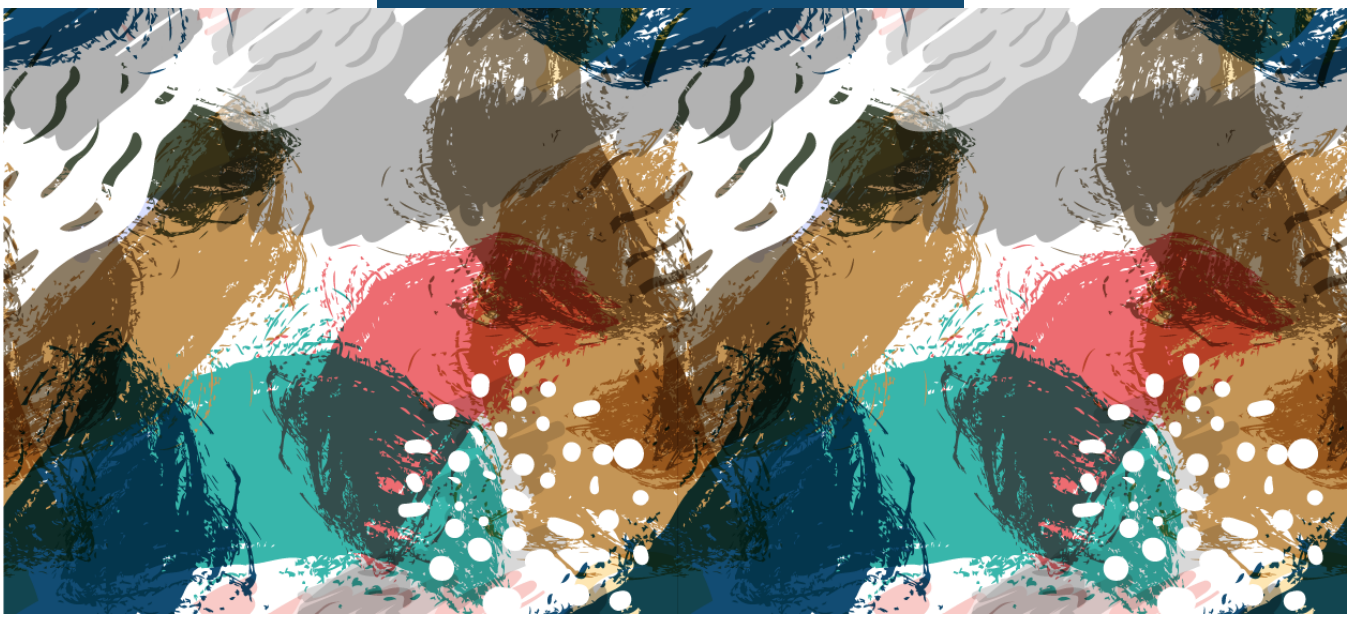


CRISE SANITAIRE LIEE AU COVID-19 ET PROTECTION DES DONNEES PERSONNELLES, PRENONS LE TEMPS DE LA REFLEXION

Livre Blanc

15 avril 2020

DS AVOCATS

SOMMAIRE

****

Les crises conduisent souvent à relativiser de nombreux impératifs qui, en temps normal, s'imposent sans grande difficulté. Elles poussent aussi, systématiquement, à raisonner en termes de circonstances exceptionnelles, de suspension des règles, et de procédures accélérées – parfois expéditives. Or, c'est précisément en temps de crise que les organisations doivent savoir distinguer l'essentiel de l'accessoire, et faire en sorte de protéger les règles fondamentales plutôt que les abolir plus ou moins durablement.

La pandémie du coronavirus 2019 (dite « covid-19 »), et l'actuelle crise sanitaire, amènent fort logiquement les entreprises et les états, à s'interroger sur la permanence des règles de droit commun. Et en l'espèce, à s'interroger sur la pertinence, voire la compatibilité, du RGPD avec les circonstances exceptionnelles actuelles. Les autorités peuvent avoir une tendance inquiétante à s'affranchir de certaines règles établies pour donner force à la protection des droits et libertés fondamentales ; les entreprises peuvent logiquement trouver fastidieuses et inappropriées les exigences procédurales et organisationnelles que le RGPD les amène à déployer depuis bientôt deux ans.

Or, c'est sans doute en temps de crise qu'il est encore plus crucial de protéger et respecter les libertés fondamentales. Et la protection des données personnelles en relève assurément : le RGPD est lié à la charte européenne des droits fondamentaux, et depuis 1978, la loi française rappelle que les données sont une émanation de la personne, et que leur protection constitue donc une question de libertés publiques.

La question se pose donc de savoir comment s'applique la protection des données à caractère personnel, et en particulier les règles du RGPD que beaucoup d'entreprise étaient encore en train de concevoir et de déployer, dans le contexte exceptionnel actuel. En France, le Parlement a adopté la loi n°2020-290 du 23 mars 2020 « d'urgence pour faire face à l'épidémie de covid-19 », qui aménage un certain nombre de règles de droit commun en fonction des impératifs sanitaires, et du confinement en place depuis fin mars. Mais cette loi n'a pas spécifiquement évoqué la protection des données personnelles, et en particulier des **données personnelles de santé**, de sorte que la plupart des entreprises et administrations s'interrogent sur son application actuelle – ou ne s'interrogent pas, ce qui est pire.

Rappelons à titre liminaire que contrairement à ce que certains ont cru pouvoir dire, le RGPD n'est nullement incompatible avec la situation actuelle. Son considérant 52 mérite à cet égard d'être intégralement cité : « *Des dérogations à l'interdiction de traiter des catégories particulières de données à caractère personnel devraient également être autorisées lorsque le droit de l'Union ou le droit d'un État membre le prévoit, et sous réserve de garanties appropriées, de manière à protéger les données à caractère personnel et d'autres droits fondamentaux, lorsque* ***l'intérêt public*** *le commande, notamment le traitement des données à caractère personnel dans le domaine du droit du travail et du droit de la protection sociale, y compris les retraites, et à* ***des fins de sécurité, de surveillance et d'alerte sanitaire, de prévention ou de contrôle de maladies transmissibles*** *et d'autres menaces graves pour la santé. Ces dérogations sont possibles à des fins de santé, en ce compris la santé publique et la gestion des services de soins de santé, en particulier pour assurer la qualité et l'efficience des procédures de règlement des demandes de prestations et de services dans le régime d'assurance-maladie, ou à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques. Une dérogation devrait, en outre, permettre le traitement de ces données à caractère personnel, si cela est nécessaire aux fins de la constatation, de l'exercice ou de la défense d'un droit en justice, que ce soit dans le cadre d'une procédure judiciaire, administrative ou extrajudiciaire* ».

De manière classique, il suffit de s'interroger sur la ou les base(s) légale(s) qui, en ces temps exceptionnels, permettraient de traiter des données personnelles de santé. Les concepts du RGPD sont donc parfaitement opérationnels, et il convient de déterminer qui (quels responsables de traitement) peuvent collecter quelles données (données de santé, données de géolocalisation…), pour quelle finalité (prévention / suivi de la pandémie) pendant combien de temps et avec quels moyens. Les réponses diffèrent bien entendu selon les responsables de traitement (entreprises, associations, collectivités territoriales, Etat, autorités sanitaires…) et les catégories de personnes concernées (salariés, clients, patients…).

Qu'en est-il à ce jour, 13 avril 2020, pour les entreprises (I), et plus généralement pour la population (II) ?

La question se pose d'une part au niveau des entreprises, dont les activités sont très fortement impactées par la pandémie comme le confinement, et qui doivent se réorganiser et mettre en œuvre des traitements complémentaires, d'une part, et au niveau des autorités, qui sont amenées à procéder à des collectes massives dans le cadre de la réponse sanitaire à apporter.

