**ALEXIS FITZJEAN Ó COBHTHAIGH**
*Avocat au Barreau de Paris*
**5, rue Daunou - 75002 PARIS**
**Tél. 01.53.63.33.10 - Fax 01.45.48.90.09**
**afoc@afocavocat.eu**

# TRIBUNAL ADMINISTRATIF DE MARSEILLE

# REQUÊTE

**POUR :** **1°) L'association « La Quadrature du Net », association soumise à la loi française du 1er juillet 1901, dont le siège est sis 60, rue des Orteaux à Paris (75020), représentée par son président en exercice ;**

**2°) L'association « Ligue des droits de l'Homme » (LDH), association soumise à la loi française du 1er juillet 1901, dont le siège est sis 138, rue Marcadet à Paris (75018), représentée par son président en exercice ;**

**3°) L'association « Fédération des conseils de parents d'élèves des écoles publiques des Alpes-Maritimes » (FCPE 06), association soumise à la loi française du 1er juillet 1901, dont le siège est 6 rue de France, à Nice (06000), représentée par sa présidente en exercice ;**

**4°) Le syndicat « CGT Educ'Action des Alpes-Maritimes », dont le siège est sis 34, avenue Jean Jaurès à Nice (06300), représentée par sa co-secrétaire générale en exercice ;**

**CONTRE :** **La délibération n° 18-893 du 14 décembre 2018 du Conseil régional Provence-Alpes-Côte d'Azur, dont le siège est Hôtel de Région, 27 place Jules Guesde à Marseille (13481), Cedex 20, concernant l'« Expérimentation du dispositif de contrôle d'accès virtuel dans les lycées »**

Les exposants défèrent la délibération susvisée à la censure du tribunal administratif de Marseille. Ils en demandent l'annulation en tous les chefs leurs faisant griefs, par les motifs suivants et tous autres à produire, déduire ou suppléer, au besoin même d'office s'il échet.

## FAITS

1. Le 18 avril 2016, par une délibération n° 16-67 votée en assemblée plénière, le conseil régional de la région Provence-Alpes-Côte d'Azur (ci-après la « région PACA ») a décidé d'approuver un « Plan de mise en sûreté des lycées », qui prévoit notamment « *l'élaboration et la mise en œuvre d'un programme prévisionnel d'équipement et de travaux dans les lycées spécifiques aux problématiques de mise en sûreté des établissements* ».

2. Il y est précisé, dans le sous-titre « La problématique spécifique à la vidéo-protection », que :

> « *Le recensement réalisé récemment par la Région laisse apparaître que 120 lycées sur 181 disposent déjà d'un équipement plus ou moins évolué. Ces installations ont été faites au fil des demandes des établissements. Toutefois la qualité et le niveau d'efficacité des différents systèmes existants restent à vérifier (...) Trois points seront également étudiés :*
> *- la mise en réseau des systèmes de vidéo-protection des établissements aux centres communaux de supervision urbains qui existent dans certaines villes du territoire régional. La démarche se fera territoire par territoire ;*
> *- un soutien régional aux communes afin que leurs systèmes de vidéo-protection puissent se développer de façon à couvrir les abords des établissements ;*
> *- l'utilisation par les lycées des systèmes de vidéosurveillance : de par leur position stratégique en la matière, ce sont dans la plupart des établissements, les personnels d'accueil qui manipulent au quotidien le système de caméras. Toutefois, il est essentiel de créer les conditions techniques pour que les personnels de direction puissent avoir accès par un réseau numérique à un retour permanent des images filmées et piloter l'utilisation du système via l'installation informatique de leur poste de travail* »

3. C'est notamment dans le cadre du « Plan de mise en sûreté des lycées » et par « *l'ambition de l'exécutif de faire de Provence-Alpes-Côte d'Azur la première région Smart Région d'Europe* » que le conseil régional a décidé d'autoriser, le 13 juillet 2016, le président du conseil régional à signer, au nom de la région, un mémorandum avec la société Cisco International Limited (ci-après, la « société Cisco ») (Délibération n° 16-567 du 13 juillet 2016).

4. L'objectif affiché est de « *capitaliser sur des réussites et projets expérimentés sur le territoire de la Métropole NCA [Nice Côte-d'Azur] pour, par exemple, dupliquer et déployer les solutions au niveau de la Région. Quatre axes de collaboration visant à faciliter la transition numérique de la Région ont ainsi été définis : Innovation, Recherche et Éducation, Ville Intelligente, Infrastructure. Ces axes ont pour objectif de déployer de nouveaux services aux citoyens et une infrastructure pour les objets connectés au niveau de la Région* ».

