



HAL
open science

“ Vidéo intelligente ” et port du masque dans les transports : la nécessité du malentendu

Emmanuel Netter

► **To cite this version:**

Emmanuel Netter. “ Vidéo intelligente ” et port du masque dans les transports : la nécessité du malentendu. Dalloz IP/IT : droit de la propriété intellectuelle et du numérique, 2021, 7-8/2021, pp.415. halshs-03294224

HAL Id: halshs-03294224

<https://shs.hal.science/halshs-03294224>

Submitted on 24 Aug 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Décret n° 2021-269 du 10 mars 2021
« Vidéo intelligente » et port du masque dans les transports : la nécessité du malentendu

Dalloz IP/IT, 2021, p. 415

Emmanuel Netter
Professeur de droit privé à l'université d'Avignon
Directeur du LBNC (EA 3788)

En avril 2011 entré en vigueur une loi « interdisant la dissimulation du visage dans l'espace public » (loi n° 2010-1192 du 11 octobre 2010). Dix ans et une pandémie mondiale plus tard, voici les pouvoirs publics en train de lutter pour obliger les citoyens à sortir de chez eux masqués. Parmi les textes contribuant à la poursuite de cet objectif, un décret n° 2021-269 du 10 mars 2021 « relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports ». Celui-ci a fait l'objet d'un avis de la CNIL en date du 17 décembre 2020 (délibération n° 2020-136 : N. Maximin, D. actu, 15 mars 2011).

L'objectif : haut les masques

Le texte affirme pour commencer que « Dans les territoires où, pour faire face à l'épidémie de covid-19, une loi ou un décret impose le port d'un masque de protection dans les véhicules ou les espaces accessibles au public et affectés au transport public de voyageurs, les exploitants de services de transport public collectif de voyageurs ainsi que les gestionnaires des espaces affectés à ces services veillent au respect de cette obligation ».

À ce stade, il est encore possible d'imaginer que l'on va chercher à identifier et sanctionner les contrevenants. Un tel texte, relatif à la détection d'infractions pénales, aurait relevé non pas du RGPD, mais de la directive dite « police-justice » du 27 avril 2016. Utilisant l'intelligence artificielle et la vidéosurveillance pour détecter et punir des comportements individuels, il aurait constitué un événement politique majeur et suscité de vives réactions des défenseurs des libertés fondamentales.

Mais ce Rubicon n'est pas – encore – franchi, et les finalités du traitement ici commenté sont plus modestes. Il s'agit ici « d'évaluation statistique » du respect de l'obligation de port du masque et « d'adaptation des actions d'information et de sensibilisation du public ». Ainsi le gestionnaire du service de transport saura-t-il que, dans une partie de son réseau, le masque n'est correctement porté que par 58 % des passagers. Il pourra alors déclencher des messages de sensibilisation, qui ne pourront en aucun cas être individualisés (« vous, Madame, à la chevelure brune et au manteau bleu»), mais seulement génériques.

Pour autant, un tel traitement de données n'est pas entièrement anodin. La CNIL rappelle tout d'abord qu'elle a « pleinement conscience de la gravité de la situation sanitaire liée à l'épidémie de COVID-19 et de la nécessité pour le Gouvernement de prendre les mesures nécessaires de protection de la population » (§2). Mais elle relève ensuite que « L'espace public est un lieu où s'exercent de nombreuses libertés individuelles (droit à la vie privée, à la protection des données à caractère personnel, liberté d'aller et venir, liberté d'expression, etc.). La préservation de l'anonymat dans l'espace public est une dimension essentielle pour l'exercice de ces libertés ; la captation et l'analyse systématiques de l'image des personnes dans ces espaces sont incontestablement porteuses de risques pour leurs droits et libertés fondamentaux » (§3).

Il faut donc mettre en balance, d'une part, « l'objectif à valeur constitutionnelle de protection de la santé » (§4) et, d'autre part, « les protections constitutionnelle et conventionnelle du droit au respect de la vie privée et à la protection des données à caractère personnel » (§5). Cela suppose, pour l'autorité de protection, d'évaluer les risques suscités par le traitement.

Les garanties : une anonymisation à bref délai

Il faut commencer par souligner que ces risques sont assez faibles à l'échelle individuelle. De sérieuses garanties techniques sont prévues par le décret.

