Focus : COVID-19 & RGPD

L'impérieuse nécessité des mesures sanitaires et de sécurité prises pour endiguer l'épidémie de Covid19 ne saurait éclipser l'importance d'inscrire ces mesures d'exception dans la légalité et le respect des droits fondamentaux, au titre desquels figure le droit à la protection des données à caractère personnel, protégé par l'article 8 de la Charte des droits fondamentaux de l'Union Européenne.

Les normes ne sont toutefois pas figées et peuvent souffrir des aménagements en cas de circonstances exceptionnelles. Ainsi, le règlement (UE) 2016/679 relatif au traitement des données à caractère personnel (d), prévoit dans son considérant n°46 que « *certains types de traitements peuvent être justifiés à la fois par des motifs importants d'intérêt public et par les intérêts vitaux de la personne concernée…, y compris pour suivre des épidémies et leur propagation* »[1].

Aussi, convient-il de s'interroger sur le cadre l'égal des traitements de données à caractère personnel et de santé effectué dans ce contexte de crise sanitaire par les entreprises et autorités publiques.

LE TRAITEMENT DE DONNEES A CARACTERE PERSONNEL PAR LES ENTREPRISES EN VUE D'ASSURER LA SECURITE DE LEURS EMPLOYES FACE A L'EPIDEMIE DE COVID19.

L'employeur est débiteur d'une obligation de sécurité et doit prendre les mesures nécessaires pour assurer la sécurité et protéger la santé physique et mentale des travailleurs. Il doit réaliser des actions de prévention, des actions d'information et de formation, ainsi que la mise en place d'une organisation et de moyens adaptés (article L4121-1 du Code du travail).

Face aux risques liés à l'épidémie de Covid19, certaines entreprises sont tenues ou peuvent poursuivre leur activité. Lorsque c'est possible, elles doivent et peuvent imposer le recours au télétravail.

Lorsque cela n'est pas possible, l'employeur, afin d'organiser le travail de ses salariés dans des conditions assurant leur sécurité, peut être amené à collecter des données les concernant afin de déterminer par exemple si des personnes présentent des symptômes du coronavirus, ou d'autres données relevant de la sphère privée.

[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

Pour être licite, un traitement de données à caractères personnel doit reposer sur une base légale (article 6 du RGPD). Le Comité Européen de Protection des Données, dans un communiqué du 19 mars 2020, considère que de tels traitements peuvent être effectués par les employeurs sur le fondement d'une des bases légales suivantes :

- un traitement nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis (article 6.1.c du RGPD), soit l'obligation de sécurité ;
- un traitement nécessaire à l'exécution d'une mission d'intérêt public (article 6.1.e du RGPD), soit le contrôle des maladies[2].

La CNIL, dans un communiqué du 6 mars 2020, rappelle tout d'abord que les employeurs ne peuvent pas prendre des mesures susceptibles de porter atteinte au respect de la vie privée des personnes concernées, **notamment par la collecte de données de santé qui irait au-delà de la gestion des suspicions d'exposition au virus**.

> Le RGPD définit les **données concernant la santé** comme « *les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* ». **Cette définition est large et inclut donc les informations concernant une maladie ou obtenues lors d'un test.**

Ces données font l'objet d'une protection toute particulière, tant par le RGPD que par les dispositions du Code de la santé publique.

> **Les employeurs doivent ainsi s'abstenir de collecter de manière systématique et généralisée, ou au travers d'enquêtes et demandes individuelles, des informations relatives à la recherche d'éventuels symptômes présentés par un employé et ses proches.**
>
> Il n'est donc pas possible de mettre en œuvre, par exemple des relevés obligatoires des températures corporelles ou la collecte de fiches ou questionnaires médicaux[3].

La CNIL précise que l'employeur peut, en revanche, sensibiliser et inviter ses employés à effectuer des remontées individuelles d'information les concernant en lien avec une éventuelle exposition.

> Il incombe, en effet, à chaque travailleur de prendre soin de sa santé et de sa sécurité ainsi que de celles des autres personnes concernées par ses actes ou ses omissions au travail (article

[2] https://edpb.europa.eu/news/news/2020/statement-processing-personal-data-context-covid-19-outbreak_fr
[3] https://www.cnil.fr/professionnel

L.4122-1 du Code du travail) : **le salarié doit donc informer son employeur en cas de suspicion de contact avec le virus**.

En cas de signalement, **un employeur peut consigner la date et l'identité de la personne suspectée d'avoir été exposée et les mesures organisationnelles prises** (confinement, télétravail, orientation et prise de contact avec le médecin du travail, etc.).

