Demande de compléments projet « portiques virtuels » Provence-Alpes-Côte d'Azur – 7/3/2018

A titre liminaire, nous vous informons que s'agissant de dispositifs biométriques à destination du grand public pour des raisons dites « de commodité » telles que l'accélération d'un parcours incluant une authentification, la Commission a établi le principe selon lequel ceux-ci doivent reposer sur : - Un impératif d'authentification manifeste afin de justifier de la pertinence du dispositif, - Le consentement des personnes concernées qui doivent pouvoir opter pour un dispositif d'authentification alternatif, - Le stockage des gabarits sous le contrôle exclusif de celui-ci (via un support individuel ou un chiffrement à sa main).	L'expérimentation n'a pas de notre point de vue pour objet de répondre à un souci de commodité d'accès ou de confort mais à une exigence de sécurité en renforçant le contrôle d'accès aux établissements tout en le fluidifiant. Le lycée n'est pas un espace public ; il doit être « sanctuarisé » et régi par un droit d'accès restreint (lycéens, personnels). Il s'agit donc de : - Prévenir les intrusions extérieures de personnes extérieures à l'établissement ; le cas est très fréquent notamment en agglomération marseillaise ; - Orienter les personnes non identifiées en s'assurant de leur cheminement vers l'accueil. Les nombreux incidents et agressions constatés aussi bien dans l'enceinte du lycée qu'à ses abords, ainsi que le contexte sécuritaire existant depuis les attentats terroristes de 2016, conduisent également à tenter de limiter les temps d'attente et les attroupements à l'extérieur des établissements aux moments de forte affluence (rentrées matinales notamment). NB : les questions relatives au consentement et au stockage sont traitées plus loin
<u>S'agissant du responsable de traitement :</u> Vous indiquez que le plan de mise en sûreté des lycées a été voté par la Région. Il apparait que le projet d'expérimentation soumis à notre Commission s'inscrit dans la cadre de ce plan. Vous mentionnez implicitement par ailleurs que ce projet ferait l'objet d'un complet financement par le conseil régional.	Ce projet s'inscrit en cohérence avec le plan de mise en sûreté des lycées (pièce jointe) voté par la Région en avril 2016. Ce plan se place dans le cadre de la mise en œuvre de la compétence obligatoire de la Région : la gestion des bâtiments et des équipements des lycées. Il comprend notamment le renforcement des clôtures et de la sécurité des accès par la mise en place de sas d'entrée piétons et véhicules et de systèmes de vidéo-protection. Cependant, l'expérimentation est financée entièrement par notre partenaire technologique, la société CISCO, qui en assure également la maîtrise d'œuvre (développement, installation, déploiement, exploitation). Conformément au Code de l'Education (art. R. 421-8), le chef d'établissement est le