5. Au titre de ce partenariat avec la société Cisco, le 20 octobre 2017, Renaud Muselier, le président du conseil régional de PACA, a adressé un courrier à la Commission nationale de l'informatique et des libertés (ci-après, la « CNIL ») sollicitant ses conseils concernant la mise en place, dans deux lycées de Nice et de Marseille, d'un traitement de reconnaissance faciale à l'entrée de ces établissements (**prod. 1 ; prod. 2**).

6. Il y était notamment énoncé que :

> « *En 2016 et 2017, nous avons investi plus de 20 millions d'euros pour la mise en sûreté de nos lycées et centres de formation des apprentis. (...) Tous les établissements sont désormais équipés d'alarmes différenciées, 1.300 caméras de vidéo-protection ont été installées, 128 médiateurs de sûreté sécurisent les abords des lycées.*
> *Je souhaite amplifier cet effort en expérimentant dans deux lycées de la région un dispositif permettant à la fois de mieux contrôler les entrées dans les lycées, d'accélérer l'entrée des élèves et de suivre le parcours des visiteurs occasionnels. Ce dispositif viendrait en appui des agents en charge du contrôle à l'entrée et de l'accueil au sein des établissements.*
> *Cette expérimentation de portique virtuel associerait des moyens classiques d'identification (badges, codes visuels portés sur un document ou sur un téléphone mobile) à un dispositif biométrique utilisant des technologies de comparaison faciale, seules à même, d'après nos premières investigations, d'apporter une solution fiable et rapide dans un contexte de contrôle d'accès portant sur un nombre potentiellement élevé de personnes (...)* ».

7. En février 2018, la Commission nationale de l'informatique et des libertés (ci-après « CNIL ») a adressé à la région une demande de renseignements complémentaires concernant le projet de « portiques visuels », à laquelle la région a répondu le 7 mars 2018, précisant par ailleurs que :

> « *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* » (**prod. 3**).

8. Le 14 décembre 2018, par une délibération n°18-893, le conseil régional, considérant notamment que « *dans le cadre de l'accord passé entre la Région et la société Cisco International Limited (...) la Région a proposé en 2017 aux lycées Ampère à Marseille et Les Eucalyptus à Nice d'expérimenter un dispositif de contrôle d'accès utilisant des techniques biométriques* », a décidé :
- *d'approuver les termes de la convention d'expérimentation type tripartite Région-lycée-société Cisco International Limited pour la mise en place d'un dispositif de contrôle d'accès par comparaison faciale et de suivi de trajectoire (...)*
- *de lancer cette expérimentation au sein des lycées Ampère à Marseille et Les Eucalyptus à Nice ;*
- *d'autoriser le président du Conseil régional à signer cette convention type tripartite entre la Région, la société Cisco International Limited et chacun des deux lycées mentionnés précédemment* » (Délibération n°18-893 du 14 décembre 2018, **prod. 4**).

9. La délibération comporte une annexe, intitulée « Convention d'expérimentation » détaillant l'expérimentation ainsi que les obligations des différentes parties (ci-après, « la Convention ») (**prod. 5**).

10. Lors du débat sur le vote de cette délibération à l'assemblée plénière du conseil régional, M. Christian Estrosi, rapporteur du projet pour le conseil régional, a par ailleurs déclaré :

> « *Avec ces deux expériences, une fois que nous l'aurons démontré, nous irons très vite sur la généralisation, à partir du réseau de vidéosurveillance déjà existant, sur lequel il ne nous restera plus qu'à mettre le logiciel qui correspond à l'usage de la reconnaissance faciale par rapport aux caméras déjà installées dans nos établissements scolaires* » (Assemblée plénière du conseil régional de PACA, 14 décembre 2018).

11. C'est la délibération attaquée.

## DISCUSSION

### Sur la recevabilité de la présente requête

En ce qui concerne l'intérêt à agir de La Quadrature du Net (LQDN)

12. L'association La Quadrature du Net, première exposante, est recevable à solliciter l'annulation de la délibération attaquée.

13. Aux termes de l'article 3 de ses statuts (**prod.6**), La Quadrature du Net est une association constituée conformément à la loi du 1er juillet 1901 qui a notamment pour objet :
- de mener des « *réflexions, études, analyses et actions* » concernant « *la défense des droits et libertés fondamentaux dans l'espace numérique, la compréhension du fonctionnement d'internet et de l'écosystème numérique* » ;
- « *l'organisation ou le soutien à des événements contribuant à cet objectif* » ;
- « *l'encouragement de l'autonomie des usagers et leur prise de contrôle sur les données les concernant et les dispositifs techniques dont il font usage ou qu'ils rencontrent dans leurs pratiques et leur environnement* » ;
- « *l'étude et la défense des intérêts sociaux, culturels, d'innovation et de développement humain des citoyens. Pour atteindre ce but, elle jouit de la capacité intégrale reconnue par la loi aux Associations et du pouvoir d'ester en justice* » ;
- « *de représenter ses membres dans ses relations : avec d'autres associations ou groupements similaires ou complémentaires, des entreprises, les pouvoirs publics, les instances et les juridictions communautaires et internationales, et dans ce cadre, d'être habilitée à ester en justice et à traiter d'aspects sociaux et réglementaires ou autres au nom de ses membres* ».