1. La protection des données personnelles dans et par l'entreprise

1.1 La protection des données personnelles des salariés de l'entreprise

Très rapidement, la CNIL a rappelé aux responsables de traitement (entreprises et administrations) ce qu'il leur était possible de faire avec les données personnelles de santé, puisqu'elles sont évidemment convoquées dès qu'un individu est suspecté d'infection à la covid-19.

En effet les entreprises, soucieuses de mettre en place des dispositifs destinés à éviter la contamination de leurs équipes ainsi qu'à suppléer les arrêts maladies et quarantaines, se sont demandées dans quelle mesure elles pouvaient collecter des informations révélatrices de l'état de santé de leurs salariés, données qui sont en principe interdites de collecte sans une justification conforme aux cas prévus par l'article 9 du RGPD.

Les entreprises ne sont pas garantes de l'intérêt général, mais peuvent participer à sa sauvegarde. Elles ne peuvent cependant en aucun cas de substituer aux autorités, et en particulier aux autorités sanitaires. La CNIL a indiqué que les employeurs ne pouvaient pas collecter des données et mettre en place des traitements qui iraient au-delà de la *gestion des suspicions d'exposition au virus*. Reste à définir ce qu'on entend par « *gestion des suspicions* ».

L'employeur doit inciter le salarié à déclarer l'éventuelle suspicion qui le concerne, afin de prendre conséquemment les mesures que la loi l'oblige à prendre en vertu de son devoir de protéger la santé et de la sécurité des salariés « *conformément au Code du travail et aux textes régissant la fonction publique (particulièrement l'article L. 4121-1 du Code du travail)* », mais il ne peut pas contraindre ses personnels à divulguer leur état de santé – ou celui de leurs proches !

L'employeur doit à ce titre mettre en œuvre des actions de prévention des risques professionnels, des actions d'information et de formation, et enfin mettre en place une organisation et des moyens adaptés en fonction des signalements qu'il reçoit, et non pas en fonction d'un recensement auquel il procéderait d'autorité.

La CNIL l'autorise à « *mettre en œuvre des actions de prévention des risques professionnels, des actions d'information et de formation, et enfin mettre en place une organisation et des moyens adaptés* », dont le fait de « *sensibiliser et inviter ses employés à effectuer des remontées individuelles d'information les concernant en lien avec une éventuelle exposition* ».

On sait également ce que les entreprises ne peuvent pas faire : il n'est pas possible de mettre en œuvre, par exemple, des relevés obligatoires des températures corporelles des employés (ou des visiteurs de l'entreprise) et de les adresser quotidiennement à la hiérarchie, non plus que de diffuser des questionnaires médicaux auprès de l'ensemble des employés ou procéder à un relevé de leurs symptômes éventuels.

Plus généralement, il n'est pas possible d'organiser la collecte de données de santé, liées à la contamination à la covid-19, autrement que sur la base de l'initiative du salarié lui-même.

C'est donc en cas de signalement qu'on peut collecter les données personnelles de santé (dont la suspicion de contamination au coronavirus). La CNIL écrit que « *En cas de signalement, un*

employeur peut consigner (i) la date et l'identité de la personne suspectée d'avoir été exposée ; (ii) les mesures organisationnelles prises ».

Il est recommandé aux employeurs de ne répertorier qu'une information liée à une « suspicion Covid-19 » plutôt que de collecter des symptômes ou, a fortiori, des diagnostics, même si les employés ont spontanément communiqué plus d'informations.

On doit en effet respecter le principe de minimisation. La CNIL indique que l'objectif poursuivi par la collecte d'informations sur la contamination de ses salariés doit lui permettre de « *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* » : il n'est pas besoin de collecter d'autres données que celles strictement nécessaires à cette finalité.

Au-delà, l'employeur peut naturellement collecter les absences, afin d'organiser sa production et les éventuels remplacements, mais là encore sans faire un état exagéré de données de santé ; le constat objectif de l'arrêt maladie du salarié, l'information sur sa mise en quarantaine, suffisent pour réorganiser la production, identifier des remplaçants, ou communiquer auprès des clients.

Ainsi, parmi ces réorganisations, les finalités autorisant à tenir compte d'une « suspicion covid-19 » peuvent être liées à la nécessité de « *sensibiliser et inviter ses employés à effectuer des remontées individuelles d'information les concernant en lien avec une éventuelle exposition, auprès de lui ou des autorités sanitaires compétentes ; faciliter leur transmission par la mise en place, au besoin, de canaux dédiés ; favoriser les modes de travail à distance et encourager le recours à la médecine du travail* » ou encore « *établir un plan de continuité de l'activité, qui a pour objectif de maintenir l'activité essentielle de l'organisation* ».

En clair, il n'est pas question de permettre aux entreprises (ou administrations non sanitaires) de tenir un « fichier des malades ».

C'est à la personne concernée, le salarié ici, de prendre ses responsabilités et d'informer son employeur de la possibilité qu'il soit contaminé : « *Chaque employé/agent doit pour sa part mettre en œuvre tous les moyens afin de préserver la santé et la sécurité d'autrui et de lui-même (article L.4122-1 du Code du travail) : il doit informer son employeur en cas de suspicion de contact avec le virus*. »

L'entreprise ne peut donc que recenser les salariés qui indiquent être contaminés ou avoir été exposés à la covid-19, sur la base de *l'intérêt légitime* de l'employeur et donc sans consentement des salariés, en n'enregistrant que (i) l'identité des salariés, (ii) la suspicion de contamination et (iii) la date à laquelle l'employeur est informé, ainsi que (iv) l'éventuel arrêt maladie qui en découle.

Ce fichier ne peut ensuite être utilisé qu'aux seules fins de prévenir la propagation du virus dans l'entreprise et de réorganiser sa production, et le cas échéant de communiquer ces informations aux autorités sanitaires si celles-ci contactent l'entreprise, dans le cadre de l'intérêt général.

Enfin, ce fichier n'est accessible qu'aux personnes ayant à en connaître dans l'entreprise, c'est-à-dire celles (i) en charge de la protection de la santé des salariés et (ii) en charge de l'organisation de la production dans ce contexte de crise.

En synthèse, les entreprises doivent :

- Limiter strictement toute collecte de donnée en lien indirect avec la santé de leurs salariés au strict nécessaire dans le cadre de la réorganisation de la production, en incitant les salariés à les déclarer, sans les interroger ni les contraindre à cet égard ;
- Informer ces salariés sur tout traitement de leurs données mis en œuvre en raison de l'épidémie de covid-19, ainsi que des finalités poursuivies ;
- Mettre en œuvre des mesures organisationnelles et techniques nécessaires sécurité adaptées pour protéger les données personnelles collectées ;
- Ne transmettre les données de santé des salariés qu'aux seules autorités sanitaires et à la seule demande de celles-ci ;
- S'abstenir absolument de communiquer auprès de leurs salariés en identifiant les salariés malades, seuls les personnels liés à l'organisation technique de la production et à la médecine du travail étant habilités à traiter ces informations ;
- Prévoir une durée limitée pour la conservation de ces données, conservation qui ne saurait aller au-delà de l'indisponibilité du salarié, et au maximum jusqu'au terme de la crise sanitaire.

1.2 La protection des données personnelles des clients de l'entreprise

Ces premières limitations à ce que peuvent faire les entreprises ayant été rappelées, dès le début du mois de mars, compte tenu du caractère sensible des données de santé *même en période de crise sanitaire*, on doit souligner que la réorganisation des entreprises a également un impact sur l'utilisation des données personnelles de leurs clients : les moyens de production usuels sont battus en brèche, et les organisations recourent massivement aux réseaux pour continuer leurs activités, pour toutes celles qui peuvent être exécutées à distance.

