



HAL
open science

La reconnaissance faciale aux abords des lycées: quelle faisabilité juridique ?

Emmanuelle Gindre

► **To cite this version:**

Emmanuelle Gindre. La reconnaissance faciale aux abords des lycées: quelle faisabilité juridique?. 2023. <halshs-04288311>

HAL Id: halshs-04288311

<https://shs.hal.science/halshs-04288311v1>

Submitted on 15 Nov 2023

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.



Copyright - All rights reserved

La reconnaissance faciale aux abords des lycées: quelle faisabilité juridique ?

Au lendemain de l'attentat perpétré dans un lycée d'Arras, Laurent Wauquiez appelle de ses vœux un changement de la loi afin de pouvoir tester la reconnaissance faciale aux abords des lycées. Les partisans de cette mesure expliquent en restreindre l'application aux individus suivis pour radicalisation terroriste. Est-ce juridiquement possible ?

Qu'est-ce que la reconnaissance faciale ?

La reconnaissance faciale est définie par la CNIL comme une technologie biométrique, informatique et probabiliste de reconnaissance des visages, de type Machine Learning. Elle s'appuie sur des algorithmes qui recensent les caractéristiques particulières d'un visage pour déterminer un gabarit unique, comparé par le logiciel à d'autres gabarits déjà collectés ou calculés en direct. Le résultat de la comparaison est donné sous la forme d'un pourcentage de correspondance, d'une probabilité.

Utiliser la reconnaissance faciale aux abords des lycées peut impliquer deux types de contrôles préventifs : un dispositif d'accès contrôlé à l'entrée du lycée, et un dispositif de surveillance de l'espace public aux environs du lycée.

Que dit le droit en vigueur ?

Les données biométriques traitées par la reconnaissance faciale étant des données à caractère personnel sensibles, leur collecte et utilisation sont encadrées par la loi informatique et libertés, le RGPD (règlement UE 2016/679) et la directive dite « Police justice » (Directive UE 2016/680).

La loi informatique et libertés pose un principe d'interdiction de traitement de ces données aux fins d'identifier une personne physique de manière unique.

Des exceptions permettent cependant de rendre licite la reconnaissance faciale, notamment si elle a reçu le consentement de la personne concernée (RGPD, art. 9), ou si elle est menée à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière.

Elle doit dans ce dernier cas être réalisée par une autorité compétente, agissant dans un cadre législatif ou réglementaire, et uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée (Loi informatique et libertés, art. 87 et 88). Le traitement des données biométriques doit être autorisé par décret en Conseil d'État pris après avis motivé et publié de la CNIL (Loi informatique et libertés, art. 31).

À ce jour, seuls deux systèmes pérennes ont été autorisés: le module de reconnaissance faciale du Traitement des antécédents judiciaires (TAJ) et celui du système Parafe permettant une authentification sur la base des données contenues dans le passeport lors des passages aux frontières extérieures.

Pourquoi les premières expérimentations de contrôles d'accès biométriques dans les lycées ont été censurées ?

Une délibération du conseil régional de la région PACA (Délib. n° 18-893 du 14 déc. 2018) a autorisé deux lycées de Nice et Marseille à tester un système d'accès par reconnaissance faciale pour l'année 2019, reposant sur le volontariat. Il consistait à comparer les données

biométriques des personnes souhaitant entrer avec la base de données des élèves et personnels du lycée, ainsi qu'à suivre la trajectoire des personnes non identifiées.

La CNIL, saisie par la région, a émis un avis défavorable le 17 octobre 2019, jugeant le dispositif disproportionné au regard des finalités de sécurisation poursuivie. La délibération de la région a finalement été annulée par le tribunal administratif (TA Marseille, 9e ch., 27 févr. 2020, n° 1901249). Ce dernier a considéré que la signature d'un formulaire de consentement était insuffisante pour s'assurer du consentement libre et éclairé propre à justifier une dérogation au principe d'interdiction de la reconnaissance faciale, notamment car « le public visé se trouve dans une relation d'autorité à l'égard des responsables des établissements publics d'enseignement concernés ». Le tribunal administratif a également dénié tout caractère nécessaire du dispositif, celui-ci ne visant pas des objectifs d'intérêt public, et a considéré, comme la CNIL, qu'il était disproportionné, les finalités poursuivies pouvant être atteintes par des moyens plus respectueux des libertés individuelles.

Quels sont les freins juridiques à la mise en œuvre d'un dispositif de reconnaissance faciale en temps réel dans l'espace public ?

Absence d'autorisation législative. En matière de prévention des atteintes à l'ordre public, le code de la sécurité intérieure et la loi du 19 mai 2023 (n° 2023-380 « JOP ») qui l'actualise et le complète, constituent le cadre législatif et réglementaire applicable. Ils n'autorisent pas la mise en œuvre d'un dispositif de reconnaissance faciale en matière de vidéoprotection et comportent des dispositions spéciales interdisant un tel dispositif, aussi bien en temps réel qu'*a posteriori*, dans l'espace public.

Le code de la sécurité intérieure interdit ainsi d'équiper les caméras embarquées à bord de véhicules ou les caméras installées sur des aéronefs tels les drones, de dispositifs de reconnaissance faciale en temps réel (Code de la sécurité intérieure, Art. L. 242-4 et L. 243-3). Ces dispositions n'autorisent pas non plus les services compétents à procéder à l'analyse des images au moyen d'autres systèmes automatisés non embarqués de reconnaissance faciale (Cons. Constit. N° 2021-834 DC du 20 janvier 2022, consid. 30). Le code proscriit également l'utilisation de la reconnaissance faciale dans les traitements de données à caractère personnel des fichiers de renseignement (Code de la sécurité intérieure, Art. R236-2, R. 236-40, R. 236-47, R. 312-85).

