Le cadre juridique des dispositifs détectant le port du masque chez les usagers des transports

Par Aloïs Ramel et **David Conerardy**, avocats, Cabinet Seban & associés

L'apparition et le développement rapide du Covid-19 en France ont pu entraîner, parfois hors de tout contrôle, la collecte de données à caractère personnel par les organismes de transport afin de vérifier que le port du masque était effectif. La responsabilité des organismes publics peut être engagée.

La collecte de données à caractère personnel est strictement encadrée par la législation et, dès lors que les obligations issues du règlement général sur la protection des données ne sont pas respectées, la responsabilité des organismes publics peut être engagée alors même qu'ils n'ont pas forcément perçu le manquement à leurs obligations.

Captation d'image : traitement de données à caractère personnel

Captation d'image automatique comme activité de traitement de données à caractère personnel soumise au RGPD

La mise en œuvre d'outils de captation d'images est un traitement de données à caractère personnel dès lors qu'il collecte des données à caractère personnel. Pour rappel, un traitement correspond à toute utilisation de données à caractère personnel.
L'article 4 du Règlement général pour la protection des données (RGPD) donne la définition des données à caractère personnel : « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».
Aussi, un visage reconnaissable est une donnée à caractère personnel puisqu'elle permet l'identification indirecte d'une personne physique au travers d'un élément spécifique propre à son identité physique.
La Cour de justice de l'Union européenne, interrogée au travers d'une question préjudicielle des juridictions tchèques en 2014, a rendu une décision soumettant l'ensemble des systèmes de vidéoprotection aux dispositions de la directive de 1995 (le texte de référence antérieur au RGPD), puisque ce système de surveillance comprenait bien des données à caractère personnel, qu'elles étaient bien identifiantes et qu'il y avait bien une activité de traitement.
Lorsque l'on évoque le concept d'activité de traitement de données, tous les procédés sont pris en compte. Il peut s'agir d'une action de collecte, d'enregistrement, d'organisation, de conservation, d'adaptation, de modification, d'extraction, de consultation, d'utilisation, de communication par transmission ou toute autre forme de mise à

© KHALIGO-ADOBESTOCK

disposition, de rapprochement ou d'interconnexion, de verrouillage, d'effacement ou de destruction de données à caractère personnel. Dans ces conditions, une surveillance effectuée par un enregistrement vidéo des personnes, stocké dans un dispositif d'enregistrement continu, à savoir le disque dur, constitue un traitement de données à caractère personnel automatisé. Ce faisant, dès lors qu'est envisagé un traitement de données, celui-ci doit respecter la législation issue du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et au RGPD du 27 avril 2016.

Régime juridique de la captation d'images

Il existe deux grands systèmes relatifs aux outils de captation d'images. Le premier, nommé vidéosurveillance, consiste à filmer des lieux privés ou des lieux de travail non ouverts au public.

Le régime juridique applicable sera celui de la loi Informatique et libertés et du RGPD. Le second, nommé vidéoprotection, consiste à filmer la voie publique et les lieux ouverts au public. Le régime juridique applicable sera celui prévu aux articles L.251-1 et suivants du code de la sécurité intérieure (CSI) et, selon la finalité du système de vidéoprotection, deux régimes juridiques européens différents peuvent s'appliquer. Pour les responsables de traitement, la difficulté, résultant du droit européen, consiste à déterminer si leur dispositif de vidéoprotection relève du champ du RGPD ou du champ de la directive « police-justice ». La détermination du régime juridique dépend de l'objectif poursuivi par le système de vidéoprotection mis en œuvre.

Ainsi, s'il est mis en œuvre, dans le cadre de leurs missions, par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, il relève des dispositions transposées de la directive.

À noter

La détermination du régime juridique dépend de l'objectif poursuivi par le système de vidéoprotection mis en œuvre.

Comme l'indique la Commission nationale de l'informatique et des libertés (Cnil) sur son site internet, les finalités prévues par le CSI entrant dans le cadre de la directive « police-justice » sont les suivantes :

- protection des bâtiments, des installations publics et de leurs abords ;
- constatation des infractions aux règles de la circulation ;
- prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants ainsi que la prévention, dans des zones particulièrement exposées à ces infractions, des fraudes douanières prévues par le dernier alinéa de l'article 414 du code des douanes et des délits prévus à l'article 415 du même code portant sur des fonds provenant de ces mêmes infractions ;
- respect de l'obligation d'être couvert, pour faire circuler un véhicule terrestre à moteur, par une assurance garantissant la responsabilité civile ;
- assurer la protection des abords immédiats des bâtiments et installations de commerçants installés dans les lieux particulièrement exposés à des risques d'agression ou de vol.

Au contraire, toujours selon la Cnil, le système de vidéoprotection relève du RGPD dès lors qu'il a pour objet l'une des finalités suivantes :

- régulation des flux de transports ;
- prévention des risques naturels ou technologiques ;
- sécurité des installations accueillant du public dans les parcs d'attractions ;
- sécurité des personnes et des biens dans des lieux et établissements ouverts au public, lorsque ces lieux et établissements sont particulièrement exposés à des risques d'agression ou de vol.