14. L'objet général de La Quadrature du Net est donc la défense des droits fondamentaux, non pas uniquement sur Internet, mais dans l'environnement numérique, et notamment la liberté d'expression, la liberté de communication ainsi que le droit au respect de la vie privée et à la protection des données personnelles.

15. Or, en autorisant la mise en œuvre d'un traitement de données biométriques au sein d'un établissement scolaire, avec l'objectif d'étendre ce système, à la fin de son expérimentation, dans l'ensemble des établissements de la région disposant d'un système de vidéosurveillance, la délibération affecte directement l'exercice des droits fondamentaux dans l'environnement numérique. En effet, en violant à plusieurs reprises certaines dispositions du règlement de l'Union européenne

n° 2016/679 « r*elatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* » (ci-après, le « RGPD ») et de la loi n°78-17 du 6 janvier 1978 « *relative à l'informatique, aux fichiers et aux libertés* », la délibération telle que votée par le conseil régional met particulièrement en danger le droit des personnes concernées au respect de leur vie privée, que l'association s'est donnée pour mission de protéger.

16. La Quadrature du Net a manifesté très tôt son opposition au projet de la région d'installer des dispositifs de reconnaissance faciale dans des lycées, soulignant à ce titre, dès le 26 septembre 2018 que « *la reconnaissance faciale risque d'être l'un des outils principaux de la surveillance de masse de la population par les autorités. Si celle-ci est déjà mise en œuvre à grande échelle dans certains États (notamment en Chine), elle se développe à grande vitesse également en France, que ce soit dans nos aéroports, dans nos gares ou dans nos lycées* » (Communiqué de presse de La Quadrature du Net du 26 septembre 2018).

17. Le 11 octobre 2018, l'association envoyait plusieurs demandes d'accès aux documents administratifs à la région PACA et à la CNIL dans le but de se voir communiquer les documents afférents à cette expérimentation. Par ailleurs, le 19 décembre 2018, à la suite de la réception de documents communiqués par la CNIL et en réaction à l'adoption de la délibération par le conseil régional, l'association publiait ces documents et dénonçait dans un communiqué « *la banalisation d'une technologie particulièrement liberticide et qui vise ici à s'étendre à l'ensemble des établissements scolaires de la région* » (Communiqué de presse de La Quadrature du Net du 19 décembre 2018).

18. Enfin, La Quadrature du Net, depuis plus de trois ans, a engagé plusieurs actions contentieuses afin de défendre les droits au respect de la vie privée et à la protection des données personnelles devant le Conseil d'État et le Conseil constitutionnel, notamment contre le décret n°2016-1460 du 28 octobre 2016 « *autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité* ». La Quadrature du Net est ainsi partie dans des affaires pendantes devant la Cour de justice de l'Union européenne à propos de la loi renseignement française et du régime français de conservation généralisé des données de connexion (*cf.* C-511/18 et C-512/18). Elle est également régulièrement conduite à défendre les droits et libertés fondamentaux devant le Conseil d'Etat[1] et le Conseil constitutionnel[2].

[1] CE, 18 octobre 2018, n° 404996 ; CE, 26 juillet 2018, n° 394924, 394922 et 393099 (trois affaires) ; CE, 21 juin 2018, n° 411005 ; CE, 18 juin 2018, n° 406083 ; CE, 25 octobre 2017, n° 411005 ; CE, 17 mai 2017, n° 405792 ; CE, 18 novembre 2016, n°393080 ; CE, 22 juillet 2016, n° 394922 ; CE, 15 février 2016, n° 389140 ; CE, 12 février 2016, n° 388134 ; CE, ord., 27 janvier 2016, n° 396220 ; CE, 9 septembre 2015, n° 393079 ; CE, 5 juin 2015, n° 388134

[2] Cons. const., 30 mars 2018, décision n° 2018-696 QPC ; Cons. const., 2 février 2018, décision n° 2017-687 QPC ; Cons. const., 15 décembre 2017, décision n° 2017-692 QPC ; Cons. const., 4 août 2017, décision

19. Il en résulte que l'intérêt à agir de l'association La Quadrature du Net est en l'espèce certain.

En ce qui concerne l'intérêt à agir de la Ligue des droits de l'Homme (LDH)

20. L'article 1er alinéas 1er et 2 des statuts de la LDH (**prod. 7**), deuxième exposante, énonce que la LDH est « *destinée à défendre les principes énoncés dans les Déclarations des droits de l'Homme de 1789 et 1793, la Déclaration universelle de 1948 et la Convention européenne de sauvegarde des droits de l'Homme et ses protocoles additionnels. Elle œuvre à l'application des conventions et des pactes internationaux et régionaux en matière de droit d'asile, de droit civil, politique, économique, social et culturel* ».