Ainsi les images, collectées par des caméras situées exclusivement dans des espaces publics, ne font-elles l'objet d'aucun stockage ni d'aucune transmission à des tiers. Sitôt produites, elles sont transformées en statistiques agglomérées, révélant un taux de non-port du masque. Pour diminuer encore le risque de réidentification, une faible granularité est imposée par le texte : les chiffres ne sont pas produits à l'échelle d'une ou de quelques caméras, mais au niveau d'une gare ou d'une station de métro dans son ensemble ; ils ne remontent pas en temps réel, mais par segments de 20 minutes au moins. Nous n'avons donc affaire à des données personnelles que durant un instant de raison. Immédiatement ou presque, les informations deviennent anonymes au sens de l'article 4 du RGPD, le lien avec les individus ayant été détruit de manière irréversible.

Par ailleurs, la finalité pédagogique du dispositif doit faire l'objet d'une interprétation stricte. Nous avons déjà vu que la « vidéo intelligente » n'aura pas pour effet de désigner des contrevenants précis. Mais, répondant aux questions de la CNIL, le ministère de l'Intérieur va plus loin et précise que les données ne serviront pas même à renforcer à court terme, dans une zone problématique, les effectifs d'agent ayant pouvoir de *sanction*. Les seuls redéploiements à bref délai concerneront des personnels chargés de la *sensibilisation* des usagers.

Le risque : la banalisation de la surveillance

Si le risque d'atteintes individuelles aux libertés semble donc plutôt bien maîtrisé, le danger est ailleurs. La CNIL tient en effet « à rappeler la nécessaire vigilance qui s'impose dans le déploiement de ces dispositifs qui impliquent une collecte et une analyse systématiques de l'image des individus circulant dans les transports publics et une détection de certains de leurs attributs. Même s'il est limité au cadre de l'état d'urgence sanitaire, un tel déploiement présente le risque réel de généraliser un sentiment de surveillance chez les citoyens, de créer un phénomène d'accoutumance et de banalisation de technologies intrusives et, en définitive, d'engendrer une surveillance accrue » (sur cette question : W. Maxwell, « Vidéo intelligente dans les trains, bus et métros : attention à l'effet "cliquet" », D., 2021, 792).

Déjà, dans son avis sur l'application « Stop Covid » (devenue « Tous Anti Covid »), la Commission craignait « un phénomène d'accoutumance propre à dégrader le niveau de protection de la vie privée » (délibération n° 2020-046 du 24 avril 2020). De ce point de vue, la vidéo intelligente nous semble cependant présenter un danger bien plus grand. L'installation et l'utilisation d'une application de contact tracing reposent sur une démarche volontaire du citoyen, qui peut changer d'avis à tout instant. La vidéo intelligente destinée à détecter le port du masque, quant à elle, n'est pas fondée sur le consentement des personnes concernées. Le décret refuse également aux passagers tout droit d'opposition - « de façon relativement inédite », ajoute la CNIL. Votre image fera l'objet d'un traitement algorithmique, que vous le vouliez ou non : une telle situation est certainement propice à accoutumer progressivement la population à une surveillance automatisée.

L'article 23 du RGPD prévoit, il est vrai, que les droits des personnes concernées par le traitement puissent être limités, « lorsqu'une telle limitation respecte l'essence des libertés et droits

fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir (...) d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines (...) de la santé publique et de la sécurité sociale (...). On relèvera la tournure surprenante du texte, qui n'adosse pas la dérogation directement à la santé publique, mais à un « intérêt économique ou financier », qui peut se manifester notamment dans le domaine de la santé publique.

L'article 23 du RGPD subordonne ensuite la limitation des droits des personnes concernées à deux conditions. La première, c'est qu'elle ait lieu « par la voie de mesures législatives ». Le considérant 41 précise cependant que cette expression doit être entendue dans un sens large de « base juridique claire et précise ». Un simple décret, en l'espèce, peut donc suffire (en droit interne, l'article 56 de la loi informatique et libertés fait sobrement référence à « l'acte instituant le traitement »). La deuxième condition (art. 23.2 du RGPD), c'est que le texte d'encadrement contienne un ensemble d'informations dont la liste est fournie. L'avis de la CNIL relevait l'absence, dans le projet de décret qui lui avait été communiqué, du h), relatif « au droit des personnes concernées d'être informées de la limitation, à moins que cela ne risque de nuire à la finalité de la limitation ». Le texte définitif a été corrigé en ce sens.

Le bilan : une utilité douteuse

Proposons une fois encore une analogie avec l'avis rendu par la CNIL sur l'application « Stop Covid ». La Commission estimait que « (...) **l'atteinte portée à la vie privée ne sera en l'espèce admissible que si**, en l'état des informations inmanquablement lacunaires et incertaines dont il dispose pour affronter l'épidémie, le gouvernement peut s'appuyer sur des éléments suffisants pour avoir l'assurance raisonnable **qu'un tel dispositif sera utile** à la gestion de la crise, et notamment à la sortie du confinement (...) » (souligné par nous).