Parmi les mesures palliatives mises en place figure bien entendu le **télétravail**. Au nombre des mesures techniques et organisationnelles que les entreprises doivent déployer, au regard non seulement de la nature des données traitées, mais aussi des circonstances, figure donc logiquement la sécurisation des connexions distantes.

Or, la situation exceptionnelle amène de nombreux salariés à utiliser des outils qui n'ont pas été mis à disposition par leurs employeurs, ou qui ne bénéficient pas des mesures de sécurité normalement déployées. Si les entreprises qui ont déjà réglementé le BYOD (utilisation des outils personnels à des fins professionnelles) et les connexions distantes (intranet sécurisé ou VPN), peuvent mettre en œuvre les règles qu'elles ont déjà encadré dans leurs charte informatiques, de nombreuses autres se sont retrouvées prises au dépourvu par le confinement, et ont demandé à leurs personnels, autant que possible, de recourir à leurs propres outils, ordinateurs et réseaux.

La CNIL a émis un certain nombre de recommandations, y compris vers les salariés eux-mêmes (*sécuriser sa propre connexion, créer des comptes spécifiques sur les webmails et applications utilisées pour travailler, sécuriser son propre PC contre les risques d'intrusion, chiffrer son accès internet avec des clés renforcées de type WPA2 ou WPA3, supprimer les accès wifi invités, s'assurer de la présence d'un pare-feu et d'un antivirus sur les outils personnels, renforcer ses mots de passe, etc.*), ce ne sont toutefois que des pis-aller.

Les services sécurité des entreprises tentent de réduire les risques, mais il est certain qu'ils ne peuvent pas assurer la sécurité d'un réseau informatique qui devient par définition hétéroclite et externalisé. Il est donc indéniable que les risques de violations de données personnelles, par fuite ou perte, se sont accrus d'un coup.

Un serveur distant indisponible, la panne d'un PC personnel, la destruction d'une sauvegarde, constituent des violations de données personnelles que le responsable de traitement reste devoir identifier et signaler, conformément aux exigences du RGPD. Pour couronner le tout, le piratage informatique profite bien entendu de la crise pour tenter de tromper la vigilance des opérationnels et la recrudescence de tentatives de phishing a été constatée…

Les organisations devraient donc également déployer une **information circonstanciée** auprès de leurs salariés, comparables aux chartes informatiques, mais axées sur l'essentiel et tenant compte du travail à distance et du recours bien plus large à des outils personnels qu'à l'habitude.

Les employeurs doivent pour beaucoup déployer des « **plans de continuité d'activité** » qui exposent l'ensemble des mesures, dont la sécurité, déployées pour permettre la poursuite de la production malgré les circonstances exceptionnelles. Ces PCA sont très orientés vers les modalités de sécurisation des outils et connexions distantes, mais devraient également être

accompagnées de l'information nécessaire sur la protection des données personnelles. Or, trop peu de PCA incluent déjà ces considérations. Pourtant, la mise en œuvre des PCA implique souvent de recourir à des technologies et traitements de secours qui vont permettre de traiter ou transférer des données personnelles, et là encore, rien ne vient exonérer les responsables de traitement de leur obligation d'information des personnes concernées.

De même, le contrôle de la sécurité des données implique non seulement les services dédiés de l'entreprise, mais également l'ensemble du personnel. A cet égard, les salariés doivent **signaler à leurs employeurs**, responsables de traitement, toute fuite de données qu'ils constateraient, ou dont ils seraient malheureusement à l'origine malgré eux, par erreur de manipulation.

Les responsables de traitement ne sont pas exonérés de leurs obligations de remédiation et de notification des fuites de données personnelles, malgré la situation actuelle. Toute faille doit donc être scrupuleusement remontée, et l'entreprise doit maintenir l'exécution de ses procédures d'instruction et de notification des violations de données, auprès de la CNIL, voire auprès des personnes concernées.

La CNIL a émis une liste de bonnes pratiques et de réflexes à adopter, que les entreprises doivent relayer, et adapter à la réalité de leurs pratiques de travail actuelles. Une page est spécifiquement consacrée au télétravail.

Le recours aux applications de **visioconférences**, en particulier, pose question. Très prisées par leur caractère convivial, et en raison des options de travail collaboratif qu'elles permettent en temps réel, certaines constituent cependant de vraies menaces sur la protection des données personnelles. L'ANSSI a certifié l'une d'elles, qu'elle recommande aux administrations. D'autres sont proposées par des fournisseurs qu'on sait largement sensibilisés aux exigences du RGPD. Mais certaines ont rapidement posé problème (failles de sécurité, data leaks…).

En synthèse, les entreprises doivent :

- Mettre en place des mesures alternatives dûment sécurisées et encadrées, dans le cadre de « plans de continuation d'activité » ou en tous cas en recourant à des technologies réellement sécurisées et structurellement protectrices des données personnelles (des salariés, des clients, des prospects, des fournisseurs…) ;
- Recourir à des VPN pour les liaisons distantes ;
- Informer les salariés des technologies alternatives mises en place et des données ainsi collectées sur les activités desdits salariés (notamment dans le cadre des applications de télétravail et de visioconférence) ;
- Mettre en œuvre des mesures techniques et organisationnelles nécessaires, y compris de sécurité, adaptées pour protéger les données personnelles traitées, y compris via les outils personnels des salariés le cas échéant ;
- Rappeler aux salariés leur obligation de signaler toute violation de données qu'ils constateraient, ou qu'ils provoqueraient accidentellement, et procéder aux notifications requises par le RGPD le cas échéant.

Au-delà de ces premières mesures prophylactiques, la CNIL comme le CEPD ont rappelé qu'en aucun cas la pandémie de covid-19 n'était de nature à justifier la suspension ou le non-respect du RGPD. Les précautions énumérées ci-avant visent à adapter son application aux circonstances exceptionnelles, en limitant ce qu'il est possible de collecter et en adaptant les traitements effectués à distance. Mais les responsables de traitement demeurent intégralement soumis au RGPD, et il n'est nul état d'urgence ou circonstance exceptionnelle qui justifierait ici de faire entorse à cette réglementation.

Et pourtant, la question est également posée au niveau de la riposte organisée par les autorités publiques. On quitte ici le domaine de ce qui s'impose aux entreprises pour protéger les données personnelles de leurs salariés et leurs clients, pour aborder le domaine de ce que les autorités publiques doivent faire pour respecter la protection des données personnelles des citoyens.

2. La protection des données personnelles par les autorités publiques

2.1 Des collectes classiques par les autorités sanitaires…

La question se pose de savoir si les autorités, qui affrontent la situation d'une façon que le présent article n'a pas vocation à qualifier, sauront également respecter la protection des données personnelles des individus, et plus largement les libertés publiques. Les interactions entre droits fondamentaux et états d'exception font l'objet d'une littérature déjà ancienne, tant juridique que philosophique, mais les progrès technologiques invitent à penser ces interactions à nouveaux frais.

En effet, désormais on songe à lutter contre la pandémie en recourant à des moyens de surveillance numérique qui n'existaient pas encore il y a peu : collecte de données biométriques comme la température corporelle, collecte de la géolocalisation des individus, tracking des interactions sociales, figurent aujourd'hui dans la palette des outils que d'aucuns imaginent mettre en œuvre, parfois avec les meilleures intentions du monde, mais sans toujours bien penser aux effets pervers.

L'Etat et les agences régionales de santé peuvent et doivent, dans le cadre de la protection de l'intérêt général et de leurs missions d'intérêt public, collecter toutes informations utiles et pertinentes pour prévenir, juguler la contamination, et surtout soigner les personnes infectées.

Or, si les soins mis en œuvre dans les établissements de santé (publics et privés) reposent sur les fondements usuels liés à la sauvegarde des intérêts vitaux des personnes et plus généralement à l'exercice de la médecine, il apparaît que d'autres autorités (Etat, ARS, voire autorités de police ?) peuvent également être amenées à collecter des données de santé dans le contexte actuel ; la question se pose de définir la **base légale** qui les y autorise.

