

Expérimentation « portique virtuel »

dans deux lycées de la région Provence-Alpes-Côte d'Azur

Expression de besoin

Depuis novembre 2015, le Ministère de l'Education nationale, de l'Enseignement supérieur et de la Recherche a transmis une série de consignes à appliquer dans les établissements scolaires :

- l'accueil à l'entrée des écoles et établissements scolaires doit être assuré par un adulte ;
- un contrôle visuel des sacs peut être effectué ;
- l'identité des personnes étrangères à l'établissement doit être systématiquement vérifiée.

L'identification de toute personne se présentant à l'entrée d'un lycée se justifie au regard des objectifs de préservation de la sécurité de l'établissement et des personnes qui le fréquentent à titre permanent ou occasionnel.

Cette identification doit être conduite sur trois populations distinctes :

- Les élèves, qui se présentent à l'entrée de l'établissement à heure fixe en très grand nombre (au début de chaque cours potentiellement)
- Les enseignants, les personnels administratifs et techniques,
- Les personnes étrangères à l'établissement (visiteurs : parents d'élèves, intervenant occasionnels...) qui ne sont pas identifiés au préalable.

Compte tenu des flux d'entrée potentiellement très importants et variables dans le temps, il est également indispensable en terme de sécurité des personnes que les personnels en charge du contrôle d'accès soient assistés de manière efficace afin de limiter la durée de présence des personnes à l'entrée du lycée.

Enfin, il est nécessaire que la bonne orientation des visiteurs à l'établissement sur l'accueil soit facilitée et contrôlée, notamment en détectant des déplacements non souhaités.

Finalité du traitement

Le traitement envisagé à titre expérimental consiste à corréler une identité numérique (QR code apposé sur un document, badge, smartphone) avec une identité faciale.

Sa finalité est d'apporter une assistance aux agents en charge du contrôle d'accès au lycée et de l'accueil afin de :

- Faciliter et réduire la durée des contrôles (pour les usagers réguliers du site comme pour les visiteurs) ;
- Lutter contre l'usurpation d'identité ;
- Détecter un déplacement non souhaité et suivre de l'alerte jusqu'à sa résolution.

Objectif de l'expérimentation

L'expérimentation a pour objectif d'évaluer la valeur ajoutée mais aussi les contraintes opérationnelles qu'impliquerait la mise en œuvre d'un dispositif de comparaison faciale au sein d'un lycée. Elle vise notamment à obtenir des éléments pertinents sur l'efficacité des nouveaux dispositifs d'identification

faciale, à éprouver la fiabilité de ces dispositifs dans un espace où circulent de nombreuses personnes, avec des déplacements variés, et à identifier les impacts relatifs à la vie privée des personnes concernées.

Justification du recours à un dispositif biométrique

Le dispositif biométrique s'impose afin de pouvoir authentifier les personnes identifiées par un dispositif classique (porteur de badge, d'un document...).

NB : Ce traitement ne sera pas appliqué au suivi des personnes non identifiées afin de s'assurer de sa bonne orientation.

Les principaux intérêts du dispositif biométrique retenu (comparaison faciale) sont la rapidité de traitement, la fiabilité et le fonctionnement sans contact. L'expérimentation doit permettre de vérifier ces hypothèses en situation réelle.

Le stockage des gabarits en base de données se justifie par la nécessité de gérer dynamiquement (création et suppression) les gabarits.

Description du système d'expérimentation

Le système d'expérimentation est constitué :

- 1- De deux bases de données créées pour l'expérimentation :
 - Une base de données « identité » : Nom, Prénom, Identifiant numérique (au choix) NFC ou QR Code ;
 - Une base de données biométrique qui contient : Identifiant numérique, gabarit biométrique (points de comparaison faciale issus du traitement algorithmique) ; ces gabarits de référence sont issus des images collectées lors de l'enrôlement des personnes volontaires au sein du lycée (lycéens, enseignants, techniques et administratifs) ; cette deuxième base de données ne peut être accessible en lecture que par le processus de comparaison. Aucun administrateur n'y a accès en lecture. Les seuls accès autorisés sont : création d'un champ et suppression d'un champ.
- 2- D'un logiciel permettant de lire l'identifiant numérique sur le lecteur (NFC ou QR Code), de détecter le visage grâce aux caméras couplées au lecteur, d'en extraire un gabarit et de le comparer à la volée avec le gabarit de référence correspondant à l'identifiant numérique.