La loi n° 2023-380 relative aux jeux Olympiques et Paralympiques de 2024, du 19 mai 2023, autorise quant à elle l'expérimentation des caméras intelligentes capables de détecter des objets ou comportements suspects, mais proscriit également tout système d'identification biométrique en temps réel dans l'espace public, dont la reconnaissance faciale.

Avis réservé des institutions nationales. Les institutions saisies de cette question se montrent réticentes quant à l'autorisation de l'identification biométrique en temps réel. La CNIL considère les dispositifs de reconnaissance faciale comme particulièrement intrusifs et présentant des risques majeurs d'atteinte à la vie privée et aux libertés individuelles (avis du 17 octobre 2019 relatif à l'expérimentation menée en région PACA).

La CNCDH souligne les risques d'une surveillance de masse et « recommande d'interdire l'identification biométrique à distance des personnes dans l'espace public et les lieux accessibles au public, en admettant par exception son utilisation, dès lors que celle-ci est strictement nécessaire, adaptée et proportionnée pour la prévention d'une menace grave et imminente pour la vie ou la sécurité des personnes et celle des ouvrages, installations et établissements d'importance vitale » (avis du 7 avril 2022).

Le Sénat à son tour propose 30 recommandations concernant la reconnaissance biométrique dans l'espace public, avec pour objectif d'écartier le risque d'une société de surveillance (Rapport d'information n° 627 du 10 mai 2022).

L'adoption prochaine d'un cadre européen. Par ailleurs, la réflexion quant à une évolution législative doit s'inscrire dans le cadre des développements européens. La proposition de règlement européen relatif à l'intelligence artificielle est en cours de discussion au Conseil de l'Union européenne et pourrait être adoptée dans les prochains mois (COM/2021/206 final). Ce texte prévoit une interdiction de principe de l'utilisation de systèmes d'identification biométrique à distance «en temps réel» dans des espaces accessibles au public à des fins répressives. Il réserve cependant la possibilité d'une exception pour la prévention d'une menace spécifique, substantielle et imminente pour la vie ou la sécurité physique des personnes physiques, ou la prévention d'une attaque terroriste, dans des conditions strictement encadrées, notamment de nécessité et de proportionnalité (art. 5 §2, 3 et 4 de la proposition de règlement).

Une proposition de loi relative à la reconnaissance biométrique dans l'espace public, appliquant le règlement européen par anticipation, a été adoptée par le Sénat le 12 juin 2023 et transmise à l'Assemblée Nationale. Elle interdit de manière générale la reconnaissance des personnes physiques sur la base de leurs données biométriques en temps réel dans l'espace public et dans les espaces accessibles au public, tout en réservant des cas exceptionnels d'expérimentation pour une durée de 3 ans.

La proposition de loi permettrait ainsi, à titre strictement subsidiaire, l'utilisation expérimentale de la reconnaissance biométrique en temps réel dans l'espace public en matière administrative, par les services de renseignement du premier cercle en charge de la sécurité intérieure, à la seule fin d'assurer la prévention du terrorisme (art. 5). Cette possibilité serait subordonnée à l'existence d'une menace préalablement identifiée, et limitée à la sécurisation des grands événements face à un risque terroriste ou des risques d'atteinte grave à la sécurité des personnes, sur un nombre limité de caméras dédiées et distinctes de celles des systèmes de vidéoprotection. Elle serait soumise à une autorisation du Premier ministre après avis de la commission nationale de contrôle des techniques de renseignement.

Ces dispositions ne permettraient donc pas l'utilisation de la reconnaissance faciale en temps réel pour une surveillance généralisée des abords des lycées qui outrepasserait la seule sécurisation de grands événements. Seule une utilisation *a posteriori* serait possible (art. 4 de la proposition), par les services spécialisés de renseignement, à des fins de prévention du terrorisme, afin de retrouver dans les images de vidéoprotection une personne préalablement identifiée susceptible d'être en lien avec une menace.

Le contrôle du Conseil constitutionnel. La surveillance généralisée des abords des lycées à l'aide d'une technologie de reconnaissance faciale pourrait enfin se heurter aux critères habituellement appliqués par le Conseil constitutionnel en matière de conciliation de la prévention des atteintes à l'ordre public avec les droits et libertés constitutionnels.

Le Conseil constitutionnel exige en effet que la mesure de surveillance concerne « une personne préalablement identifiée susceptible d'être en lien avec une menace ». Il considère donc que le législateur n'opère pas une conciliation équilibrée entre, d'une part, la prévention des atteintes à l'ordre public et, d'autre part, le droit au respect de la vie privée, lorsque la technique de renseignement mise en œuvre touche « un nombre élevé de personnes, sans que leur lien avec la menace soit nécessairement étroit » (décision n° 2017-648 QPC du 4 août 2017 à propos du recueil en temps réel des données de connexion pour la prévention du terrorisme).

La reconnaissance faciale implique de collecter les données biométriques de toutes les personnes circulant dans le périmètre du système de vidéoprotection, puis de les traiter à des fins d'identification, par comparaison avec des bases de données préconstituées. Quand bien même les fichiers interrogés se limiteraient au fichier de traitement des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT), ou aux fiches S du fichier des personnes recherchées, toutes les données biométriques collectées font l'objet du traitement algorithmique, ce qui ne manque pas d'interroger la proportionnalité de l'atteinte au droit au respect de la vie privée.

De même, le Conseil constitutionnel vérifie que le champ de la mesure de surveillance est correctement circonscrit, ce qui interdit une surveillance généralisée et pérenne des abords des lycées.

Autant d'obstacles faisant douter de l'issue du vœu formulé.

Le 23 octobre 2023

Emmanuelle Gindre
Maître de conférences HDR, Université de la Polynésie française