Certes, le traitement et la collecte des données personnelles de la population est permis, pour les autorités compétentes, en se fondant sur *l'intérêt général*, l'une des bases légales listées à l'article 6 du RGPD qui permet de se passer du consentement individuel des personnes concernées. Combattre la pandémie et prévenir les contaminations relève à l'évidence de cet intérêt général.

Mais le recours à cette base légale n'est pas dispensé du respect des principes de minimisation, de proportionnalité ou encore de privacy by design. Et en la matière, un équilibre doit nécessairement être trouvé entre la protection de la vie privée des individus – y compris leurs **données de santé** et donc leur éventuelle infection par la covid-19, d'une part, et l'intérêt général d'autre part.

A cet égard, l'Agence nationale de la santé publique française, Santé Publique France, a pour mission l'observation et la surveillance épidémiologique pour approfondir sa connaissance de l'état de santé de la population afin de mettre en place les politiques de santé les plus adaptées aux besoins, aux problèmes de santé, et pour faire face aux situations sanitaires exceptionnelles comme celle à laquelle nous sommes aujourd'hui confrontés.

Celle-ci indique que les données collectées à cet effet ne peuvent être conservées par les autorités que *pour la seule durée des investigations nécessaires à la maîtrise de la pandémie*, après quoi elles devront être détruites ou anonymisées définitivement. Cette collecte est en

effet uniquement liée à la finalité de suivi et de maîtrise de la pandémie, par élaboration des statistiques de propagation notamment.

2.2 …Aux collectes « innovantes »

Mais actuellement, le débat porte sur d'autres collectes que la seule collecte des données de santé par les autorités sanitaires en charge de lutter contre la covid-19. On parle depuis quelques semaines de déployer des applications permettant un suivi plus corseté et systématique des personnes infectées ou supposées telles. Et ici, les questions liées aux finalités poursuivies, aux destinataires des données, au respect de la proportionnalité ou aux risques de détournement de données gagnent en acuité.

➢ *Les diverses expériences observées*

En effet, dès lors qu'il est question de collecter des données de **géolocalisation** (et a fortiori de les croiser avec des données de santé), la Directive eprivacy 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, s'applique également.

Or, cette directive n'autorise la données de telles collectes que (i) si une loi nationale ou un texte européen le prévoit expressément, (ii) elles font l'objet d'une anonymisation, ou (iii) si la collecte fait l'objet du consentement préalable de la personne concernée, pour des finalités qui lui sont clairement exposées.

Les médias prennent en exemple les initiatives d'autres pays face à la covid-19, telle la Corée du Sud qui collecte des données issues des dispositifs de vidéosurveillance, d'utilisation des cartes bancaires ou de bornage des téléphones portables, c'est-à-dire une collecte massive de données personnelles, relatives à des personnes malades ou non. On parle donc ici d'un suivi indifférencié des personnes, potentiellement sans leur consentement.

A titre d'exemples, le ministère de la Santé polonais a mis en place une application « *Home Quarantine* », qui exige la prise de selfies tout au long de la journée pour prouver son confinement continu, tandis que l'Irlande a instauré une application de suivi reposant sur le consentement de l'utilisateur à ce que ses déplacements soient tracés. Un état australien a voté une loi imposant un bracelet électronique aux personnes contaminées, avec comme alternative l'emprisonnement. Ailleurs encore, l'on veut croiser les données de géolocalisation et les données de réseaux sociaux afin de contrôler les fréquentations des individus contaminés, et l'on songe sérieusement à des applications qui iraient jusqu'à noter le niveau de contagiosité des individus et en informer les autorités… pendant qu'une société américaine propose de déployer des objets connectés pour permettre aux *entreprises* de suivre elles-mêmes leurs salariés malades. Et il ne s'agit là que d'un rapide florilège des idées qui fleurissent, peu compatibles avec les libertés publiques et la protection de la vie privée.

Des voix se sont élevées en Europe pour réclamer de mettre à contribution des données de communications électroniques (en clair, la géolocalisation des terminaux téléphoniques) pour contrôler les mouvements des populations, les attroupements et le respect du confinement ou des quarantaines.

En France, Orange a transmis à l'INSERM des informations sur les déplacements de ses abonnés, et notamment l'information selon laquelle 20% de ses abonnés franciliens avaient quitté la capitale à l'annonce du confinement.

L'opérateur a toutefois précisé qu'il n'avait nullement transmis de données individuelles à l'INSERM, mais uniquement des données *agrégées, statistiques* et donc non personnelles, pour permettre à l'INSERM d'analyser la mobilité autour du confinement (et pour s'il est respecté) et affiner son modèle épidémiologique en fonction de la mobilité des personnes, pour ajuster la réponse sanitaire globale. SFR a fait de même début avril avec les données de ses abonnés, utilisées pour produire des statistiques transmises à l'AP-HP et l'INRIA.

Il est certain que tant que les opérateurs de communications électroniques ne fournissent aux autorités que des données agrégées, exemptes de donnée relative aux terminaux mobiles ou à leurs porteurs, il n'y a pas là de traitement de données personnelles. Ce sont des données statistiques utiles aux autorités pour détecter et encadrer les déplacements dans le cadre là encore de la lutte contre la pandémie.

Toujours en France, d'aucuns ont proposé de mettre en œuvre la reconnaissance faciale, dont le secrétaire d'état au numérique, qui n'a cependant pas détaillé en quoi la reconnaissance faciale permettrait de prévenir les contagions sans croisement avec d'autres données dont les données de santé… En parallèle le ministère des armées lançait, mi-mars 2020, un appel d'offres pour solutions innovantes pour aider à « *limiter les déplacements* » et « *lutter contre la transgression* » des mesures de confinement.

Des expérimentations de surveillance des rues par drones ont été lancées à Paris et Marseille (ils ne sont pas équipés, au contraire des drones chinois, de détecteur thermiques qui renseigneraient sur l'éventuelle infection de la personne observée…). Puis, le développement d'applications de « tracking » des personnes contaminées, ou suspectées de contamination, a été lancé.

➢ *Les technologies de « contact tracing »*

Devant ces initiatives dispersées, plus ou moins gravement intrusives, le CEPD invite l'UE à procéder au développement d'une application commune aux états-membres, sécurisée et conforme au RGPD (notamment en termes de privacy by design). Un groupe de 130 chercheurs de huit pays européens entend donc lancer une plate-forme baptisée PEPP-PT (« *Pan-European Privacy Preserving Proximity Tracing* ») qui permettra de concevoir des applications ayant recours à ce fameux « ***contact tracing*** ».

La logique de ces applications, en résumé, consiste à pouvoir identifier les gens avec lesquels une personne contaminée (déterminée par un test si un test a pu être pratiqué), ou suspectée de contamination (parce que la personne se déclare d'elle-même infectée), a pu être en contact.