21. L'alinéa 4 poursuit :

> « *Elle lutte en faveur du respect des libertés individuelles en matière de traitement des données informatisées et contre toute atteinte à la dignité, à l'intégrité et à la liberté du genre humain pouvant notamment résulter de l'usage de techniques médicales ou biologiques* »

22. L'article 3 de ces mêmes statuts poursuit :

> « *la Ligue des droits de l'Homme intervient chaque fois que lui est signalée une atteinte aux principes énoncés aux articles précédents, au détriment des individus, des collectivités et des peuples. Ses moyens d'actions sont l'appel à la conscience publique, les interventions auprès des pouvoirs publics, auprès de toute juridiction, notamment la constitution de partie civile lorsque les personnes sont victimes d'atteintes aux principes ci-dessus visés et d'actes arbitraires ou de violences de la part des agents de l'État* ».

23. L'intérêt à agir de la LDH est ainsi patent, s'agissant d'une requête visant à solliciter l'annulation d'une délibération autorisant la mise en œuvre d'un traitement de données biométriques, concernant notamment des mineurs, et ayant pour objet le contrôle d'accès par comparaison faciale à l'entrée des lycées.

n° 2017-648 QPC ; Cons. const., 21 juillet 2017, décision n° 2017-646/647 QPC ; Cons. const., 2 décembre 2016, décision n° 2016-600 QPC ; Cons. const., 21 octobre 2016, décision n° 2016-590 QPC ; Cons. const., 24 juillet 2015, décision n° 2015-478 QPC

En ce qui concerne la « Fédération des conseils de parents d'élèves des écoles publiques des Alpes-Maritimes » (FCPE 06)

24. L'article 2 des statuts de la FCPE 06 (**prod. 8**), troisième exposante, énonce que l'association a notamment pour buts :

> - « *De regrouper l'ensemble des parents d'élève des établissements d'enseignements publics et laïques du département, de formuler en leur nom des vœux sur tout objet concernant les intérêts moraux et matériels de l'enseignement public, des élèves qui le fréquentent et de leurs parents, d'en suivre la réalisation et de veiller à leur application* » ;
> - « *De propager et défendre l'idéal laïque, de promouvoir et faire créer un service national public d'éducation gratuit, respectueux de toutes les familles, de penser sans en privilégier aucune et soucieux d'apporter à chacun des élèves le plus complet épanouissement de sa personnalité et les meilleures chances d'insertion sociale* ».

25. Il est par ailleurs précisé que :

> « *Les moyens d'action de l'association consistent en (…) toutes initiatives propres à faciliter la scolarisation des jeunes, à intéresser les parents à la vie de l'établissement que fréquente leur enfant, à en rechercher et obtenir le meilleur fonctionnent possible (…)* ».

26. Or, au cas présent le dispositif contesté consiste en un outil de reconnaissance faciale placé à l'entrée d'un établissement scolaire et qui pour but de surveiller les élèves et le personnel de l'établissement, a des conséquences aussi bien sur les intérêts moraux de l'enseignement public que sur les élèves qui le fréquentent.

27. Il en résulte que l'intérêt à agir de la FCPE 06 est certain.

En ce qui concerne le syndicat « CGT Educ'Action des Alpes-Maritimes »

28. L'article 3 des statuts du syndicat (**prod. 9**), quatrième exposant, énonce que :

> « *La CGT Educ'Action des Alpes-Maritimes a pour but :*
> *- d'organiser la défense collective et individuelle des syndiqué-e-s et des personnels ;*
> *- de défendre et de promouvoir un enseignement général, technique, professionnel, démocratique et moderne, dans le cadre d'un vaste secteur public décentralisé placé sous la responsabilité essentielle du*

*Ministre de l'Éducation Nationale et couvrant toutes les formations initiale et continue ;*
*- d'établir tous les liens nécessaires de solidarité dans l'action avec l'ensemble des organisations représentatives de travailleurs, de travailleuses, de fonctionnaires, d'enseignant-e-s et au sein de la corporation des liens d'amitié entre tous ses membres et toutes catégories qui la composent* ».

29. En l'espèce, il s'agit, encore une fois, d'un dispositif de surveillance par reconnaissance faciale placé à l'entrée d'un établissement scolaire, concernant aussi bien le personnel de l'établissement, les enseignants que les élèves. Un tel dispositif concerne la défense des personnels et pourrait avoir des conséquences sur l'enseignement général, technique, professionnel, démocratique et moderne que défend et promeut le syndicat.

