

Déclaration conjointe
sur le droit à la protection de données dans le contexte de la pandémie à
COVID-19

par Alessandra Pierucci, Présidente du Comité de la Convention 108

et

Jean-Philippe Walter, Commissaire à la protection des données du
Conseil de l'Europe

Strasbourg, le 30 mars 2020

La pandémie COVID-19 (plus connue sous le nom de Coronavirus) crée des menaces et des défis sans précédent pour les personnes et les pays du monde entier. La nécessité d'arrêter sa propagation et de soigner ceux qui souffrent est un objectif majeur partagé par toutes les nations.

Les efforts déployés par l'Organisation mondiale de la santé, d'autres organisations internationales, les gouvernements, les établissements de soins de santé et leur personnel ainsi que les entreprises pour empêcher une propagation du virus à plus grande échelle encore, pour sauver des vies et protéger la société sont illimités et doivent être fortement soutenus.

Les États doivent faire face à la menace que fait peser la pandémie COVID-19 tout en veillant au respect de la démocratie, de l'État de droit et des droits de l'homme, y compris des droits au respect de la vie privée et à la protection des données.

Dans les efforts déployés afin de réduire le nombre de nouvelles contaminations, les gouvernements ont dû recourir à des mesures extraordinaires, y compris déclarer dans de nombreux cas l'état d'urgence. Si la situation alarmante en matière de santé publique de ces pays a justifié la mise en place de régimes spécifiques, il convient de souligner que, pendant ces périodes limitées, l'exercice des droits de l'homme tels qu'ils sont consacrés par plusieurs instruments nationaux et internationaux (tels que le Pacte international relatif aux droits civils et politiques et la Convention européenne des droits de l'homme) est applicable et ne peut être suspendu ; on peut seulement y déroger ou le limiter en vertu de la loi, dans la stricte mesure où la situation l'exige, tout en respectant l'essence des droits et libertés fondamentales.

Principes généraux et règles de protection des données

En ce qui concerne le droit à la protection des données, il convient tout d'abord de noter que la Convention 108, ainsi que la "[Convention 108+](#)" modernisée, énoncent des normes élevées pour la protection des données à caractère personnel qui sont compatibles et conciliables avec d'autres droits fondamentaux et intérêts publics pertinents.

Il est important de rappeler que la protection des données ne peut en aucun cas constituer une entrave au fait de sauver des vies et que les principes applicables permettent toujours de trouver le juste équilibre entre les intérêts en présence.

Conformément à la Convention 108+, il est essentiel que, même dans des situations particulièrement difficiles, les principes de protection des données soient respectés et qu'il soit donc garanti que les personnes concernées soient tenues informées du traitement des données personnelles qui les concernent, que le traitement des données personnelles ne soit effectué que s'il est nécessaire et proportionné à la finalité explicite, déterminée et légitime poursuivie, qu'une analyse d'impact soit effectuée avant le début du traitement, que le respect des principes soit assuré dès la conception (« *privacy by design* ») et que des mesures appropriées soient adoptées pour assurer la sécurité des données, en particulier lorsqu'elles concernent des catégories particulières de données telles que les données relatives à la santé, enfin, que les personnes concernées soient habilitées à exercer leurs droits.

L'un des principaux principes de protection des données prévu par la Convention 108+ est celui de la licéité, selon lequel le traitement des données peut être effectué soit sur la base du consentement de la personne concernée, soit sur la base d'un autre fondement légitime prévu par la loi. Il convient de noter que, comme le prévoit explicitement le [rapport explicatif](#) de la Convention 108+, cette base légitime peut notamment comprendre le traitement de données nécessaire aux intérêts vitaux des personnes et celui effectué sur la base de motifs d'intérêt public, comme dans le cas de la surveillance d'une épidémie mortelle.

Ainsi, le droit à la protection des données, n'empêche par exemple pas les autorités de santé publique de partager la liste des professionnels de la santé (noms et coordonnées) avec les entités chargées de la distribution de masques FFP2. Pas plus qu'on ne peut prétendre que le droit à la protection des données est incompatible avec la surveillance épidémiologique, les données anonymisées n'étant pas couvertes par les exigences de la protection des données. L'utilisation d'informations de localisation agrégées pour signaler des rassemblements enfreignant les règles de confinement ou pour indiquer des mouvements de personnes s'éloignant d'une zone gravement touchée (en termes de nombre de personnes positives COVID-19) ne serait donc pas empêchée par les exigences de protection des données.

