

Coronavirus et protection des données personnelles : un enjeu mondial

le 1 avril 2020

IP/IT ET COMMUNICATION | Protection des données

Afin de suivre et de limiter la pandémie de covid-19, tant les autorités publiques que les employeurs ont eu besoin de mettre en œuvre de nouveaux traitements de données personnelles, ce qui a conduit les autorités du monde entier à préciser les principes à appliquer dans ce contexte.

Une prise de conscience mondiale

Nombre d'autorités de protection des données ou d'agences gouvernementales ont publié sur leurs sites des recommandations en lien avec la pandémie de covid-19. L'association internationale des professionnels de la protection des données (IAPP) a produit un tableau listant les documents mis en ligne dans plus d'une cinquantaine de pays ([DPA guidance on covid-19](#)).

En Europe, [le 19 mars 2020](#), le Comité européen de la protection des données (CEPD), qui regroupe les autorités de contrôle de l'Union européenne, a rappelé les principes européens de la protection des données dans le contexte du covid-19 (v. [Dalloz actualité, 30 mars 2020, obs. A. Guérin-François](#)). En parallèle, la plupart des autorités nationales ont publié leurs propres recommandations. Certaines avaient devancé le besoin de leurs concitoyens comme le *Garante* italien, [le 3 mars 2020](#), ou la CNIL française, [le 6 mars 2020](#), tandis que d'autres ont souhaité compléter les recommandations du CEPD (par exemple l'Espagne, [le 25 mars 2020](#), ou les Pays-Bas, [le 20 mars 2020](#)).

En dehors des États européens, plus d'une vingtaine de pays dans le monde ont déjà publié des « avis » ou des foires aux questions. Ce besoin de rappeler les bonnes pratiques s'étend du Mexique à la Chine en passant par la Russie, le Pérou, l'Argentine, la Nouvelle-Zélande, la Suisse ou le Canada. En ce qui concerne les États-Unis (le pays n'ayant pas d'autorité fédérale en charge de la protection des données), l'agence fédérale qui administre et applique les lois sur les droits civils contre la discrimination en milieu de travail (EEOC) a, notamment, publié [une foire aux questions sur le thème de l'emploi](#).

Des problématiques communes

Si chaque autorité a formulé ses propres recommandations, on constate leur volonté commune de s'assurer que la protection des données ne soit pas un frein aux traitements de données nécessaires à la lutte contre la pandémie. Les autorités européennes insistent sur le fait que tant le [règlement \(UE\) 2016/679](#) du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD) que la [directive 2002/58/CE](#) du 12 juillet 2002 (directive « vie privée ») offrent assez de souplesse pour mettre en œuvre des traitements liés à la pandémie.

Notons que c'est **la question des traitements des données de santé liées au covid-19 dans les relations de travail** qui prédomine à l'échelle mondiale. En effet, dans le cadre de la propagation du virus, se pose notamment la question de la responsabilité de l'employeur quant à son obligation d'assurer la sécurité de ses collaborateurs. Les « recommandations » des autorités font ainsi écho à des pratiques soudaines, et parfois disproportionnées, souhaitées (ou mises en place) dans certaines organisations, comme les relevés des températures corporelles des salariés ou visiteurs ou des questionnaires médicaux obligatoires.

Les autorités semblent s'accorder sur le fait que les organisations ne doivent pas mettre en place de traitements systématiques et généralisés relatifs aux données de santé de leurs collaborateurs, en dehors de ceux qui leur seraient demandés par les autorités de santé publique. Les traitements mis en œuvre doivent se conformer à la législation nationale applicable, y compris celle qui imposerait de nouvelles obligations dans le cadre de l'urgence sanitaire, et également aux principes de proportionnalité et de transparence.

L'autre problématique majeure posée par le covid-19 concerne **le suivi des personnes par les gouvernements** afin d'endiguer la pandémie, à l'image de ce qui a été mis en œuvre en Corée du Sud ou en Chine. Ce suivi *via* les données GPS des téléphones portables pourrait prendre diverses formes, telles que la détection des sorties du confinement ou le *backtracking*, permettant de tracer les itinéraires d'une personne contaminée afin d'identifier les personnes en contact avec elle. Ces pratiques qui impliquent la réutilisation des données des opérateurs de télécommunication soulèvent de nombreuses inquiétudes en matière de libertés publiques, notamment au regard des risques de détournement d'usage et de pérennisation de telles mesures.

Le Comité européen de la protection des données a abordé cette question dans sa déclaration du 19 mars 2020, en rappelant le cadre légal applicable (v. A. Guérin-François, art. préc.). En ce qui concerne les autorités nationales, leur position officielle dépendra des projets proposés par leur gouvernement. Ainsi, l'autorité de contrôle des institutions européennes (l'EDPS) [a publié la réponse](#) qu'elle a adressée, le 25 mars 2020, à la Commission européenne. Celle-ci l'avait consultée concernant un projet de collecte massive des métadonnées (anonymisées) des opérateurs de télécommunication afin de cartographier les mouvements des personnes dans le cadre de la pandémie actuelle. L'EDPS a ainsi formulé plusieurs recommandations afin de garantir que les données soient réellement anonymisées, sécurisées et supprimées dès la fin de la crise.

Par ailleurs, la CNIL a dû, [le 19 mars 2020](#), rassurer les Français sur la légalité des SMS qu'ils avaient reçus au nom du gouvernement pour annoncer le confinement en expliquant que cette campagne avait pu être réalisée sur le fondement de l'article L. 33-1 du code des postes et des communications électroniques. Quelques jours auparavant, dans un communiqué daté du [12 mars 2020](#), l'autorité britannique, l'ICO, a indiqué de manière plus générale que « les lois sur la protection des données et les communications électroniques n'empêchent pas le gouvernement, le NHS ou tout autre professionnel de la santé d'envoyer des messages de santé publique aux personnes, par téléphone, SMS ou e-mail, car ces messages ne sont pas du marketing direct ».

D'autres thèmes périphériques sont également abordés par les autorités, tels que les mesures de sécurité liées au télétravail (par ex. au [Danemark](#)), la collecte de données de santé par les établissements de santé (par ex. en [Slovénie](#)) ou la difficulté, en cette période d'activité perturbée, de respecter les délais de réponse lorsque des personnes exercent leurs droits tels que le droit d'accès ou d'effacement (par ex. en [Irlande](#)).

On notera également les questions liées à la sécurité et à la confidentialité des données de santé dans le cadre de la télémédecine. Ainsi, le département de la santé américain (HHS) en charge de faire respecter la législation américaine spécifique aux données de santé (HIPPA) [a déclaré qu'il serait clément avec les professionnels de santé utilisant des applications populaires de communication](#).

Pour la France, les traitements liés à la recherche étant soumis à une autorisation de la CNIL, celle-ci a rappelé [le 26 mars 2020](#) le régime juridique applicable et s'est engagée à traiter les dossiers qui lui seraient adressés de manière extrêmement courte *via* une adresse e-mail dédiée.

En conclusion, les autorités de contrôle, en particulier européennes, veulent faire preuve de pragmatisme dans leur application des législations en vigueur tout en préservant les principes fondamentaux de la protection des données personnelles et les libertés publiques.

par Alexandra Guérin-François