30. Il en résulte que l'intérêt à agir de la CGT Educ'Action des Alpes-Maritimes est patent.

## Sur l'illégalité de la délibération attaquée

En ce qui concerne l'illégalité externe de la délibération attaquée

**31. En premier lieu**, la délibération est illégale en ce que le conseil régional était incompétent *ratione materiae* pour voter une mesure concernant la sécurité lors de l'entrée dans les lycées.

32. Aux termes de l'article L. 214-6 du code de l'éducation :

> « *La région a la charge des lycées, des établissements d'éducation spéciale et des lycées professionnels maritimes. Elle en assure la construction, la reconstruction, l'extension, les grosses réparations, l'équipement et le fonctionnement (...).*
> *La région assure l'accueil, la restauration, l'hébergement ainsi que l'entretien général et technique, à l'exception des missions d'encadrement et de surveillance des élèves, dans les établissements dont elle a la charge* ».

33. L'article L. 421-3 du code de l'éducation énonce que le chef d'établissement des établissements publics locaux d'enseignement (EPLE) représente l'État au sein de l'établissement.

34. L'article R. 421-10 du code de l'éducation dispose, à ce titre, que :

> « *En qualité de représentant de l'État au sein de l'établissement, le chef d'établissement (...) (3°) Prend toutes dispositions, en liaison avec les autorités administratives compétentes, pour assurer la sécurité des personnes et des biens, l'hygiène et la salubrité de l'établissement* ».

35. A ce titre, la circulaire du 12 avril 2017 relative au renforcement des mesures de sécurité et de gestion de crise applicables dans les écoles et les établissements scolaires énonce, au paragraphe 2.4.1. « *Le rôle des directeurs d'école et des chefs d'établissement* », que :

> « *Les directeurs d'école et les chefs d'établissement veillent au quotidien à la sécurité des élèves et plus généralement des membres de la communauté éducative. En particulier, ils tiennent compte de l'objectif de sécurité pour définir et organiser les tâches qui incombent, à l'intérieur des espaces scolaires, aux agents de l'éducation nationale*

*et aux agents des collectivités territoriales affectés dans l'établissement.* »

36. Enfin, dans son « Guide juridique du chef d'établissement », le ministère de l'éducation nationale précise que si la mission de surveillance est « l*'affaire de tous les personnels de l' EPLE, « la responsabilité première en incombe au chef d'établissement ». Cette mission de surveillance comprend le « régime des entrées et sorties durant le temps scolaire » et le « régime des déplacements d'élèves » ((ministère de l'éducation nationale, « Guide juridique du chef d'établissement* », Février 2009).

37. Par ailleurs, l'article L214-6-1 du code l'éducation prévoit que :

« *La région assure le recrutement et la gestion des personnels techniciens, ouvriers et de service exerçant leurs missions dans les lycées. Ces personnels sont membres de la communauté éducative et concourent directement aux missions du service public de l'éducation nationale dans les conditions fixées aux articles L. 421-23 et L. 913-1* ».

38. L'article L. 421-23 du code de l'éducation précise également que :

« *Le chef d'établissement est assisté des services d'intendance et d'administration ; il encadre et organise le travail des personnels techniciens, ouvriers et de service placés sous son autorité* ».

39. Il en résulte que si la région est compétente pour organiser l'accueil, la restauration, l'hébergement ainsi que l'entretien général et technique des lycées, elle n'est pas compétente concernant les missions d'encadrement et de surveillance des élèves du lycée, mission qui comprend l'encadrement des entrées et sorties des élèves durant le temps scolaire ainsi que tout le régime de leurs déplacements. Cette mission revient au chef d'établissement du lycée.

**40. En l'espèce**, la Délibération, telle qu'adoptée par le Conseil régional énonce notamment que :

- « *L'authentification 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* » ;
- « *la finalité de cette expérimentation 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 occasionnels), lutter contre l'usurpation d'identité et détecter un déplacement non souhaité* ».
- « *Cette expérimentation a pour objectif d'évaluer la valeur ajoutée mais aussi les contraintes opérationnelles qu'impliquerait la mise en œuvre d'un dispositif de contrôle d'accès par comparaison faciale, couplé à un dispositif de suivi de trajectoire, au sein d'un lycée* ».

41. C'est donc au titre de la sécurité du lycée, de la surveillance des élèves et du régime de l'accès à l'établissement, c'est à dire l'entrée et la sortie des élèves, que le conseil régional a voté la délibération attaquée permettant la mise en œuvre du dispositif de reconnaissance faciale.

42. Or, seul le chef d'établissement était compétent pour prendre de telles mesures, comme cela ressort des dispositions précitées du code de l'éducation.