La loi n° 78-17 du 6 janvier 1978 modifiée et le Règlement général relatif à la protection des données prévoient que le « responsable du traitement » est l'organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement. Compte tenu de ces éléments, pourriez-vous préciser qui, du conseil régional et/ou de chaque établissement scolaire concerné par l'expérimentation serait qualifié de responsable du traitement envisagé ?	représentant de l'État et l'organe exécutif de l'E.P.L.E.; à ce titre, il détient la responsabilité de décider de la création d'un traitement de données à caractère personnel et de procéder aux formalités liées à sa déclaration auprès de la CNIL. Le « responsable du traitement » est donc bien le chef d'établissement de chacun des deux lycées concernés. Il agit à ce titre comme maître d'ouvrage de l'expérimentation. Le principe de cette expérimentation a été accepté par délibération du conseil d'administration de chacun des deux lycées, qui comprend des représentants de la collectivité régionale, des enseignants, des personnels administratifs, des parents d'élèves et des élèves. Le Conseil régional intervient quant à lui en accompagnement et en suivi de l'expérimentation, dans l'optique d'éventuels investissements ultérieurs, en fonction des résultats et retours d'expérience obtenus.
<u>S'agissant de la finalité du dispositif :</u> Nous vous rappelons que le principe de minimisation implique que les données collectées et traitées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités poursuivies. Dans la mesure où les données biométriques, dont le caractère sensible a été consacré par le « paquet européen de protection des données », ont la particularité d'être uniques et permanentes et leur utilisation doit, de ce fait, faire l'objet d'une vigilance spécifique. Il convient dès lors de s'assurer de la légitimité et de la pertinence de mettre en place un dispositif biométrique plutôt que de maintenir le système d'identification ou d'authentification existant. Vous indiquez que depuis novembre 2015, l'accueil des entrées des établissements scolaires doit être assuré par un adulte et l'identité des personnes étrangères à l'établissement systématiquement vérifiée. Afin que nous puissions mesurer les consignes qui doivent effectivement être mises en œuvre et évaluer, sur cette base, la pertinence du dispositif	Le système d'identification et d'authentification existant repose exclusivement sur l'examen et le contrôle visuel de l'identité des personnes entrantes, au vu des pièces suivantes : carnet de correspondance portant l'identité et la photographie de l'élève, carte professionnelle pour les enseignants et personnels techniques et administratifs, carte d'identité pour les visiteurs. Ce dispositif constitue une réponse au différentiel croissant constaté entre les exigences de sécurisation des entrées dans les établissements et les moyens humains disponibles dans les lycées, dans le cadre des plans successifs de réduction des effectifs dans la fonction publique. Il apporte une assistance aux personnels du lycée, qui peuvent ainsi mieux se concentrer sur les cas nécessitant une intervention humaine, et reporter leur vigilance sur les multiples situations menaçant la sécurité, en augmentant la présence humaine dans les lieux de vie de l'établissement. Les consignes sont décrites dans la circulaire du MEN du 12 avril 2017, la fiche Vigie-Pirate et le guide sécurité des chefs d'établissement (pièces

envisagé, pourriez-vous nous préciser et fournir le document comportant une telle consigne ?	jointes). Ces instructions prévoient notamment les actions suivantes : - Organiser l'accueil à l'entrée de l'établissement scolaire. - Effectuer, si cela est possible, un contrôle visuel des sacs des adultes avec le consentement de leurs propriétaires ; seul un officier de police judiciaire (OPJ) peut contraindre à la fouille des effets personnels. - Vérifier systématiquement l'identité des personnes étrangères à l'établissement. - Demander aux familles de ne pas s'attarder devant les portes d'accès pendant la dépose ou la récupération de leurs enfants. - Assouplir éventuellement les horaires d'entrées et de sorties pour mieux contrôler les flux d'élèves. Il est nécessaire d'éviter que les élèves attendent l'ouverture des portes de l'établissement sur la voie publique. - Signaler tout comportement ou objet suspect.
<u>S'agissant des personnes concernées par l'expérimentation :</u> Vous indiquez que ce dispositif aurait pour but de fiabiliser les contrôles d'entrée dans les lycées, d'en accélérer le processus et de suivre le parcours de visiteurs occasionnels. Vous précisez par ailleurs que la participation à l'expérimentation est volontaire et qu'elle est susceptible de concerner des lycéens, personnels enseignants, techniciens et administratifs du lycée, soit des personnes amenées à se rendre régulièrement dans l'établissement. De tels visiteurs occasionnels sont-ils susceptibles d'être concernés par l'expérimentation ? Si oui, pourriez-vous précisez dans quels cas et sous quelles modalités ?	Les visiteurs occasionnels sont notamment : - Les parents d'élèves ; - Les fournisseurs, prestataires de services. Les visiteurs occasionnels empruntent le même chemin d'entrée que les personnes à authentifier, mais ne présentent pas de support d'identification. Le système biométrique ne s'active que sur présentation d'un support d'identification : les visiteurs occasionnels ne sont de ce fait pas traités par le système biométrique ; leur visage n'est pas photographié, leur gabarit facial n'est ni déterminé ni stocké.