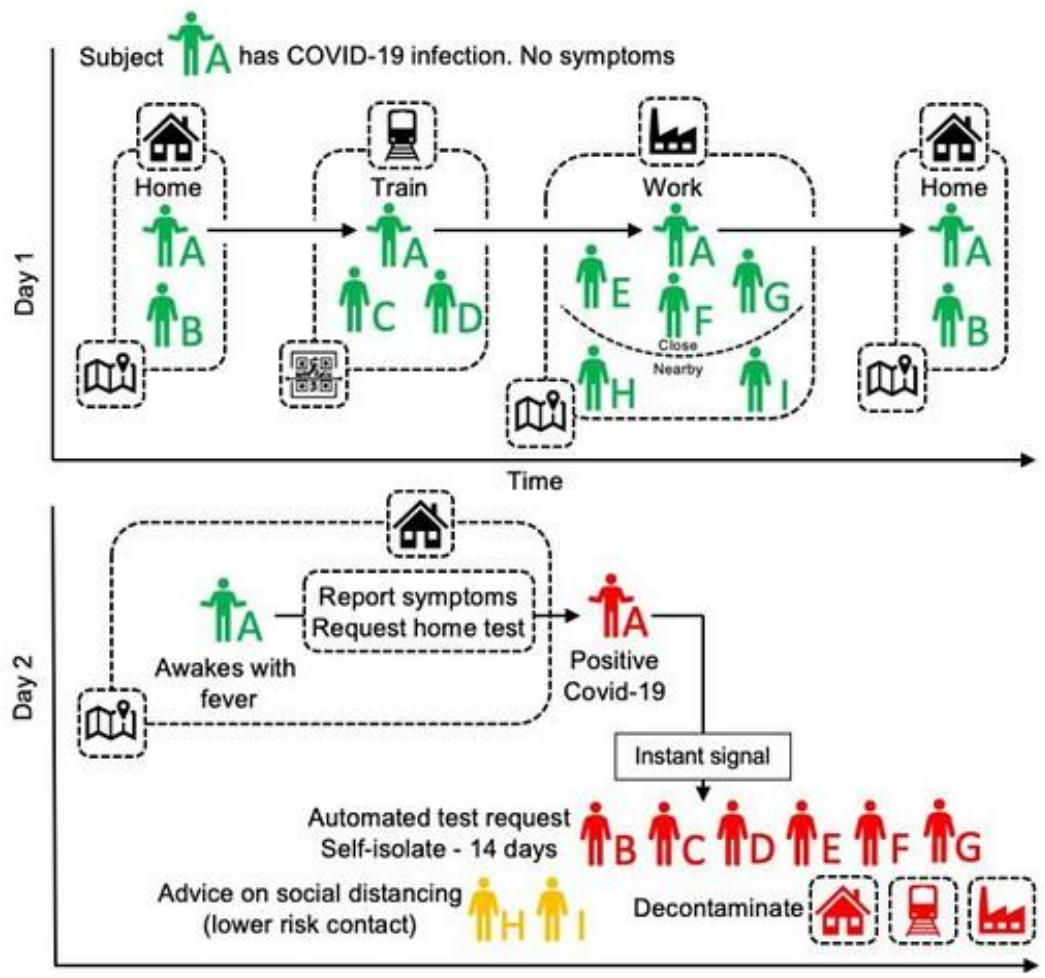
Concrètement, lorsque le possesseur d'une telle application est diagnostiqué positif à la covid-19, les personnes qu'il a côtoyés doivent être averties immédiatement et les autorités sanitaires les inviteront à se mettre en quarantaine. Les personnes ainsi alertées ne sont pas censées savoir à quel porteur elles ont été exposées ou qui les a potentiellement contaminé ni à quel endroit, mais simplement apprendre qu'elles ont été exposées. Le but de cette démarche

est de pouvoir sortir du confinement, en ne plaçant en quarantaine que les individus potentiellement porteurs.

Indépendamment de leur pertinence, réelle ou supposée, dans la lutte contre la propagation du virus, ces technologies permettent donc potentiellement la collecte de données personnelles de santé et de données comportementales, de manière certes indirecte mais tout aussi réelle, sur des millions d'individus, et à destination d'autorités qui n'ont rien de spécifiquement *médicales*.

La plate-forme PEPP-PT d'initiative européenne (reposant sur un protocole « DP-3T » pour « *Decentralized Privacy-Preserving Proximity Tracing* ») utilisera la technologie Bluetooth des téléphones mobiles « *de façon anonyme* » et sur la base du volontariat, et donc du consentement individuel des personnes (ce qui par construction en relativise l'efficacité comme on le verra *infra*, mais qui mise sur la responsabilité individuelle).

L'application est censée stocker « *via un chiffrement renforcé* » l'historique des connexions entre smartphones (les smartphones se détectant entre eux dès qu'ils sont suffisamment longtemps à proximité l'un de l'autre). Cet historique des contacts entre terminaux (et donc entre leurs propriétaires) doit être stockée sur le terminal lui-même, et non sur un serveur centralisé (à l'instar des applications de contrôle d'accès biométrique qui conservent les gabarits en local), et cette conservation sera limitée à une durée de deux semaines. Seules les autorités sanitaires locales, considérées comme des « *tiers de confiance* », seront censées pouvoir accéder aux données (ce qui invalide la notion de stockage en local), afin de pouvoir contacter les personnes concernées et leur recommander de se placer en isolement.



Source : *https://science.sciencemag.org/content/early/2020/03/30/science.abb6936*

La version française de ces applications, « ***StopCovid*** », doit elle aussi reposer sur la technologie Bluetooth, dont on explique qu'elle « *ne géolocalisera pas les personnes* » mais retracera uniquement « *l'historique des relations sociales qui ont eu lieu dans les jours précédents, sans permettre aucune consultation extérieure, ni transmettre aucune donnée* » selon le secrétaire d'état au numérique.

Ses promoteurs expliquent que cette application répondra à trois finalités :

- L'observation des pratiques collectives de mobilité et de confinement (finalité qui pourtant pourrait se satisfaire des données agrégées non personnelles transmises par les opérateurs de communication électroniques français) ;
- L'identification des sujets contact en retraçant le parcours récent des personnes testées positives (ce qui permet de constituer un profil individuel) ;
- Le contrôle des confinements individuels (ce qui là aussi a trait à un comportement individuel).

Comme on le verra plus loin, il va falloir choisir. L'application ne pourra pas permettre de répondre à ces trois finalités en même temps.

L'historique des terminaux croisés par l'appareil est certes moins intrusif que la géolocalisation, certes, mais contient néanmoins un très grand nombre d'informations sur la personne concernée, à l'instar des métadonnées associées aux courriers électroniques.

De plus, les données sont censées être **anonymisées**, et l'application ne permettra pas l'accès à la liste des personnes contaminées – affirmation problématique puisque dès lors qu'une liste existe, il est nécessairement possible d'y accéder, la vraie question étant de déterminer *qui* est habilité à le faire.

Enfin, l'installation de l'application serait faite sur la base du **volontariat** – ce qui permettrait ainsi de fonder le traitement sur la base légale du consentement des personnes, s'il est réellement éclairé.

La crise est telle que même des organes habituellement très opposés à toute forme de suivi systématique des populations à grandes échelles, et très sensibles aux risques d'avènement d'un « *big brother* », comme le Chaos Computer Club, se sont penchés sur les conditions qui permettraient de déployer de tels traitements. Et il est certain qu'un tel déploiement ne doit être permis qu'en respectant des conditions drastiques, techniques et légales.

➢ *Les exigences légales à satisfaire*

Rappelons donc les caractéristiques d'un consentement éclairé : la personne concernée doit a minima avoir été informée des éléments suivants :

- L'identité du responsable de traitement, ou, le cas échéant, des responsables conjoints du traitement ou de responsables de traitement ultérieurs souhaitant effectuer des traitements sur la base du consentement initial ;
- La ou les finalité(s) correspondant aux traitements pour lesquels le consentement est recueilli ;
- Les catégories de données qui seront collectées et utilisées ;
- Les destinataires des données collectées ;
- Les croisements de données qui seraient effectués, ainsi que l'éventuelle existence d'un dispositif de prise de décision algorithmique ou automatisée à partir des données collectées, incluant le profilage de la personne concernée, conformément à l'article 22 du RGPD ;
- Les risques liés aux éventuels transferts de données vers des pays tiers en l'absence d'une décision d'adéquation ou de garanties appropriées (clauses contractuelles types, BCR…) ;
- Le rappel du *droit à révocation du consentement* à tout moment et les moyens pour ce faire.

On le voit, les conditions pour l'obtention d'un consentement éclairé sont encore bien floues, tant que les promoteurs de cette application n'auront pas répondu à l'ensemble des points ci-dessus et prévu les modalités d'information des personnes concernées.