Il pourra aussi communiquer aux autorités sanitaires qui le demanderaient les éléments liés à la nature de l'exposition, nécessaires à une éventuelle prise en charge sanitaire ou médicale de la personne exposée. [4]

LA PROTECTION DES DONNEES A CARACTERE PERSONNEL DANS UN CONTEXTE DE RECOURS MASSIF AU TELETRAVAIL ET DE RISQUES ACCRUS DE CYBERATTAQUES

Le recours massif au télétravail dans un contexte de confinement de la population fait peser des risques accrus sur la sécurité des données traitées par les entreprises. La démultiplication des échanges dématérialisés, par messagerie,e-mails et/ou plateformes de video-conférence, est en effet propice à une explosion des cyber-attaques[5] :

- virus informatiques, faux e-mails des autorités de santé, fausses notes internes en entreprise ou encore fausses alertes de retard de livraison ;
- les e-mails de « *phishing* » utilisent de fausses pages d'accueil et demandent aux gens de saisir leur nom d'utilisateur et leur mot de passe ;
- cliquer sur une pièce jointe peut déclencher l'installation d'un logiciel d'exfiltration de données.

Le gouvernement français relève que de nombreuses campagnes de cyberattaques liées à cette crise sont déjà observées dans le monde et alerte sur un accroissement prévisible des cyberattaques et des cyber-escroqueries. Il souligne que pour beaucoup d'entreprises, la mise en place du télétravail a dû se faire dans l'urgence, voire être initiée « à distance » avec des collaborateurs confinés et sans réelle maîtrise des mesures de sécurité à mettre en place. Dans certains cas, et faute d'avoir pu déployer les moyens nécessaires, le télétravail s'opère même depuis les équipements personnels des collaborateurs, dont le niveau de sécurité ne peut pas être évalué et encore moins garanti [6].

[4] https://www.cnil.fr/professionnel
[5] https://www.lesechos.fr/tech-medias/hightech/les-cyberattaques-capitalisent-sur-le-coronavirus-1184259
[6] https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/coronavirus-covid-19-vigilance-cybersecurite

Il est utile de rappeler que les responsables de traitements de données personnelles et leurs sous-traitants sont tenus de mettre en œuvre les « *mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* » (article 32). **Dans un contexte où les ressources informatiques sont focalisées sur la continuité de l'activité, les entreprises sont invitées à ne pas baisser la garde et à redoubler de vigilance sur les questions de sécurité. L'essentiel des sanctions prononcées par la CNIL l'ont d'ailleurs été pour donner suite à des failles de sécurité**. Rappelons-nous que la formation restreinte de la CNIL a prononcé une sanction de 400.000 euros à l'encontre de la société UBER pour avoir insuffisamment sécurisé les données des utilisateurs de son service de VTC.

Les entreprises et leurs salariés peuvent consulter les recommandations de sécurité que l'on peut trouver sur le site de la CNIL https://www.cnil.fr/fr/salaries-en-teletravail-quelles-sont-les-bonnes-pratiques-suivre, le site https://www.cybermalveillance.gouv.fr/, ou encore le site de l'Agence Nationale de Sécurité des Systèmes d'Information https://www.ssi.gouv.fr/. Parmi les recommandations de sécurité :

- se méfier des messages (mail, SMS, chat…) ou appels téléphoniques d'origine inconnue ou inattendus ;
- ne télécharger des applications que depuis les sites ou magasins officiels des éditeurs ;
- vérifier la fiabilité et la réputation des sites visités (vérifier les adresses URL, les certificats de sécurité) ;
- vérifier les liens (passer la souris sur le lien sans cliquer permet d'identifier les adresses URL suspectes : nombreux chiffres…) ;
- être attentif aux fausses commandes ou aux modifications de virements bancaires frauduleux ;
- **faire régulièrement des sauvegardes des données (ordinateurs, téléphone…) et garder en une copie déconnectée** ;
- installer les mises à jour de sécurité sur les équipements connectés (serveurs, ordinateurs, téléphones…) dès qu'elles sont disponibles ;
- utiliser des mots de passe uniques et solides et activer la double authentification chaque fois que possible.

LE TRAITEMENT DES DONNEES DE SANTE LIEES AU COVID19 RELEVE DE LA RESPONSABILITE DES AUTORITES SANITAIRES

Le RGPD définit les données concernant la santé comme « *les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* ». Cette définition est large et inclut donc les informations concernant une maladie ou obtenues lors d'un test.

Dans le cadre des efforts pour endiguer l'épidémie de Covid 19, la CNIL précise que les données de santé peuvent être collectées par les autorités sanitaires, qualifiées pour prendre les mesures adaptées à la situation. **L'évaluation et la collecte des informations relatives aux symptômes du coronavirus et des informations sur les mouvements récents de certaines personnes relèvent de la responsabilité de ces autorités publiques**[7].