En outre, la Convention 108+ reconnaît la nécessité d'autoriser certaines exceptions et restrictions au nom d'objectifs impérieux d'intérêt public et des intérêts vitaux des personnes. Néanmoins, les restrictions à ses principes et droits doivent répondre à des exigences très claires, même pendant l'état d'urgence, pour garantir le respect persistant de l'État de droit et des droits fondamentaux.

Selon la Convention 108+ (voir article 11), une exception est admise dès lors qu'elle est « *prévue par une loi, qu'elle respecte l'essence des droits et libertés fondamentales, et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique* ».

Lorsque des restrictions sont appliquées, ces mesures doivent être prises à titre provisoire uniquement et pour une période explicitement limitée à l'état d'urgence. Il est également essentiel que des garanties spécifiques soient mises en place et que des assurances soient données quant à la pleine protection des droits et libertés individuelles une fois l'état d'urgence levé. Cela devrait inclure des mesures et des procédures concrètes concernant le retour à des régimes de traitement des données "normaux", avec une attention particulière aux bases de données contenant des données relatives à la santé ou d'autres catégories spéciales de données et/ou à celles créées dans le but de suivre, de traquer et de profiler les personnes dont le traitement a été effectué pendant l'état d'urgence.

Les autorités de protection des données sont invitées à évaluer soigneusement les mesures prises par les autorités nationales au regard de ces conditions.

Traitement des données relatives à la santé

La primauté de l'être humain et l'adoption de normes professionnelles devant prévaloir en matière de soins santé, le traitement des données relatives à la santé doit garantir le respect des droits et des libertés fondamentales de chaque personne, notamment le droit au respect de la vie privée et à la protection des données à caractère personnel. La recommandation [CM/Rec\(2019\)2](#) relative aux données relatives à la santé fournit des lignes directrices spécifiques à cet égard. Ses dispositions portant sur le partage des données entre les professionnels de la santé et entre le secteur de la santé et d'autres secteurs devraient notamment guider les pratiques des professionnels concernés. Un chapitre spécifique de la Recommandation est consacré à la recherche scientifique qui est actuellement l'un des domaines les plus cruciaux de la coopération internationale dans la lutte contre le COVID-19.

La communication au public par les autorités sanitaires et gouvernementales devrait rester une priorité pour être en mesure de protéger, d'informer et de conseiller le public. Néanmoins, lors de ces communications, la publication de données sensibles (telles que les données relatives à la santé) concernant des personnes spécifiques devrait être évitée et il est recommandé que le traitement de ces données ne soit effectué que si des mesures techniques et organisationnelles supplémentaires complétant celles appliquées aux données qui ne revêtent pas une nature sensible sont mises en place.

Traitement des données à grande échelle

Étant donné que de vastes quantités de données et de bases de données sont générées, au moyen des potentialités offertes par les techniques et technologies de traitement des données telles que les mégadonnées (*Big Data*) ou l'intelligence artificielle, ces données devraient être traitées dans ces environnements d'une manière qui respecte la dignité humaine et la protection des données.

Les orientations développées par le Comité de la Convention 108 dans le contexte des [mégadonnées](#) (*Big Data*) et de [l'intelligence artificielle](#) peuvent être des outils utiles pour les développeurs ainsi que pour les gouvernements afin de façonner ces traitements de manière à éviter les abus volontaires ou les conséquences négatives fortuites, y compris la discrimination de personnes ou de groupes.

La transparence et « l'explicabilité » des solutions d'analyse ou de l'IA, une approche de précaution et une stratégie de gestion des risques (y compris le risque de ré-identification dans le cas de données anonymes), l'accent mis sur la qualité et la minimisation des données, et le rôle du contrôle réalisé par un être humain personne sont parmi les points clés à prendre en compte dans le développement de solutions innovantes pour lutter contre le COVID-19.

Traitement des données par les employeurs

Les employeurs éprouvent des difficultés à maintenir leur entreprise ou leur activité tout en protégeant le public et leur personnel, très souvent en faisant travailler leurs employés à distance. Cette pratique ne doit cependant pas conduire à la surveillance des employés, y compris par des moyens vidéo ; des mesures non intrusives doivent être pensées lors de l'organisation du travail et de leurs conditions.