Les données utilisées pendant le passage de la personne à travers le portique ne seront pas sauvegardées. Il n'y aura pas de fichier journal consultable a posteriori sur les accès au lycée.

L'identification se fait par fusion d'une ou plusieurs identités numériques enregistrée(s) avec une identité biométrique.

La photo du visage est collectée mais n'est pas traitée telle quelle : seuls les points de comparaison faciale déterminés par l'algorithme de comparaison seront comparés avec ceux stockés dans la base de données). Cette photo n'est pas non plus stockée.

Les personnes entrant dans le lycée sont informées par affichage des zones concernées par l'expérimentation et de la possibilité d'emprunter un chemin alternatif non concerné par l'expérimentation.

Un écran mis à disposition des agents en charge du contrôle d'accès et de l'accueil permet de visualiser 3 types de profils :

- Profil « vert »: les personnels autorisés à pénétrer dans l'enceinte du lycée seront représentés par un rectangle vert. Ces personnes seront authentifiées par le dispositif grâce à la fusion de données provenant d'une caméra (identité faciale), du badge magnétique et/ou du smartphone (identité numérique).
- Profil « jaune »: les personnes non identifiées au préalable sont repérées par un dispositif de vidéosurveillance et autorisées à pénétrer dans l'enceinte du lycée pour se présenter à l'accueil ; elles seront représentées par un rectangle jaune, et leur circulation suivie par le système.
- Profil « rouge »: les personnes non identifiées au préalable, autorisées à pénétrer dans l'enceinte du lycée et ne se dirigeant pas dès leur entrée vers l'accueil, seront représentées par un rectangle rouge. Une alerte sera envoyée aux agents d'accueil et de contrôle.

En sortie de portique :

- Les personnes entrantes connaissent leur statut, qui leur est donné sur un écran ;
- Les agents d'accueil et de contrôle connaissent le statut des personnes entrantes par consultation de leur écran de contrôle et peuvent se concentrer uniquement sur ceux présentant des défauts d'identification ou d'authentification.

Cette information peut être rendue sur plusieurs supports (écran de contrôle local, loge, bureaux de direction, etc).

Les alertes seront partagées au sein d'une communauté à définir au travers d'outils de collaboration instantanés multimédias.

Modalités de mise en œuvre

Le traitement projeté est une expérimentation limitée dans le temps. Elle serait mise en œuvre à compter de l'adoption de l'autorisation demandée à la CNIL, pour une durée de six mois, comprenant deux semaines nécessaires pour mettre en place l'expérimentation, 5 mois de test en situation réelle et environ deux semaines d'analyse des résultats de la phase de test.

En pratique, le traitement de comparaison faciale sera réalisé sur les images captées par les caméras installées spécifiquement à l'entrée du lycée et couplées aux lecteurs d'identité numérique.

La base de données biométrique, contenant les gabarits de visages, est constituée grâce à l'enrôlement d'un maximum de 800 lycéens, personnels enseignants, techniciens et administratifs du lycée, participant volontairement à l'expérimentation.

Les personnes volontaires (ou leur représentant légal pour les mineurs) doivent signer préalablement un formulaire de recueil du consentement expliquant la finalité de l'expérimentation, la durée de conservation des données ainsi que la manière d'exercer les droits Informatique et Libertés. Les participants sont également informés qu'ils peuvent à tout moment retirer leur consentement et demander la suppression de leurs gabarits.

Les autres personnes passant dans le champ des caméras ne feront pas l'objet d'un calcul de gabarits : la mise en œuvre de l'expérimentation ne conduit pas au stockage de gabarits de personnes se trouvant dans le champ des caméras mais ne participant pas à l'expérimentation du dispositif biométrique.