Comme les entreprises, les autorités publiques sont tenues de s'appuyer sur une base légale pour que leurs traitements de données à caractère personnel soient licites.

> S'agissant des traitements de données à caractère personnel, hors données de santé, réalisés par les autorités dans le cadre de la crise du Covid19, le Comité Européen de Protection des Données préconise, dans son communiqué du 19 mars 2020, le recours à la base légale de « ***l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement*** » (article 6.1.e du RGPD).
>
> Pour les **traitements de données de santé**, qualifiées de catégorie particulière de données à caractère personnel (article 9 du RGPD), le Comité Européen de Protection des Données recommande de s'appuyer sur la base légale du « ***traitement nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique*** » (article 9.1.i du RGPD) ou sur celle du « *traitement nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement* » (article 9.1.c du RGPD). Dans ce dernier cas, l'article 9 précise que le droit de l'État membre doit prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel.

Il convient enfin de souligner qu'outre le RGPD, les données de santé obéissent à un régime particulier défini dans la loi Informatique et Libertés (art. 8 et chapitre IX), ainsi que dans le Code de la santé publique.

> Les données de santé sont couvertes par le secret (art. L. 1110-4 du Code de la santé publique) et ne sont accessibles qu'aux professionnels et établissements de santé, ainsi qu'aux organismes et institutions visés à l'article L. 1460-1 du Code de la santé, dans les conditions définies par la loi Informatique et Libertés.

[7] https://www.cnil.fr/fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees-personnelles

Des dispositions de sécurité renforcée sont en outre applicables, notamment des référentiels de sécurité et d'interopérabilité des données de santé (art. L. 1110-4-1 du Code de la santé publique), ainsi que des dispositions relatives à leur hébergement (art. L. 1111-8 et R. 1111-8-8 et s. du Code de la santé publique).

Les administrations et services de santés sont d'ailleurs victimes d'une recrudescence de cyberattaques. La cellule d'accompagnement cybersécurité des structures de santé (ACSS) de l'Agence du numérique en santé (ANS) a ainsi publié une alerte indiquant que « le coronavirus est utilisé pour réaliser des cyberattaques »[8].

Les éditeurs d'applications de santé relevant du régime des dispositifs médicaux (article L5211-1 du Code de la santé publique) seront donc particulièrement vigilants sur l'obtention ou le renouvellement des agréments, labels et certifications requises (ex : certification hébergeur de données de santé de l'Agence du Numérique en Santé).

LE TRAITEMENT DE DONNEES DE LOCALISATION COMME STRATEGIE DE CONTROLE DES SORTIES DU CONFINEMENT

Le gouvernement français envisage le traitement de données de localisation. Jusqu'à aujourd'hui, les analyses de données de localisation faites par les autorités françaises et la commission européenne l'ont été à partir de données anonymisées par agrégation, afin d'observer si la population respecte le confinement ou encore de cartographier les concentrations et les mouvements de population. C'est ainsi que les données de localisation conservées par Orange ont permis de constater que 17 % des habitants du Grand Paris avaient quitté la région entre le 13 et le 20 mars[9].

Le gouvernement réfléchit désormais à des scénarii de sortie du confinement incluant un possible traçage numérique des citoyens français, qui pourrait utiliser des données de localisation croisées à des données de santé et non anonymisées. A ce titre, le Comité Analyse, Recherche et Expertise (Care) a été missionné par le Gouvernement le 24 mars dernier. Plusieurs pays européens, dont l'Italie, ont déjà recours massivement à la géolocalisation à des fins notamment de surveillance des citoyens en quarantaine[10].

[8] https://www.cyberveille-sante.gouv.fr/index.php/accueil
[9] https://www.lesechos.fr/tech-medias/hightech/coronavirus-la-geolocalisation-des-telephones-confirme-lexode-de-parisiens-1189565
[10] https://www.lefigaro.fr/international/italie-contre-le-coronavirus-l-utilisation-massive-de-la-geolocalisation

Mercredi 01 avril, le Premier ministre Edouard Philippe a évoqué un possible traçage des citoyens, sur le fondement d'un engagement volontaire (comme l'Allemagne le fait en ce moment en utilisant Bluetooth), pour mieux suivre la circulation du virus et les contacts réalisés par chacun, tout en reconnaissant que la France ne dispose pas encore d'instrument légal pour réaliser un tel traçage. On sait par ailleurs que l'opérateur téléphonique national fournit des données sur le flux de population au prétexte que « avec cette information, les autorités peuvent se préparer à bien dimensionner les services sanitaires » d'après un représentant de l'opérateur téléphonique. Cette démarche serait également initiée au niveau européen à la demande du Commissaire Breton.

