNÉES PERSONNELLES DES INDIVIDUS

IT et données personnelles Droit de la concurrence, consommation et distribution Contrats commerciaux et internationaux | 30/03/20 | Florence Chafiol Roxane Blanc-Dubois

SCIENCES DE LA VIE & SANTÉ

La crise du coronavirus est l'occasion de constater l'émergence de certaines initiatives, tantôt légitimes et encadrées, tantôt abusives et intrusives, venant tant d'entités privées que d'autorités étatiques, impliquant l'utilisation, parfois de masse, de données y compris personnelles.

Des dérives ont pu être constatées de la part d'entités privées : certaines d'entre elles ont profité de la crise sanitaire pour collecter, de manière déloyale, des données personnelles sur des individus en leur proposant de remplir en ligne des attestations de déplacement dérogatoire. La CNIL a mis en garde les citoyens contre cette pratique en rappelant que seules sont valables les attestations disponibles sur le site du gouvernement français.

Du côté des autorités étatiques, plusieurs d'entre elles ont entrepris de se rapprocher des opérateurs de téléphonie mobile, des réseaux sociaux, moteurs de recherche ou autres sociétés technologiques, afin de recueillir, auprès d'eux, des données sur les utilisateurs. A l'ère des nouvelles technologies et du smartphone, il est en effet potentiellement aisé de tracer les déplacements des individus. Ces informations peuvent s'avérer utiles afin d'identifier les individus ayant été en contact de personnes infectées et/ou pour anticiper les besoins médicaux.

Dans certains pays, notamment en dehors de l'Union européenne, certaines autorités sont allées jusqu'à tracer massivement les individus, parfois sans leur consentement, en obtenant les données auprès des opérateurs télécoms et/ou via des applications mobiles et ont alors divulgué publiquement des informations permettant d'identifier les personnes infectées par le virus.

Au sein de l'Union européenne, des initiatives basées sur la collecte de masse de données de géolocalisation sont également à l'œuvre ou envisagées, et ce, dans l'objectif notamment de modéliser la propagation du virus et/ou d'éviter que les individus ne se contaminent. Si ces initiatives semblent légitimes et utiles dans le cadre de l'actuelle crise sanitaire, ces dernières ne sauraient toutefois s'affranchir des règles édictées par l'Union européenne et les Etats membres en matière de protection de la vie privée et des données personnelles des individus. En effet, ce type d'initiative est notamment encadré par le Règlement Général sur la Protection des Données Personnelles (« **RGPD** ») et la Directive ePrivacy laquelle comporte des dispositions relatives aux données de localisation issues des communications électroniques.

Les données de communications électroniques telles que les données mobiles de localisation (lesquelles intéressent particulièrement les autorités) ne peuvent, en principe, être traitées que si elles sont anonymisées ou avec le consentement de la personne concernée (article 9 de la Directive ePrivacy). Néanmoins, la Directive ePrivacy prévoit (par exception) que les Etats membres peuvent prendre des mesures législatives spécifiques visant à déroger à la précédente règle et ce à des fins de sauvegarde de la sécurité publique (article 15 de la Directive ePrivacy). Toutefois, les mesures législatives en question qui permettraient l'utilisation de données de localisation non anonymisées et sans consentement des personnes, doivent être nécessaires, appropriées et proportionnées par rapport au risque de sécurité publique en cause. Ainsi, de telles mesures ne sauraient être mises en œuvre sans garanties appropriées.

A cet égard, le Comité Européen de la Protection des Données (« **CEPD** ») a recommandé aux autorités des Etats membres, par deux communiqués publiés le 16 et 19 mars dernier, de privilégier, en premier lieu, le traitement de données anonymisées (pour mémoire, le RGPD ne s'applique pas à de telles données). Si le traitement de telles données anonymisées ne permet pas d'atteindre l'objectif visé en lien avec la lutte contre la propagation du virus, alors des mesures législatives pourraient permettre le traitement de localisation non-anonymisées. En ce cas, le CEPD recommande que les mesures les moins intrusives possibles pour les individus soient privilégiées. De tels traitements doivent en outre être limités dans le temps (à savoir limités à la gestion de la crise sanitaire et les données supprimées dès la fin de la crise sanitaire) et ne pas être utilisées pour d'autre finalités.

A noter que certaines craintes émergent concernant l'utilisation des données de localisation à des fins de sanction des individus ne respectant pas le confinement. En Italie, les autorités italiennes ont pu détecter qu'environ 40% de la population en Lombardie n'aurait pas respecté les règles de confinement. Néanmoins, ce constat ne pourrait en principe se traduire en sanctions dans la mesure où les données utilisées par les autorités italiennes sont anonymisées.

Au niveau européen, des rumeurs circulent concernant un projet de la Commission européenne relatif à la surveillance de masse sur la base de données agrégées et anonymisées fournies par des opérateurs télécoms (dans un objectif de modélisation de la propagation du virus et d'anticipation des besoins médicaux).





En France, le gouvernement a réuni, le mardi 24 mars dernier, une instance dénommée le « CARE » (Comité Analyse, Recherche et Expertise) qui a notamment pour mission « *d'accompagner la réflexion des autorités sur l'opportunité de la mise en place d'une stratégie numérique d'identification des personnes ayant été au contact de personnes infectées* ». Pour l'instant, aucune autre information plus précise n'a été communiquée. Ladite stratégie pourrait, par exemple, consister à collecter des données de localisation anonymisées auprès des opérateurs télécoms comme préconisé par le CEPD ou, éventuellement, à proposer aux Français de télécharger une application visant à lutter contre la propagation du virus sous réserve que le téléchargement d'une telle application et la fourniture des données se fassent sur une base volontaire et de l'existence de garanties appropriées. A l'image de certains pays européens voisins qui ont entrepris des initiatives similaires et pour lesquelles l'avis de l'autorité locale de protection des données personnelles a été recueilli, la CNIL pourrait être consultée de manière officielle sur le projet final envisagé par l'Etat français concernant le traitement de données de géolocalisation dans ce contexte de crise sanitaire.

A noter que lors de l'examen du projet de loi d'urgence sanitaire (dont la version définitive a été adoptée le 23 mars dernier), un amendement, de portée imprécise, visant à autoriser « *toute mesure permettant la collecte et le traitement de données de santé et de localisation* » pendant six mois à compter de la publication de ladite loi, a été rejeté par le Sénat.

#### Liens utiles

[Communiqué du CEPD en date du 16 mars 2020 \(en anglais\)](#)

[Communiqué du CEPD en date du 19 mars 2020 \(en anglais\)](#)

[Communiqué de l'Elysée en date du 24 mars 2020 au sujet du CARE](#)

---