De plus, ces personnes disposeront-elles bien de leurs droits d'accès, de modification et surtout d'effacement de leurs données ?

En outre, rien n'est encore dit des services (sanitaires ? gouvernementaux ? de police ?) qui seraient autorisés à accéder aux données ainsi collectées. Et rien n'est dit de l'indispensable destruction rapide et définitive des fichiers de malades et des cartographies relationnelles ainsi constitués. Or, ces deux aspects sont indispensables pour que le consentement donné soit réellement éclairé, et donc légal.

Sur le plan légal, une telle solution semble donc sujette à caution, d'autant qu'on peut s'interroger sur le caractère réellement libre du consentement qui serait donné dans le contexte de peur actuel.

A cet égard, la CNIL, dont la présidente a été auditionnée par la commission des lois le 8 avril et à qui on promet de soumettre la version finale de l'application dont le code source sera ouvert et auditable, se tient à disposition du conseil scientifique mis en place pour gérer la crise sur ces sujets également.

La CNIL a indiqué à cet égard que les applications de « contact tracing » doivent impérativement :

- Répondre à des **finalités clairement définies** (s'agit-il donc ici de vérifier si les personnes respectent le confinement et restent chez elles, ce qui semblerait particulièrement intrusif compte tenu par ailleurs des nombreuses dérogations admises pour sortir de chez soi… ou s'agit-il de contrôler les personnes avec lesquelles un individu potentiellement contaminé a été en contact ? Apparemment les deux, ce qui pose la question du caractère spécifique du consentement donné) ;

- Collecter des **données strictement pertinentes et proportionnées** à l'objectif poursuivi (s'agit-il de collecter par géolocalisation l'ensemble des déplacements d'une personne, ou seulement la liste des terminaux que son téléphone a croisés, indépendamment du lieu ?) ;

- Ne conserver les données que pendant une durée très provisoire, sans réutilisation à quelque autre fin que ce soit (durée de l'infection de la personne concernée ? durée de la crise sanitaire, dont on sait qu'elle risque de se prolonger dans le temps tant qu'aucun vaccin n'est trouvé ?) ;

- Faire l'objet soit de modalités d'**anonymisation réelle**, soit du **consentement préalable** et éclairé des personnes, conformément aux exigences du RGPD et de la directive eprivacy ;

- Etre assorties de **mesures de sécurité techniques renforcées** (chiffrement des données, conservation en local sur l'appareil, etc.) ;

- Ne permettre l'accès aux données qu'à des **destinataires pertinents et limitativement énumérés** (s'agit-il de confier ces données à des autorités sanitaires uniquement ? A des autorités de police ?).

Quel que soit le sort de l'application « *StopCovid* » envisagée, elle devra impérativement respecter les exigences ci-dessus. Mais au-delà de cette *conformité juridique*, une question *d'opportunité* doit également être explorée, car elle participe aussi de la licéité du traitement en cause.

➢ *Une efficacité technique à prouver ?*

Par ailleurs, Du coup, certains commentateurs soulignent les failles de cette application : d'abord, la technologie Bluetooth ne trace qu'imparfaitement les contacts de la personne suivie, et manque de précision. La distanciation sociale implique quelques mètres, or le Bluetooth ne permet pas un tel degré de précision, d'où des risques d'alerte erronée et conséquemment, des mesures de quarantaine injustifiées (« faux positifs »). A l'inverse,

certaines interactions comportant le risque de contagion pourraient ne pas être identifiées, ce qui ruinerait en partie l'intérêt de la démarche (« faux négatifs »).

A cet égard, Antoine Courmont, chargé d'études prospectives à la CNIL, a rappelé, en récapitulant les options actuellement discutées, que les données qu'il s'agit de collecter n'ont rien d'infaillible : « *Tout comme les données de dépistage, les données de localisation issues des téléphones reposent sur des infrastructures techniques dont la précision et la fiabilité varient. La localisation par téléphonie mobile peut être effectuée par les opérateurs téléphoniques par bornage : relativement précise dans les zones denses aux nombreuses antennes relais, beaucoup moins dans les zones peu denses. Seuls les opérateurs télécom disposent de cette information. La deuxième option est la localisation par positionnement satellitaire (GPS). Elle présente l'avantage d'être disponible hors des zones de couverture des réseaux téléphoniques. Leur précision varie selon les modèles de smartphones, mais elle est de l'ordre de 5 mètres environ. Inconvénient : les GPS fonctionnent mal dans les environnements intérieurs et ne permettent pas, par exemple, de déterminer à quel étage d'un bâtiment vous vous trouvez. Les données de localisation GPS sont collectées par les fournisseurs des systèmes d'exploitation des smartphones (iOS, Android), ainsi que par certaines applications directement pour l'usage du service ou par le biais de SDK au profit d'acteur tiers. Ces derniers commercialisent ces données auprès d'autres acteurs, généralement à des fins publicitaires. La troisième option est la technologie Bluetooth qui permet de détecter les téléphones mobiles à proximité et d'estimer la distance entre ceux-ci en mesurant la puissance du signal. Elle est fréquemment utilisée, avec le wifi, dans les centres commerciaux ou les aéroports pour comprendre les déplacements des individus* ».

Ensuite, cette approche n'est pertinente que si une proportion majoritaire de la population décide d'y recourir et donne son consentement à ces collectes (à cet égard, seulement 29% de la population de Singapour a téléchargé l'application locale, ce qui l'a rendue largement inefficace). Cette application est aujourd'hui présentée comme une alternative en sortie de confinement : notons alors qu'en dépit de son déploiement, Singapour vient à son tour de confiner sa population.

Enfin et surtout, l'efficacité d'une telle application de « contact tracing » est directement conditionnée par la généralisation de tests fiables d'infection à la covid-19, ce qui n'est toujours pas d'actualité. Ce point, à lui seul, doit faire s'interroger sur la pertinence des traitements de suivi massif qui sont envisagés, et exige en tous cas de les entourer de toutes les précautions exigées par le RGPD.

Quelles conséquences doit avoir la détection d'un contact avec une personne contaminée ? L'individu qui reçoit l'alerte doit-il alors se confiner ? Que se passe-t-il s'il passe outre l'alerte ? Doit-on alors le *contraindre* à se mettre en quarantaine, alors qu'on n'a pas la certitude qu'il est atteint, ce qui pose un grave problème de liberté de circulation… ou choisit-il lui-même le comportement à tenir, ce qui amoindrit l'intérêt de ce suivi automatisé ?

Autre point majeur : si a collecte est anonymisée, comment pourrait-on ensuite appliquer des mesures *individuelles* aux personnes concernées ? Tant qu'il s'agit de contrôler des données statistiques de risque de propagation, l'anonymisation permet d'atteindre l'objectif. Mais comment pourrait-elle permettre également « *l'identification des sujets contacts* » et « *le respect des confinements individuels* » évoqués par le secrétaire d'état ? L'anonymisation,

présentée comme une garantie de protection des droits des personnes, pose également des questions, moins légales que techniques, auxquelles il est difficile de répondre.

➢ *Une anonymisation réelle ?*

A cet égard, l'anonymisation (largement revendiquée en temps normal par de nombreux développeurs) constitue souvent un leurre. Il faut rappeler qu'une véritable anonymisation est en réalité difficile à atteindre, car par recoupement ou déduction, il est souvent possible de réattribuer des données à une origine, et donc à une personne concernée.

A cet égard, même des informations que l'on pense totalement anonymisées peuvent conduire à l'identification d'une personne en fonction du comportement observé, comme ses habitudes de navigation web, ses déplacements, ou d'autres données que détiendrait l'administration sur elle. Ces données comportementales permettent de ré-identifier une personne dont on avait pourtant cru anonymiser les données.