<u>S'agissant du dispositif de suivi des personnes non identifiées :</u> Pourriez-vous préciser les modalités de mise en œuvre du dispositif de détection des déplacements non autorisés de visiteurs de l'établissement qui est mentionné dans le descriptif du projet expérimental en en précisant les liens exacts avec le projet de portique virtuel ?	L'expérimentation comporte : - Un volet biométrique, qui ne concerne que les personnes « identifiées » (lycéens, personnels) ; - Un volet « suivi de trajectoire » (suivi de silhouette sans surveillance de comportement) qui concerne à la fois les personnes « identifiées » et « non identifiées » (visiteurs occasionnels). Les images issues des caméras utilisées par le suivi de trajectoire ne sont pas stockées ; cette partie de l'expérimentation ne nécessite donc pas de signalétique spécifique. Elle se place dans le cadre des déploiements de vidéosurveillance traditionnels.
Comment le dispositif est-il en mesure d'identifier les personnes « non identifiées » sans utilisation du dispositif biométrique ?	L'identification des personnes « non identifiées » est faite par l'agent d'accueil au terme de leur cheminement entre l'entrée et la loge d'accueil de l'établissement.
Le portique expérimenté n'est-il pas exclu du chemin alternatif mis à la disposition des visiteurs, ainsi qu'à toutes les personnes n'ayant pas expressément consenti à la mise en œuvre du dispositif expérimental ?	Les personnes « identifiées » n'ayant pas expressément consenti à la mise en œuvre du dispositif expérimental se verront attribuer un identifiant spécifique ne déclenchant pas le système biométrique mais permettant de s'assurer de leur parcours.
Pourriez-vous en outre indiquer concrètement quel est le chemin alternatif qui sera proposé dans chacun des lycées participant à l'expérimentation ?	Plutôt qu'un chemin physique alternatif, les personnes n'ayant pas consenti expressément à participer à l'expérimentation empruntent le même cheminement mais ne sont pas soumises au système biométrique. Le processus d'entrée est précisé sur un schéma détaillé de circulation reporté sur les plans masse du lycée Ampère (pièce à joindre).
<u>S'agissant des modalités de mise en œuvre du dispositif :</u> Vous indiquez par ailleurs que le stockage des gabarits en base de données se justifie par la nécessité de gérer dynamiquement les gabarits. Pourriez-vous quantifier, de manière non exhaustive, les mouvements de personnel et d'étudiants susceptibles de devoir donner lieu à des créations/suppressions de gabarits ?	Sur la période d'expérimentation (année scolaire), les mouvements de personnel et de lycéens sont estimés pour chaque lycée à : - 600 à 1000 créations/suppressions en début de période ; - 50 créations/suppressions en cours de période.

A cet égard, comme indiqué précédemment, la Commission recommande que les gabarits soient stockés sous le contrôle exclusif de la personne concernée, soit en l'enregistrant sur un support individuel de type badge ou téléphone, soit en le conservant en base en le protégeant par un élément ou un secret que la personne concernée est seule à détenir. Ceci a pour objectif de limiter la constitution de bases de données centralisant un nombre important de gabarits biométriques et, de ce fait, les risques de préjudice en cas de violation de données. Cela vise en effet à éviter tout accès non autorisé aux données et, en cas de compromission, à faire en sorte que celle-ci porte exclusivement sur la seule donnée stockée et non tous les gabarits des personnes concernées par le traitement. Dans la mesure où vous indiquez que le « portique virtuel » serait associé à des moyens classiques d'identification (badges ou codes virtuels sur un téléphone mobile par exemple), ne serait-il pas envisageable de prévoir que le gabarit biométrique utilisé pour la comparaison faciale soit stocké sur un tel support ?	Deux options sont possibles en matière de stockage : OPTION 1 : Stockage en base de données Le système est constitué : 1- De deux bases de données créées pour l'expérimentation : - Une base de données « identité » : le nom, le prénom, un identifiant numérique (au choix NFC ou QR Code) ; - Une base de données « biométrique » qui contient : l'identifiant numérique, un hachage obtenu par cryptage du gabarit biométrique. Les images faciales prises lors de l'enregistrement d'une personne (lycéen, personnel) sont traitées par un algorithme qui détermine le profil biométrique facial. Ce gabarit, composé de points de références, n'est pas conservé en base de données. La seule donnée conservée en base est un hachage, produit par un cryptage irréversible du gabarit biométrique, qui ne permet pas de reconstituer le gabarit initial. Cette deuxième base de données n'est accessible en lecture que par le processus de comparaison. Aucun administrateur humain n'y aura accès en lecture ; les seuls accès autorisés pour cet administrateur sont : la création d'un champ et la suppression d'un champ. 2- D'un système 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, de le passer dans le processus de cryptage et de hachage explicité ci-dessus puis de le comparer à la volée avec la donnée stockée en base correspondant à l'identifiant numérique.