Il s'agit tout simplement d'appliquer le principe de minimisation, qui commande, parmi toutes les voies permettant d'atteindre la finalité recherchée, de toujours utiliser la moins intrusive pour les individus. Cette démarche peut même aboutir à ce qu'une surveillance automatisée soit rejetée dans son principe, lorsqu'une surveillance exercée par des êtres humains est susceptible d'une efficacité comparable : c'est l'un des arguments qui avaient conduit le tribunal administratif de Marseille à refuser la mise en place d'un dispositif de reconnaissance faciale à l'entrée de lycées de la région PACA (TA Marseille, 27 févr. 2020, req. n° 1901249).

En l'espèce, il a été démontré que le traitement était peu risqué d'un point de vue individuel, mais dangereux collectivement, en ce qu'il contribue à habituer la population aux surveillances algorithmiques dans l'espace public. Or, en contrepartie de ces risques, l'utilité apparaît très faible.

Imaginons en effet que le responsable du traitement exécute parfaitement ses obligations en matière de transparence. Les passagers sauront alors qu'*en aucun cas* une absence de port du masque ne pourra aboutir, par le biais de la vidéo intelligente, à une forme de sanction. Les seules conséquences ? Des annonces stéréotypées par haut-parleur, ou un déploiement d'agents de sensibilisation. Or, qui peut sérieusement affirmer, après une année durant laquelle la pandémie aura occupé la première place de l'actualité du matin au soir, qu'il reste des citoyens ignorants de l'utilité du port du masque ? Le non-port ou le port incorrect sont, à l'évidence, des actes pleinement conscients. Dès lors, le dispositif ici commenté n'aura un quelconque intérêt que s'il est *mal compris* par les voyageurs, craignant à tort une sanction et rectifiant leur comportement en conséquence. Une telle issue est tout à fait envisageable. Il est vraisemblable que l'impossibilité d'une sanction ne sera pas proclamée par une voix de synthèse dans les bus et métros – le résultat d'ensemble serait

grotesque – mais simplement révélée par la voie d'un affichage que personne ne lira. On peut avoir confiance : les politiques de confidentialité jamais consultées, l'opacité dans la transparence sont des savoir-faire parfaitement maîtrisés dans la pratique du droit des données personnelles.

Triste paradoxe : le traitement ici projeté ne servira à rien s'il est bien compris. Il n'aura la moindre utilité que s'il fait l'objet d'un quiproquo. Il aura quoi qu'il en soit contribué à acclimater la vidéo « intelligente » comme moyen de surveillance sans opposition possible, malgré un service rendu qu'on prédit très faible.

La CNIL n'est d'ailleurs pas dupe de l'inutilité possible du système projeté. Après avoir rappelé qu'il doit en principe durer un an, elle précise qu'il devra s'éteindre avant cela si le port du masque cesse d'être obligatoire. Mais elle va plus loin et « recommande (...) que l'impact de tels dispositifs sur la stratégie sanitaire globale soit évalué et documenté de manière régulière, afin que l'efficacité et la pertinence de ceux-ci au cours du temps puissent être évaluées. La Commission recommande que ces analyses lui soient, lorsqu'elles seront disponibles, communiquées afin de lui permettre d'exercer sa mission de contrôle de la conformité de la mise en œuvre des dispositifs projetés ».

Par ailleurs, on peut se demander ce qui empêchera le dispositif d'essaimer hors du secteur des transports. Si la *ratio legis* du texte est la nécessité, pour les pouvoirs publics, de vérifier le respect des gestes barrières dans toutes les situations à risque se produisant sur l'espace public, on ne voit pas ce qui empêcherait qu'on appelle par haut-parleurs au respect des distances sur les quais de Seine ou dans les salles d'attente des administrations, à la suite d'une analyse vidéo automatisée.

Il faut alors conclure cette analyse en rappelant les appels lancés par la CNIL à une réflexion d'ensemble sur l'utilisation de caméras « intelligentes » (V. sur cnil.fr, le 17 juin 2020, « La CNIL appelle à la vigilance sur l'utilisation des caméras dites « intelligentes » et des caméras thermiques »). Cela englobe, mais dépasse la question de la reconnaissance faciale (V. sur cnil.fr, le 15 novembre 2019, « Reconnaissance faciale : pour un débat à la hauteur des enjeux »). La France montre hélas peu d'empressement en la matière. Les propositions européennes en matière d'intelligence artificielle, qui viennent d'être dévoilées, pourraient contribuer à faire progresser ces réflexions (ec.europa.eu, 21 avril 2021, « Une Europe adaptée à l'ère du numérique: La Commission propose de nouvelles règles et actions en faveur de l'excellence et de la confiance dans l'intelligence artificielle »).