Une donnée est dite « anonyme » lorsque (i) elle n'a plus de caractère intrinsèquement nominatif (plus de nom patronymique, plus d'adresse identifiante, etc.), (ii) elle ne peut plus être utilement corrélée à d'autres données qui, elles, demeurent identifiantes (données du smartphone), et (iii) on ne peut plus en inférer d'information sur une personne. Seule une donnée anonymisée ne permettant définitivement et absolument plus d'identifier une personne, elle peut être librement exploitée (par exemple, à des fins scientifiques, statistiques, d'études de flux, etc.).

Or, la CNIL insiste sur le fait que « *pour qu'une solution d'anonymisation soit efficace, elle doit empêcher toutes les parties d'isoler un individu dans un ensemble de données, de relier entre eux deux enregistrements dans un ensemble de données (ou dans deux ensembles de données séparés) et de déduire des informations de cet ensemble de données.* »

Or s'agissant des applications de « contact tracing », certains doutent, sur le plan technique, que le protocole permette une anonymisation complète dès lors qu'une personne se déclare infectée. Il s'agit d'un débat hautement technique, mais qui confirme que des failles peuvent exister.

Du reste, l'anonymisation est parfaitement antinomique avec tout traitement *individualisé* des personnes : ainsi, s'il est question de contacter une personne identifiée par une application de « *contact tracing* », il est alors parfaitement illusoire de prétendre que ses données auraient été collectées ou traitées de manière anonyme. S'il s'agit d'effectuer un tracé individuel, ou de « *contrôler les confinements* », il n'est tout simplement pas possible de recourir à une vraie anonymisation. Il ne s'agirait au mieux que d'une *pseudonymisation*, qui conserve donc le caractère personnel des données, et qui implique de recourir à une base légale autorisée par le RGPD.

Seul le consentement préalable et parfaitement éclairé, de la personne peut donc permettre le déploiement d'une application de « *contact tracing* » qui aurait d'autres finalités que la seule élaboration de statistiques agrégées – sauf si le législateur décidait que ces collectes ont justement pour fondement… la loi.

- ***Faut-il envisager une obligation légale ?***

Dans le cadre de ces projets envisagés en Europe, le CEPD a émis un avis en date du 19 mars 2020, pour indiquer que « *Le RGPD est un vaste texte législatif et prévoit des règles qui s'appliquent également au traitement des données personnelles dans un contexte tel que celui relatif au covid-19. Le RGPD permet aux autorités sanitaires et employeurs de traiter les données personnelles dans le contexte d'une épidémie, conformément au droit national et dans les conditions qui y sont fixées* ».

Autrement dit, en contexte exceptionnel, les états membres demeurent libres de voter des lois spécifiques permettant de déroger aux règles de base du RGPD, mais dans le respect des articles 6 et 9 du RGPD. La base légale ne pourrait donc être ici que l'intérêt général, et le législateur doit entourer ces collectes exceptionnelles de garanties solides.

Le CEPD se réfère également à la Directive eprivacy lorsqu'il écrit que « *l'article 15 de la directive ePrivacy permet aux États membres d'introduire des mesures législatives pour garantir la sécurité publique. Une telle législation exceptionnelle n'est possible que si elle constitue un instrument nécessaire, approprié et mesure proportionnée dans une société démocratique. Ces mesures doivent être conformes aux Charte des droits fondamentaux et la Convention européenne de sauvegarde des droits de l'homme et Libertés fondamentales. De plus, elles sont soumises au contrôle judiciaire de la Cour européenne des Justice et Cour européenne des droits de l'homme. En cas de situation d'urgence, il convient également de strictement limité à la durée de l'urgence.* »

Ainsi, s'agissant des projets de collecte massive de données de géolocalisation, le CEPD précise que si elles souhaitent géolocaliser des individus par exemple pour leur envoyer des messages de santé publique dans une zone spécifique par téléphone ou message texte, « *les autorités publiques doivent d'abord chercher à traiter les données de localisation de manière anonyme (c'est-à-dire traiter des données agrégées de manière à ce que les individus ne puissent être ré-identifiés), ce qui pourrait générer des rapports sur la concentration d'appareils mobiles à un certains endroits* ».

Un tel traitement « *devrait être soumis à un contrôle et à des garanties renforcés pour garantir le respect des principes de protection des données (proportionnalité de la mesure en termes de durée et de portée, limitation conservation des données et limitation de la finalité)* ».

On ne parle donc pas ici de constituer un fichier des malades par croisement avec des données de santé collectées par ailleurs, pour suivre spécifiquement les individus atteints par la covid-19, mais de diffuser des informations sanitaires afin de faire respecter les mesures de confinement ou de distanciation sociale.

Si la loi devait être choisie pour fonder de tels traitements, alors la collecte de données qui demeurent identifiantes doit impérativement respecter les principes de proportionnalité et de pertinence du RGPD, et donner lieu à une information renforcée des personnes *incluant le droit à un recours juridictionnel en cas d'abus*.

Cela signifie que l'Etat qui voterait une telle loi devra nécessairement assortir les collectes et traitements de dispositions très claires sur la durée maximale desdits traitements, sur les finalités limitatives pour lesquelles elles seront collectées, et sur les seuls services et personnels habilités à accéder à ces données.

De plus, imposer à l'ensemble de la population le recours à une application en dépit de la fracture numérique, placerait ipso facto certaines catégories de population hors la loi, tout simplement parce qu'elles ne pourront pas l'utiliser ou s'y conformer correctement.

De toute façon, à ce jour, l'Etat ne prévoit pas de rendre obligatoire le recours aux applications de « contact tracing ». On en revient donc aux deux possibilités précédentes : l'anonymisation réelle et définitive des données collectées dès leur collecte, ou le consentement éclairé préalable de chaque personne.

➢ *Une estimation risques / bénéfices qui reste à faire*

Récapitulons : (i) le consentement, libre et éclairé, demeure sujet à débat ; (ii) l'anonymisation pourrait être illusoire voire contre-productive ; (iii) il n'existe pas, pour l'heure, d'encadrement législatif prévoyant les garanties en termes de durée limitée, de destinataires spécifiquement définis et de mesures techniques et organisationnelles (incluant l'incontournable AIPD) : l'application envisagée actuellement (même si elle se contente de relever des interactions techniques entre téléphones portables pour retracer les contacts avec des personnes potentiellement infectées au lieu de géolocaliser les individus) semble encore peu efficace, et insuffisamment conforme au RGPD.

Il n'est pas question de s'opposer à tout crin au recours à des solutions technologiques reposant sur des collectes de données. Le chargé d'études prospectives de la CNIL rappelle à cet égard que « *Les données sont à la fois une technologie cognitive de mise en visibilité et un instrument d'action publique qui inclut une conception particulière du rapport gouvernant / gouverné. Ce dispositif de surveillance du virus et des populations est utilisé à des fins sanitaires et sécuritaires. En rendant visible le virus, sa propagation ou les déplacements des populations en temps de confinement, les données permettent d'appréhender un phénomène et de donner des prises à l'action* ».

Mais puisqu'il s'agit bien d'instruments de surveillance, ces « *coronoptiques* » doivent convoquer une réflexion juridique et philosophique, dans le moment « foucaldien » actuel, et ce nonobstant l'urgence. En matière de technologie, la question est et demeure en tous temps, surtout les plus troublés : « *qui garde les gardiens ?* » En substance, qui doit se charger de la surveillance ? Qu'est-ce qui doit être surveillé ? Comment doit-on surveiller ? Quelles décisions prend-on sur la base des données collectées (alors même que la médecine sait que les données de dépistage sont parfois fragiles ou trompeuses – que dire alors de données simplement comportementales ?)