Il est indiqué que le visage des personnes concernées serait détecté à la volée grâce à des caméras, qu'un gabarit en serait extrait afin qu'il soit comparé au gabarit de référence correspondant à l'identifiant numérique lu à partir d'un support (badge ou QR code par exemple). Qu'en est-il des personnes qui passeraient dans le champ des caméras ? Un gabarit biométrique serait-il extrait de l'image de leur visage ? Pourquoi ne pas prévoir un dispositif requérant de présenter son visage devant un lecteur dédié afin de limiter les risques de captation d'images de personnes non volontaires à l'expérimentation ?	OPTION 2 : Stockage sous le contrôle exclusif de la personne sur un support individuel Cela consiste à modifier le système de badges pour leur permettre de stocker un identifiant augmenté d'un gabarit crypté avec une clé individuelle au moyen d'un algorithme unidirectionnel. La clé de cryptage serait stockée en base pour l'identifiant et serait propre à cet identifiant. Cela permettrait d'éviter le risque qu'une clé unique pour toutes les personnes puisse être compromise et permette ainsi de générer de faux badges en masse. La photographie du visage n'est collectée que si la personne fournit volontairement son titre d'identification (badge numérique, QR code…). De cette photographie, il est déterminé dynamiquement un gabarit biométrique du visage (points de comparaison faciale déterminés par l'algorithme utilisé) qui est d'abord crypté puis comparé avec le gabarit crypté stocké dans la base de données ou dans le support individuel). Cette photographie et le gabarit crypté déterminé dynamiquement sont détruits instantanément après l'étape de comparaison. Les gabarits existent exclusivement sous forme cryptée ; l'algorithme de cryptage est unidirectionnel et ne permet donc pas de déterminer le gabarit initial à partir de la donnée cryptée.