Dans les circonstances actuelles, les employeurs peuvent être amenés à traiter des données personnelles ou sensibles qu'ils ne traitent généralement pas (comme celles relatives à la santé) ; il convient donc de rappeler que, ce faisant, ils doivent respecter les principes de nécessité, de proportionnalité et de responsabilité et doivent également être guidés par des principes visant à minimiser les risques que ce traitement pourrait faire peser sur les droits et les libertés fondamentales des salariés, en particulier leur droit au respect de la vie privée tel qu'il est développé dans la Recommandation [CM/Rec\(2015\)5](#) sur le traitement des données à caractère personnel dans le cadre de l'emploi. En particulier, les employeurs ne devraient pas traiter les données personnelles au-delà de ce qui est nécessaire à l'identification des employés potentiellement exposés.

S'ils sont tenus par la loi de divulguer certaines données aux autorités publiques pour des raisons de santé publique, ils sont invités à le faire dans le strict respect de la base juridique pertinente et de prendre les mesures nécessaires pour revenir à un traitement "normal" (y compris l'effacement définitif) lorsque le régime d'état d'urgence ne sera plus en vigueur.

Données mobiles numériques

Les entreprises de télécommunications, les plateformes en ligne et les fournisseurs de services internet participent également activement à la lutte contre la propagation du COVID-19 et sont de plus en plus tenus de partager avec les autorités publiques les données des abonnés, les informations personnelles qu'elles recueillent et d'autres types d'informations, afin de contribuer notamment à la surveillance épidémiologique, y compris l'analyse des données pour déterminer la localisation des personnes potentiellement infectées.

De même, les organismes privés et publics peuvent développer des solutions informatiques pour la surveillance de l'épidémie.

Le traitement à grande échelle des données à caractère personnel ne peut être effectué que lorsque, sur la base de preuves scientifiques, les avantages potentiels pour la santé publique d'une telle surveillance numérique des épidémies (par exemple, le suivi des contacts), y compris leur exactitude, l'emportent sur les avantages d'autres solutions alternatives qui seraient moins intrusives.

L'élaboration de ces solutions de surveillance doit être fondée sur une évaluation préalable de l'impact potentiel du traitement de données envisagé sur les droits et libertés fondamentales des personnes concernées, et doit concevoir le traitement de données de manière à prévenir ou à minimiser le risque d'interférence avec ces droits et libertés fondamentales.

À la lumière des principes de précaution et de proportionnalité, des tests préalables dans différents « *sandboxes* » devraient également être recommandés, comme c'est actuellement le cas pour divers médicaments testés dans le cadre d'essais cliniques.

Si des informations en temps réel sur la propagation du virus peuvent contribuer à l'isoler, il convient de souligner que les solutions les moins intrusives doivent toujours être privilégiées.

Le traitement des données dans les systèmes éducatifs

Les écoles et les universités déploient tous les efforts possibles pour accroître les compétences et les ressources en matière d'enseignement à distance, les professeurs et les enseignants étant eux-mêmes confrontés au défi de l'isolement. Lors de l'examen de solutions techniques pour assurer la continuité du travail éducatif, il convient de privilégier des configurations standard axées sur la protection des données, par exemple en ce qui concerne les paramètres par défaut (« *privacy by default* »), afin que l'utilisation des applications et des logiciels ne porte pas atteinte aux droits des personnes concernées et d'éviter de traiter plus de données que nécessaire pour atteindre le but légitime de continuité de l'enseignement.

Il est également primordial de choisir une base légale appropriée (y compris l'accord des parents ou du tuteur légal si nécessaire) et de veiller à ce que les parents bénéficient d'un maximum de transparence en ce qui concerne le traitement des données de leurs enfants.

Des lignes directrices¹ supplémentaires concernant le traitement des données à caractère personnel dans le contexte de l'éducation sont en cours d'élaboration par le Comité de la Convention 108 et serviront aux praticiens et aux décideurs.

Alors que nous traversons une période difficile et menaçante, alors que la situation évolue rapidement et que les gouvernements prennent des mesures pour les protéger, ils doivent le faire sans exposer les sociétés à des risques plus importants encore à l'avenir.

¹ [Projet de Lignes directrices : La protection des données personnelles des enfants dans les systèmes éducatifs:enjeux et solutions possibles](#)

Ce n'est qu'en étant unis et solidaires, dans le plein respect de l'État de droit, des droits de l'homme et de la démocratie, que nous parviendrons à surmonter cette situation sans précédent.