43. Il en résulte que la région n'était pas compétente pour prendre cette Délibération.

44. Par ailleurs, la région ne saurait tirer utilement argument de la circonstance qu'elle se serait bornée à mettre ce dispositif à la disposition des établissements concernés. En effet, eu égard à la chronologie des décisions administratives (notamment les délibérations du conseil régional telles que rappelées ci-dessus), l'initiative de l'installation du dispositif de reconnaissance et de son expérimentation est celle de la région, et non des établissements, et cela dans un domaine qui ne concerne pourtant pas la collectivité territoriale. Il ressort également des échanges avec la CNIL que seule l'administration de la région a supervisé le développement du dispositif et non, encore une fois, le personnel des établissements concernés.

45. De ce chef, déjà, la délibération attaquée ne pourra être qu'annulée.

46**. En second lieu**, la délibération attaquée doit également être annulée en ce qu'elle autorise la mise en œuvre d'un traitement de données biométriques, concernant notamment des mineurs, alors qu'elle n'a été précédée d'aucune analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

47. L'article 35.1 du RGPD dispose que :

« *Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le*

*responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel* ».

48. L'article 35.4 du RGPD dispose que :

« *L'autorité de contrôle établit et publie une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise conformément au paragraphe 1 (...)* »

49. Par ailleurs, le considérant 84 du RGPD dispose que :

« *Afin de mieux garantir le respect du présent règlement lorsque les opérations de traitement sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement devrait assumer la responsabilité d'effectuer une analyse d'impact relative à la protection des données pour évaluer, en particulier, l'origine, la nature, la particularité et la gravité de ce risque. Il convient de tenir compte du résultat de cette analyse pour déterminer les mesures appropriées à prendre afin de démontrer que le traitement des données à caractère personnel respecte le présent règlement. Lorsqu'il ressort de l'analyse d'impact relative à la protection des données que les opérations de traitement des données comportent un risque élevé que le responsable du traitement ne peut atténuer en prenant des mesures appropriées compte tenu des techniques disponibles et des coûts liés à leur mise en œuvre, il convient que l'autorité de contrôle soit consultée avant que le traitement n'ait lieu* ».

50. Enfin, dans ses « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est susceptible d'engendrer un risque élevé aux fins du règlement (UE) 2016/679, le G29 (le « Groupe de travail Article 29 sur la protection des données », l'organe consultatif européen indépendant sur la protection des données et de la vie privée) énonce que :

« *Une AIPD est un processus dont l'objet est de décrire le traitement, d'en évaluer la nécessité ainsi que la proportionnalité et d'aider à gérer les risques pour les droits et libertés des personnes physiques liés au traitement de leurs données à caractère personnel, en les évaluant et en déterminant les mesures nécessaires pour y faire face. Les AIPD sont un outil important au regard du principe de responsabilité, compte tenu de leur utilité pour les responsables du traitement non seulement aux*

*fins du respect des exigences du RGPD, mais également en ce qui concerne leur capacité à démontrer que des mesures appropriées ont été prises pour assurer la conformité au règlement (...). Autrement dit, une AIPD est un processus qui vise à assurer la conformité aux règles et à pouvoir en apporter la preuve* » (p. 4).

51. Il précise également que l'analyse d'impact doit être effectuée « *avant le traitement* (...). *Cette exigence est cohérente avec les principes de protection des données dès la conception et de protection des données par défaut (...). L' AIPD doit être lancée le plus tôt possible dans le cycle de conception du traitement, même si certaines opérations de traitement sont encore inconnues* ».

52. Dans une délibération n° 2018-327 du 11 octobre 2018 « *portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise* », la CNIL a énoncé que parmi les « *opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise* » figure les « *traitements de données biométriques aux fins de reconnaissance des personnes parmi lesquelles figurent des personnes dites « vulnérables » (élèves, personnes âgées, patients, demandeurs d'asile, etc.)* ».

53. Une analyse d'impact est donc nécessaire avant la mise en œuvre d'un traitement de données biométriques aux fins de la reconnaissance d'élèves à l'entrée d'un établissement scolaire.

54**. En l'espèce**, comme rappelé ci-dessus, par sa délibération n°18-893 du 14 décembre 2018, le Conseil régional a décidé de :

« A*pprouver les termes de la convention d'expérimentation type tripartite Région-lycée-société Cisco International Limited pour la mise en place d'un dispositif de contrôle d'accès par comparaison faciale et de suivi de trajectoire, dont un exemplaire est annexé à la présente délibération » ;*
*« Lancer cette expérimentation au sein des lycées Ampère à Marseille et Les Eucalyptus à Nice » ;*
*« Autoriser le président du Conseil régional à signer cette convention type tripartite entre la Région, la société Cisco International Limited et chacun des deux lycées mentionnés précédemment* ».

55. La Convention prévoit par ailleurs que celle-ci « *prend effet à compter de sa notification par la Région et prendra fin le 31 décembre 2019. La notification interviendra au plus tard le 30 juin 2019 (...)* » (Convention, p. 12).