Dans le cadre de la mise en place de caméras couplées à un logiciel permettant la reconnaissance du port du masque dans les transports en commun, il semble principalement s'agir, à l'heure actuelle, de la poursuite de fins statistiques.

Bien que ce système puisse être rapidement appelé à évoluer, il ne s'agit pas de missions à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière. Par ailleurs, on pourrait rapprocher cette activité de traitement aux missions relatives à la régulation des flux de transports. À l'heure actuelle, il nous semble que les dispositions applicables au

.../...

.../... traitement mis en œuvre par les structures de transports intéressées par la technologie seront celles relatives au CSI et au RGPD. Aussi, il ne fait aucun doute qu'une image de visage captée par un tel système vidéo est en soi un traitement de données relevant du RGPD (contrairement à ce que certains prestataires ayant vendu le système aux autorités organisatrices de transports ont pu prétendre).

Contrôle de la légalité du traitement

Comme tout traitement de données à caractère personnel, le système vidéo de détection automatique de port du masque doit respecter un certain nombre de principes fondamentaux pour être valide, notamment lorsque la collecte peut sembler attentatoire à la vie privée.

Licéité du traitement

S'agissant de la licéité, cela suppose, pour qu'un traitement soit valablement mis en œuvre, qu'il se fonde sur l'une des bases légales prévues par le RGPD. Cette base légale est ce qui va autoriser légalement la mise en œuvre du traitement et entraînera de nombreuses conséquences quant aux droits et libertés des personnes dont les données seront collectées. Il existe six bases distinctes :

- le consentement de la personne : la personne a consenti au traitement de ses données ;
- l'obligation légale : le responsable de traitement se voit imposer son activité de traitement de données par un texte légal ;
- la mission d'intérêt public : le traitement de données permet l'exercice d'une mission de service public ou d'intérêt public ;
- la sauvegarde des intérêts vitaux : le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne ou d'un tiers ;
- le contrat : le traitement est nécessaire à l'exécution ou à la préparation d'un contrat avec la personne concernée ;
- l'intérêt légitime : le traitement est nécessaire à la poursuite d'intérêts légitimes de l'organisme qui traite les données ou d'un tiers, dans le strict respect des droits et intérêts des personnes dont les données sont traitées.

Chacun de ces six fondements juridiques présente des avantages et des inconvénients, tout en n'étant pas également accessible par le responsable de traitement. Par exemple, se fonder sur une obligation légale ne sera évidemment pas possible dès lors qu'il n'y a pas de fondement textuel. En l'espèce, dans le cas d'une collectivité territoriale gérant un service de transport, il est immédiatement possible d'écarter la sauvegarde des intérêts vitaux, inapplicable à ce traitement, ainsi que le consentement, insusceptible d'être recueilli dans les conditions requises (libre et éclairé). Par ailleurs, aucun texte légal n'impose aux autorités gérant des activités de transport de vérifier, au moyen de caméras, la réalité du port d'un masque. Il reste donc trois bases légales envisageables.

S'agissant du contrat, il semble peu probable qu'une clause ait pu prévoir le port d'un masque individuel et le contrôle au moyen d'un système de vidéoprotection avec application d'un logiciel. Si cela devait être le cas, il s'agirait de modifications ultérieures du contrat qui ne seraient pas applicables à l'immense majorité des usagers des transports avant le renouvellement de leur titre de transport. Aussi, cette base légale ne pourrait pas être légitimement mobilisée.

S'agissant de l'intérêt légitime, il n'est tout d'abord pas permis aux autorités publiques d'utiliser cette base légale dans le cadre de leurs missions de service public. Or dans le cas d'une collectivité territoriale gérant un service de transport, c'est elle qui, en tant qu'autorité organisatrice de la mobilité, a décidé de l'installation de ce système et qui en est responsable de traitement. Aussi, cette base légale ne pourrait pas être légitimement mobilisée.

À noter

L'utilisation d'un logiciel mis en place pour contrôler en temps réel le port du masque dans les services de transports publics aura pour finalité de donner une estimation en temps réel du nombre de personnes portant ou non ledit masque, dans une logique de contrôle.

S'agissant de la mission d'intérêt public, dernière base légale encore applicable, il s'agit de la base légale privilégiée des autorités publiques. Le recours à cette base légale se justifie en particulier pour les traitements mis en œuvre par les autorités publiques aux fins d'exécuter leurs missions. Le recours à la mission d'intérêt public pour fonder légalement un traitement est soumis à deux conditions : la condition de nécessité, précédemment évoquée, et le fait que l'intérêt public doive être défini par le droit européen ou le droit national.

La Cnil, au sujet de cette base légale, développe : « Le traitement concerné doit ainsi permettre d'exercer, de manière pertinente et appropriée, la mission dont est investie l'autorité publique et ne doit pas viser un autre objectif, sans rapport particulier ou trop éloigné des spécificités de la mission d'intérêt public en cause ». En l'espèce, dans le cas d'une collectivité territoriale gérant un service de transport, il faudrait accorder un soin attentif aux développements relatifs à l'utilité de cette mission d'intérêt public.