<u>S'agissant de l'information et du recueil du consentement des personnes :</u> Nous appelons votre attention sur la nécessité de prévoir des panneaux d'information des visiteurs aux abords de la zone concernée par le « portique virtuel » qui soient suffisamment lisibles et qui comportent toutes les mentions exigées par l'article 32 de la loi du 6 janvier 1978 modifiée.	Des panneaux seront bien prévus à cet effet.
S'agissant des personnes susceptibles d'être concernées par l'expérimentation, pourriez-vous préciser comment sera diffusée l'information et l'appel à participation ?	Les modalités d'information sur l'expérimentation et l'appel à participation seront les suivantes : - Information et approbation du Conseil d'administration du lycée (déjà réalisée) ; - Présentation du projet finalisé au Conseil d'administration du lycée avant son installation ; - Présentation par le proviseur aux usagers (élèves, agents régionaux des lycées, professeurs, parents d'élève) ; - Article dans la revue interne du lycée.
Pourriez-vous également nous fournir le projet de formulaire de recueil du consentement que les volontaires seraient invités à signer ? Nous vous rappelons à cet égard que pour être valable, le consentement des personnes doit être libre. Pour ce faire, la personne doit disposer d'un choix réel, ni contraint, ni influencé par des conséquences négatives qui pourraient résulter de son refus.	Le projet de formulaire de recueil de consentement figure en pièce jointe.
<u>Sur les destinataires</u> Il est indiqué que les alertes sur les personnes entrantes seront « partagées au sein d'une communauté à définir au travers d'outils de collaboration instantanés multimédias ». Pourriez-vous donner plus de précision sur cette « communauté » ?	Le système de report des alertes concerne une « communauté » incluant les personnels d'accueil et les surveillants situés en bout de portique. Si le dispositif de suivi de trajectoire détecte soit une entrée frauduleuse, soit un visiteur qui s'écarterait du trajet vers l'accueil, soit des entrées frauduleuses massives simultanées, cette communauté est étendue à la vie scolaire et au proviseur du lycée, qui juge de l'opportunité de déclencher le système d'alerte prévu dans le plan particulier de mise en sûreté de l'établissement.
Il est également indiqué que les destinataires sont les agents habilités et les personnels ayant souscrit aux engagements de confidentialité requis par le lycée. Pourriez-vous préciser, de manière exhaustive, qui sont exactement ces agents et personnels ?	Ce sont, selon le statut des personnes concernées : a) Le Conseiller principal d'éducation pour les lycéens ; b) L'adjoint gestionnaire du proviseur, qui a par délégation la gestion des agents non enseignants ;

	c) Le proviseur adjoint, qui a par délégation le fonctionnement pédagogique et la relation avec les enseignants.
Le dossier de présentation évoque des responsables du projet, des membres de l'équipe projet. Pourriez-vous préciser qui sont ces personnes ?	L'équipe projet est constituée de la manière suivante : d) Maître d'ouvrage (lycée) : - Le proviseur, responsable de l'ensemble des activités de l'établissement, chef de projet. - Le proviseur adjoint ; - L'adjoint gestionnaire du proviseur ; - L'informaticien du lycée (en support) ; e) Maître d'œuvre (CISCO) : - Le responsable de l'équipe d'innovation en charge du projet ; - Les développeurs du projet. Aucune personne de la société Cisco n'est destinataire des alertes.
Enfin, il est précisé que 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. Pourriez-vous confirmer, d'une part, que ces directions relèvent de la région PACA et, d'autre part, que les résultats auxquels elles auront accès sont anonymes ?	Cette formulation, qui concernait les personnels de la Région associés à l'expérimentation, n'est pas appropriée et doit être revue. Les personnels de la Région ne font en effet pas partie des « destinataires des données » mais auront seulement accès aux résultats généraux de l'expérimentation dans le volet « bilan et retour d'expérience » du projet. Aucune donnée personnelle ne leur sera communiquée dans ce cadre. Ils ne participeront pas directement à l'expérimentation et ne seront pas destinataires des alertes. Ces personnels appartiennent aux services suivants : - La direction des lycées ; - La direction sécurité ; - Le service Smart Région.
<u>Sur les mesures de sécurité</u> Pourriez-vous préciser comment sont composés les mots de passe destinés à assurer l'authentification des utilisateurs ?	Les utilisateurs et administrateurs du système auront accès aux différents éléments de service au travers d'un réseau privé virtuel qui leur permettra dans un premier temps de se connecter au sous réseau du portique. Le portique fonctionnant quasiment en mode autonome, à l'exception des alertes générées qui devront pousser des informations sur des réseaux externes, sera isolé dans sa propre « zone démilitarisée » sécurisée.

	Les logins sur tous les équipements sont uniquement autorisés par des sessions cryptées et uniquement pour des utilisateurs dont les clés publiques sont sur les serveurs. Aucune authentification uniquement pas mot de passe ne sera possible. Des clés cryptées individuelles (openssh ou openssl) seront requises pour chaque utilisateur validé afin de s'identifier et accéder aux serveurs.