56. La délibération, telle que votée le 14 décembre 2018, constitue donc la première étape dans la mise en œuvre du traitement, alors qu'aucune analyse d'impact n'a été réalisée par la région.

57. Pourtant, la délibération ne fait aucune mention d'une étude d'impact ou du projet d'établir une étude d'impact avant toute mise en œuvre du traitement. Concernant la Convention, s'il est indiqué qu'il revient à la Région de « *piloter les démarches administratives et réglementaires liées au projet, notamment pour la réalisation de l'étude d'impact sur la vie privée* » (p. 4), aucune mention n'est faite d'une étude déjà réalisée ou d'une date quant à la réalisation d'une telle étude.

58. Par ailleurs, par message électronique du 18 décembre 2018, la CNIL nous a indiqué que :

> « *La CNIL a été saisie d'une demande de conseil sur cette expérimentation biométrique basée sur le consentement des personnes. Les personnes n'ayant pas expressément consenti à participer à l'expérimentation feront l'objet d'un contrôle d'accès par les moyens classiques. Il nous a été indiqué qu'une analyse d'impact était en cours de réalisation* » (CNIL, courrier électronique du 18 décembre 2018, prod. 10).

59. Ainsi, en contrariété avec ce qui est prévu dans le RGPD et dans les lignes directrices qui énonce que l'étude doit « *être lancée le plus tôt possible dans le cycle de conception du traitement* », aucune étude d'impact n'a été réalisée au moment du vote de la Délibération, ce vote constituant pourtant la première étape dans la mise en œuvre du traitement.

60. Or, cette étude d'impact aurait dû permettre d'évaluer, comme cela est détaillé dans le RGPD, la nécessité du traitement et les risques qu'il contient pour la vie privée des élèves et du personnel de l'établissement scolaire ainsi que les mesures appropriées à mettre en place pour la protection des personnes concernées. Une telle étude d'impact aurait pu également entraîner la consultation obligatoire de la CNIL.

61. Il ne fait donc aucun doute que l'absence de l'étude d'impact nuit donc à l'information complète de la population et a nécessairement, eu égard notamment aux développements ci-dessous concernant l'illégalité du traitement, influer sur la sens de la décision prise par le conseil régional, au sens de la jurisprudence *Danthony* (*cf.* CE, 23 décembre 2011, *Danthony*, n° 335033 ; voir dans ce sens également : CE, 14 octobre 2011, n° 323257). En particulier, cette étude d'impact aurait permis, une meilleure information de la population et du conseil régional qui aurait été en mesure, conformément aux motifs développés ci-dessous, de constater

notamment l'absence de toute nécessité de ce traitement ainsi que les nombreux risques qu'il contient pour la protection de la vie privée des personnes concernées.

62. A ce titre, il convient de souligner que la demande de conseil effectuée par la région à la CNIL au cours de l'année 2018 ne constitue en aucun cas une étude d'impact au sens du RGPD.

**63. Il en résulte que** la délibération est illégale en ce qu'elle autorise la mise en œuvre d'un traitement de données biométriques concernant des lycéens alors qu'aucune étude d'impact n'a été réalisée au moment de son adoption.

En ce qui concerne l'illégalité interne de la délibération attaquée

**64. A titre liminaire**, il convient de noter que, selon la CNIL :

> « *La Commission a toujours accordé une attention particulière aux dispositifs biométriques qui pouvaient concerner des mineurs, notamment en ce qu'ils sont susceptibles de les habituer aux techniques de surveillance reposant sur des éléments corporels propres à leur identité, conformément à l'article 1er de la loi du 6 janvier 1978 modifiée qui pose le principe que : « L'informatique doit être au service de chaque citoyen. […] Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.*
> *La Commission réaffirme sa vigilance s'agissant de dispositifs concernant des élèves, mineurs de surcroît, et la nécessité d'examiner les traitements qui lui sont soumis au regard des évolutions technologiques et sociologiques qui sont portés à sa connaissance* » (CNIL, Délibération n°2011-388 du 1er décembre 2011 ; voir dans ce sens également : Délibération n°2011-147 du 19 mai 2011).

65. Il en résulte que la légalité de la délibération autorisant le traitement en l'espèce, c'est à dire un traitement de données biométriques concernant l'accès par des mineurs à leur établissement scolaire, doit être évaluée avec une attention particulière.