Finalité du traitement

La finalité d'un traitement est l'objectif principal poursuivi par l'utilisation de données à caractère personnel. Il est imposé par le RGPD que les données personnelles en question doivent être collectées pour des finalités déterminées, explicites et légitimes. Cela suppose que le traitement en question doive poursuivre des objectifs clairement annoncés, notamment aux personnes dont les données sont collectées, que cet objectif doit être autorisé par son fondement légal et surtout qu'il ne puisse pas évoluer ultérieurement.

Dans le cas d'une autorité organisatrice de transport, l'utilisation d'un logiciel mis en place pour contrôler en temps réel le port du masque dans les services de transports publics aura pour finalité de donner une estimation en temps réel du nombre de personnes portant ou non ledit masque, dans une logique de contrôle.

Dans ce cadre, il faudrait que la finalité soit spécialement indiquée, particulièrement claire, accessible et légitime.

En effet, il n'est pas possible de justifier une activité de traitement en indiquant qu'il vise une finalité statistique relative au port du masque alors qu'il pourrait, en même temps, servir de base à des activités de contrôle des polices municipales et des contrôleurs sur ce même port de masque. Il est impossible de traiter ultérieurement des données à caractère personnel sur une finalité qui n'avait pas été à l'origine prévue, à moins d'informer préalablement l'ensemble des personnes concernées de la modification ou de l'élargissement de la finalité en leur laissant la possibilité de s'y opposer.

Aussi, soit le logiciel de port du masque permet uniquement d'avoir une information statistique, soit il permet d'avoir cette information statistique et permet la mise en œuvre de mesures de contrôle. Les mesures de contrôle ne sont pas en elles-mêmes interdites. Ce qui est interdit, c'est d'entretenir le flou sur les finalités d'une activité du traitement. Un traitement ne peut être déterminé et explicite si les finalités poursuivies ne sont pas clairement assumées par le responsable de traitement.

Pertinence du traitement

Un des principes fondamentaux de toute activité de traitement est son adéquation, sa pertinence et sa limitation au regard


© ALEXZEER-ADOBESTOCK

des finalités qui ont été définies par le responsable de traitement. On retrouve ici la condition évoquée au sujet du critère de nécessité, inhérent aux bases légales.

Au-delà de ce qui a déjà été évoqué, dès lors qu'une autorité décide de concourir à la santé de la population au travers des gestes barrières et du contrôle du port du masque, le moyen le plus évident pour arriver à l'efficience de la finalité recherchée n'est pas tant de contrôler le port du masque que de distribuer les masques gratuitement à l'entrée des services de transports. En faisant ce choix, la finalité est réalisée sans que les droits et libertés des personnes soient atteints (et en déployant certainement moins de moyens financiers). Au-delà, d'autres systèmes alternatifs sont possibles. On pourrait imaginer que la mesure du port du masque pourrait être réalisée par des personnes physiques dans les bus (par exemple le conducteur), ou ce contrôle pourrait être réalisé d'ores et déjà au travers des caméras de vidéoprotection existantes.

La question de l'adéquation et de la pertinence du traitement pose également celle de la proportionnalité des données collectées. Autre principe cardinal du droit des données : est-il absolument nécessaire de filmer les gens pour se donner une idée du nombre de personnes ne portant pas de masque ? Aussi, il ressort des éléments du dossier à notre disposition que la pertinence du traitement de données à caractère personnel pourrait sans doute être contestée.

Contrôle de la Cnil : le problème du droit d'opposition

Finalement, il ressort de l'ensemble des débats sur la détection du port du masque par logiciel dans les transports en commun qu'il n'est pas possible pour les particuliers de s'opposer à la collecte de leurs données à caractère personnel. En effet, dès lors que des données à caractère personnel apparaissent dans des fichiers non obligatoires, le droit d'opposition doit permettre aux individus dont les données sont collectées de s'opposer à ce que leurs données soient utilisées par un organisme pour un objectif précis. Or en l'espèce, le particulier devait bouger la tête d'une certaine manière pour faire comprendre au logiciel de captation d'image que celui-ci entendait exercer son droit d'opposition. Cela supposait donc que celui-ci doive établir un acte positif pour s'opposer.

La Cnil, au sujet de cette technologie, résume sa position en indiquant : « Leur développement incontrôlé présente le risque de généraliser un sentiment de surveillance chez les citoyens, de créer un phénomène d'accoutumance et de banalisation de technologies intrusives, et d'engendrer une surveillance accrue, susceptible de porter atteinte au bon fonctionnement de notre société démocratique. […] Le déploiement massif de ces dispositifs de captation de l'image des individus et de détection de certains de leurs attributs, comportements ou émotions pourrait conduire, chez les personnes concernées, à une modification – voulue ou subie – de leurs comportements ».

Ainsi, la Cnil entend se positionner comme la garante de la protection des libertés individuelles en empêchant le développement anarchique de cette technologie qu'elle estime potentiellement attentatoire à la vie privée.

Références

- **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.**
- **Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.**
- **Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.**