Nature des données traitées

Les données collectées sont les photographies des personnels et des lycéens participant à l'expérimentation sur la base du volontariat, à partir desquelles sont produits les gabarits de comparaison, leur nom et prénom (sur le formulaire de consentement uniquement) ainsi qu'un pseudonyme (identifiant numérique unique référant les gabarits).

L'enrôlement des personnes volontaires s'effectuera en présence de ..., sur un poste informatique dans un local sécurisé, à proximité du serveur. Le personnel volontaire est pris en photo sous différents angles (photo d'identité, de face, de biais, etc.) et éventuellement avec un accessoire (lunettes, chapeau...). Les gabarits calculés à partir des photos sont stockés dans une base sécurisée avec un accès restreint et sont associés à un identifiant numérique unique remplaçant les données d'identification des personnes. Le numéro pseudonyme, reporté sur le formulaire de consentement, permettra aux personnes retirant leur consentement d'obtenir la suppression de leur gabarit.

Durée de conservation des données

Les séquences vidéo produites par les caméras déployées pour l'expérimentation ne sont pas conservées au-delà de la fin du processus d'authentification (pour les personnels participant à l'expérimentation du dispositif biométrique), ou du processus d'identification et de suivi (pour les visiteurs).

Les gabarits biométriques du visage des volontaires sont conservés pour la durée de l'expérimentation, à savoir six mois. Leurs photographies ne sont pas conservées.

Destinataires des données

Les destinataires des données sont uniquement et spécifiquement les agents habilités et les personnels ayant souscrit aux engagements de confidentialité requis par le lycée dans le cadre de l'expérimentation.

Par ailleurs, seuls les membres spécifiquement habilités de la direction des systèmes d'information, de la direction de la sûreté et de la direction projet auront accès aux résultats de l'expérimentation.

Information des personnes

Les personnes volontaires du lycée sont informées de la finalité de l'expérimentation, de sa durée et de leurs droits, sur le formulaire de recueil du consentement qu'ils doivent signer préalablement à l'expérimentation.

Le lycée s'engage par ailleurs à avertir les participants en cas d'accès non autorisé à leurs données et à procéder à la suppression immédiate de celles-ci.

Les personnes empruntant les zones concernées par l'expérimentation seront averties par des panneaux d'affichage situés à la périphérie des zones concernées, d'une part, de l'existence de l'expérimentation, de sa finalité et de la manière d'exercer leurs droits auprès du correspondant Informatique et Libertés du lycée et, d'autre part, de l'étendue de la zone concernée, et de la possibilité d'emprunter un chemin alternatif non couvert par l'expérimentation et ne présentant pas de difficultés additionnelles en termes d'accès.

Droits d'accès, de rectification et d'opposition des personnes

L'exercice des droits d'accès, de rectification et d'opposition des personnes s'effectue de manière directe auprès du correspondant Informatique et Libertés du Lycée, ou par défaut du chef d'établissement.

Sécurité des données et la traçabilité des actions

Bilan et retour d'expérience sur l'expérimentation

Le Lycée s'engage à adresser à la CNIL un bilan à la fin de l'expérimentation, dans un maximum de six mois à compter de la fin de l'expérimentation ; il comporte, a minima, les éléments suivants :

- une description des conditions de mise en œuvre technique et opérationnelle du dispositif expérimenté (description des résultats des tests réalisés, pourcentage de réussite des algorithmes de comparaison faciale, éventuels dysfonctionnements liés aux conditions de l'expérimentation, échecs à l'enrôlement lors de la mise en œuvre de la comparaison faciale, etc.) ;
- des éléments de conclusion généraux relatifs aux connaissances et aux perspectives d'exploitation technique, économique ou sociétale de ces apports ;
- une description détaillée de la procédure mise en œuvre pour assurer le plein exercice des droits des personnes ;
- les suites envisagées par le lycée sur la base du bilan effectué (abandon du projet, demande de nouvelle expérimentation, demande d'autorisation de mise en œuvre à titre permanent).