C'est à ces questions que le RGPD demande de répondre. Lorsqu'il est question d'assurer la transparence, la précision des finalités, la limitation dans le temps du traitement, la limitation des personnes susceptibles d'accéder aux données, leur protection contre les détournements, c'est une *méthodologie* qu'on doit faire respecter – exactement comme les essais cliniques doivent respecter des méthodologies scientifiques dûment établies pour avoir un caractère probant et donc fiable ; la méthodologie juridique impose qu'on encadre la collecte et l'usage des données afin que le traitement ne puisse pas donner lieu à des discriminations, dégénérer en surveillance totalitaire au prétexte de la santé publique, ni créer un précédent en la matière.

A titre d'exemple, si les applications numériques évoquées pourraient permettre le suivi de la pandémie et le déploiement de préconisations de quarantaine en pistant les contacts des personnes contaminées, ce qui relève de la santé publique, on peut en revanche s'inquiéter qu'elles puissent également être utilisées aux fins de contrôler le respect du confinement, qui est une mesure de police indirectement liée, et très restrictive en termes de libertés publiques. Les promoteurs de l'application expliquent que le but n'est pas de mettre en place une surveillance généralisée de la population : on leur répondra que cet argument est invalide, dès lors que la technologie *peut permettre* une surveillance généralisée de la population.

En matière de technologies de surveillance, les autorités doivent garantir – pas seulement s'efforcer d'assurer, mais *garantir* la transparence sur les traitements effectués et les destinataires des données, ainsi que la destruction des fichiers dès la crise passée. Les pratiques observées ces dernières années, notamment en matière de fichiers de police, n'invitant pas vraiment à la confiance, le contrôle citoyen est indispensable, sauf à poser les bases d'une société de contrôle dont nous ne voulons pas.

C'est aussi pour cela qu'il faut regarder les applications d'initiative privée avec la plus grande circonspection, car elles véhiculent le risque de détournements de finalités, et peuvent même propager… des virus informatiques. A cet égard, Apple et Google viennent d'annoncer qu'elles travaillaient sur le contact tracing pour combattre la pandémie. Cela peut paraître une bonne nouvelle, compte tenu de leurs capacités financières et des compétences techniques de leurs services R&D… mais qu'on permette ici aux juristes, habitués aux condamnations récurrentes de certains grands acteurs du numérique sur la base du RGPD, de se poser des questions quant au respect des règles susmentionnées par ces entreprises. Les données de santé de la population française iront-elles aux USA ? Comment y seront-elles protégées le cas échéant ?

Compte tenu du caractère intrusif de la finalité évoquée et du caractère sensible des données collectées, une telle application ne devrait qu'être fournie sous les auspices de l'Etat, et soumise au contrôle des autorités compétentes en matière de données personnelles. Ces applications permettent par construction, un suivi de masse de toute la population. Et à cet égard, certaines CNIL européennes sont plus que réticentes.

Dans tous les cas, une analyse d'impact est à mener. Le RGPD impose en effet d'effectuer une analyse exposant les risques encourus par les personnes physiques dont les données seront traitées via l'outil de traitement envisagé. L'article 35 du RGPD dispose que « *Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel* ».

Compte tenu de l'échelle envisagée (toute la population), des données concernées (données de santé), des technologies utilisées, l'AIPD apparaît ici incontournable. C'est cette analyse qui pourra permettre de se prononcer sur le bilan à faire entre avantages espérés et risques induits par ce traitement de surveillance de masse.

Conclusion (provisoire)

Il est donc légitime de s'interroger sur le rapport bénéfice / inconvénients des applications de « contact tracing » dont l'efficacité est largement conditionnée par des facteurs qui lui sont extérieurs, en même temps qu'elle introduirait un précédent problématique en matière de suivi généralisé de la population…

Si les outils numériques et le « big data » peuvent fournir des approches inédites et efficaces à grande échelle, qu'on doit évidemment considérer pour optimiser nos chances d'enrayer la pandémie, on doit cependant se protéger du *solutionnisme* qui voudrait que nos problèmes soient réglés par des applications et des algorithmes qu'on sait parfois défaillants, et dont on n'assurerait pas l'encadrement juridique adéquat. Certes, chercheurs et développeurs travaillent actuellement à corriger les effets pervers mentionnés plus haut, à renforcer l'efficacité technique encore incertaine, et à limiter les impacts sur les libertés individuelles. Sera-ce suffisant ?

« StopCovid » n'arrêtera pas la pandémie, car c'est de la science médicale que la solution viendra. Les applications numériques doivent rester des outils, entre les mains *des populations elles-mêmes* et non pas de leurs dirigeants, pour que tout un chacun participe individuellement à cet effort, sans nous faire collectivement courir le risque d'un recul des libertés publiques.

Certaines voix se sont élevées pour rappeler que les crises telles que celle que nous connaissons, peuvent conduire à la suspension de certaines libertés publiques, mais qu'alors de telles mesures doivent être formellement limitées à ce qui est strictement nécessaire, soigneusement encadrées par la loi, extrêmement provisoires, et approuvées par voie démocratique, afin de ne jamais sacrifier les libertés publiques sur l'autel de l'urgence ou de la peur.

Ces précautions, qui pourraient paraître byzantines face à la menace sanitaire, sont néanmoins des garde-fous indispensables si nous voulons préserver les droits fondamentaux qui distinguent les pays démocratiques d'autres régimes bien moins enviables. C'est précisément dans la tempête qu'on éprouve la solidité de ces principes fondamentaux : la vigilance de tous est donc de mise, face à des traitements de données personnelles qui ouvriraient la voie à une société de surveillance bien plus liberticide encore, avec ou sans pandémie.

Il est aisé de critiquer d'autres pays, comme la Chine, pour le peu de cas qu'ils font des droits fondamentaux en temps normal ; il serait extravagant de s'aligner sur eux, même face à des défis exceptionnels – défis qui pourraient d'ailleurs être de moins en moins exceptionnels dans les années qui viennent. La tentation sécuritaire, qu'elle puise ses motivations dans la lutte contre le terrorisme ou les crises sanitaires, sera toujours un mauvais choix – et ce d'autant plus qu'elle s'avère le plus souvent, en définitive, inefficace contre les menaces en question.

Thomas Beaugrand,
Counsel
beaugrand@dsavocats.com

Pour plus d'information, notre équipe se tient mobilisée pour répondre à vos questions :

Catherine Verneret,
Associée
verneret@dsavocats.com

Bertrand Potot
Associé
potot@dsavocats.com

Sylvain Staub,
Associé
staub@dsavocats.com

Antoine Gravereaux,
Associé
gravereaux@dsavocats.com

A propos de DS Avocats

Fondé en
1972

300
professionnels du droit

22
bureaux

13
pays

4
continents

Un grand cabinet français de droit privé et public des affaires,

Créé en 1972 à Paris, DS Avocats a développé son savoir-faire au bénéfice des entreprises et des collectivités publiques. Cette double culture du public et du privé est un atout et constitue la signature du Cabinet.

organisé autour de spécialistes renommés dans tous les domaines du droit

Le Cabinet compte aujourd'hui près de 300 professionnels intervenant dans tous les domaines du droit des affaires, aussi bien en conseil qu'en contentieux. Nos équipes sont régulièrement citées parmi les meilleures du marché par les classements de référence dans le domaine juridique.

qui unissent leurs forces pour proposer une offre juridique de qualité et de proximité.

Les professionnels de DS Avocats interviennent en équipe (le cas échéant avec des partenaires non juridiques) pour permettre aux projets de ses clients d'allier excellence technique, expertise sectorielle et vision transversale.

Un des leaders européens en Asie,

DS Avocats, présent depuis plus de 30 ans en Chine, dispose aujourd'hui de 4 bureaux sur le continent asiatique.

résolument tourné vers l'international

DS Avocats poursuit et développe sa stratégie vers l'international, avec aujourd'hui 22 bureaux répartis dans 13 pays sur 4 continents.

www.dsavocats.com