Dans ce contexte, l'un des comités scientifiques établis par l'Elysée a été mandaté pour réfléchir à « *l'opportunité de la mise en place d'une stratégie numérique d'identification des personnes ayant été au contact de personnes infectées* ».[11] Interrogée sur la faisabilité juridique du déploiement d'une solution de « *contact tracing* » dans une hypothèse de déconfinement, la présidente de la CNIL, Marie-Laure Denis, a répondu par l'affirmative sous certaines conditions : « *Si nous parlons de suivi individualisé des personnes, il y a deux solutions. La première, c'est que ce suivi repose sur le volontariat, c'est-à-dire le consentement libre et éclairé. Il ne faut pas qu'il y ait des conséquences pour celui qui refuserait de télécharger une application, par exemple (…). Pour le suivi individualisé des personnes qui ne reposerait pas sur le consentement, il faudrait, d'une part, une disposition législative et, d'autre part, que le dispositif soit conforme aux principes de la protection des données.* »[12] En d'autres termes, que ce dispositif repose ou non sur le consentement, il devra respecter les principes élémentaires de protection des données (tes que : la proportionnalité, la durée provisoire de conservation des données, et la sécurité) et intégrer, pour des raisons juridiques mais aussi comme gage de confiance, le droits des personnes à leur vie privée. « *Une application utilisant la technologie Bluetooth, pour détecter si un autre téléphone équipé de cette même application se trouve à proximité immédiate, apporte d'avantage de garanties qu'une application géolocalisant précisément et en continu,* ajoute la présidente de la CNIL. *D'une façon générale, il faut privilégier les solutions qui minimisent la collecte des informations, par exemple en utilisant un identifiant plutôt que des données nominatives. Les solutions doivent aussi privilégier le chiffrement de l'historique de connexion et le stockage des données sur un téléphone, plutôt que de les envoyer systématiquement sur une base centralisée.* »[13]

[11] https://www.lemonde.fr/pixels/article/2020/04/05/coronavirus-les-applications-de-contact-tracing-appellent-a-une-vigilance-particuliere_6035639_4408996.html

[12] https://www.lemonde.fr/pixels/article/2020/04/05/coronavirus-les-applications-de-contact-tracing-appellent-a-une-vigilance-particuliere_6035639_4408996.html

[13] https://www.lemonde.fr/pixels/article/2020/04/05/coronavirus-les-applications-de-contact-tracing-appellent-a-une-vigilance-particuliere_6035639_4408996.html

LES TRAITEMENTS DE DONNEES LIES AUX RECHERCHES PORTANT SUR LE COVID-19

Dans le contexte de la crise sanitaire liée au COVID-19, la CNIL a publié, le 26 mars 2020, sur son site internet, une communication détaillant les formalités à accomplir lorsqu'un responsable de traitement réalise un traitement de données à caractère personnel lié à la recherche sur le COVID-19[14].

Ainsi, selon la CNIL, si le projet de recherche est une recherche interne, aucune formalité n'est requise, si ce n'est d'inscrire le traitement dans le registre des activités de traitement.

Si le projet de recherche n'est pas interne mais est néanmoins conforme aux dispositions d'une des méthodologies de référence homologuées par la CNIL, aujourd'hui au nombre de 6 (Recherches dans le domaine de la santé avec recueil du consentement, Etudes non interventionnelles de performances concernant les dispositifs médicaux de diagnostic in vitro, Recherches dans le domaine de la santé sans recueil du consentement, Recherches n'impliquant pas la personne humaine, Etudes et évaluation dans le domaine de la santé, Etudes nécessitant l'accès aux données du PMSI et/ou des RPU par les établissements de santé et les fédérations hospitalières, Etudes nécessitant l'accès aux données du PMSI par les industriels de santé), le responsable du traitement doit faire une déclaration de conformité à la méthodologie de référence correspondante.

Si le projet de recherche n'est pas conforme aux dispositions d'une méthodologie de référence, le responsable du traitement doit déposer une demande d'autorisation « recherche » et est invité à :

- détailler les points de non-conformité de son projet de traitement à une méthodologie de référence ;
- vérifier que le protocole ou tout document présentant l'étude précise clairement :
    - les destinataires des données directement identifiantes ;
    - la durée de conservation des données à caractère personnel traitées :
- transmettre, en cas d'inclusion en situation d'urgence et en situation d'urgence vitale immédiate :
    - la note d'information de poursuite à destination du patient ;
    - la note d'information de poursuite à destination du proche ou de la personne de confiance

****

[14] https://www.cnil.fr/fr/recherches-sur-le-covid-19-la-cnil-se-mobilise