S'agissant du manque de base légale du traitement autorisé par la délibération attaquée

**66. <u>En premier lieu</u>**, la délibération attaquée méconnaît l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

67. L'article 8.2 de la Convention de sauvegarde des droits de l'homme et libertés fondamentales (ci-après, la « CEDH »), intitulé « Droit au respect de la vie privée et familiale » dispose que :

> « *Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des*

*infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui* »

68. La Cour européenne des droits de l'Homme a ainsi considéré que l'ingérence devait avoir « *une base en droit interne* », être par ailleurs « *suffisamment accessible* », le citoyen devant « *pouvoir disposer de renseignements suffisants, dans les circonstances de la cause, sur les normes juridiques applicables à un cas donné* » et enfin que ne pouvait être considéré comme une loi au sens de la CEDH « *qu'une norme énoncée avec assez de précision pour permettre au citoyen de régler sa conduite ; en s'entourant au besoin de conseils éclairés, il doit être à même de prévoir, à un degré raisonnable dans les circonstances de la cause, les conséquences de nature à dériver d'un acte déterminé* » (CEDH, 25 mars 1983, *Silver et autres c. Royaume-Uni*, n° 5947/72 et a., § 85 à 88).

69. De la même façon, il a été jugé que :

« *Les mots « prévue par la loi » veulent d'abord que la mesure incriminée ait une base en droit interne, mais ils ont trait aussi à la qualité de la loi en cause : ils exigent l'accessibilité de celle-ci à la personne concernée, qui de surcroît doit pouvoir en prévoir les conséquences pour elle, et sa compatibilité avec la prééminence du droit (...). Cette expression implique donc notamment que la législation interne doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à recourir à des mesures affectant leurs droits protégés par la Convention* » (CEDH, 12 juin 2014, *Fernandez Martinez c. Espagne*, n° 56030/07, § 117).

70. Il a ainsi suffi à la Cour européenne de constater que la mesure incriminée n'était pas prévue par la loi pour conclure à la violation de l'article 8 de la Convention (*cf.* CEDH, 8 avril 2003, *M.M. c. Pays-Bas*, n° 39339/98, § 46 ; voir dans ce sens également : CEDH, Guide sur l'article 8 de la Convention - Droit au respect de la vie privée et familiale, §. 14).

71. Il en résulte que toute ingérence dans la vie privée des personnes doit être fondée sur un cadre juridique clair et précis, suffisamment accessible, permettant au citoyen de disposer de renseignements suffisants sur les normes juridiques applicables à un cas donné.

**72. En l'espèce**, la délibération n°18-893 du 14 décembre 2018 a pour objectif d'autoriser « *la mise en place d'un dispositif de contrôle d'accès par comparaison faciale et de suivi de trajectoire* », divisée en en deux volets : « *un volet « contrôle*

*d'accès biométrique* » qui ne concerne que les personnes identifiées (lycées, à l'exclusion des personnels du lycée) et un volet « *suivi de trajectoire* » (sans surveillance de comportement) qui concerne à la fois les personnes « *identifiées* » et « *non identifiées » (visiteurs occasionnels)* ».

73. Or, sur le sujet précis de la reconnaissance faciale, la CNIL, après avoir énoncé que « *les enjeux de protection des données et les risques d'atteintes aux libertés individuelles que de tels dispositifs sont susceptibles d'induire sont considérables* », dont notamment la liberté d'aller et venir anonymement, a elle-même a reconnu l'absence d'un cadre légal adéquat au déploiement de tels traitements :

> « *Il est aujourd'hui impératif que des garde-fous soient prévus afin d'encadrer les finalités pour lesquelles ces dispositifs peuvent être déployés et prévenir tout mésusage des données traitées par leur biais. Or la CNIL constate que le cadre juridique actuel, précis sur certaines technologies (caméras fixes, certains usages de caméras-piétons) et certaines finalités (visionnage « simple » d'images), n'apporte en revanche pas nécessairement de réponse appropriée à l'ensemble des techniques et usages nouveaux mentionnés ci-dessus. Le droit français, qui comporte un certain nombre de règles spécifiques (code de la sécurité intérieure notamment), se trouve en outre renouvelé, pour ces dispositifs, par l'entrée en application du règlement général sur la protection des données et des textes de transposition de la directive dite « police justice » du 27 avril 2016. Un réexamen d'ensemble, à la lumière des nouvelles règles européennes, s'impose.*
> *Aussi, la CNIL appelle d'urgence à un débat démocratique sur cette problématique, et à ce que le législateur puis le pouvoir réglementaire se saisissent de ces questions afin que soient définis les encadrements appropriés, en recherchant le juste équilibre entre les impératifs de sécurisation, notamment des espaces publics, et la préservation des droits et libertés de chacun* » (Communiqué de presse de la CNIL, « La CNIL appelle à la tenue d'un débat démocratique sur les nouveaux usages des caméras vidéo », 19 septembre 2018).

74. Les dispositifs de reconnaissance faciale constituent en effet une ingérence dans la vie privée des personnes concernées, et comporte des enjeux de protection des données et des risques d'atteinte aux libertés individuelles considérables.

75. C'est notamment en raison de ces risques qu'en janvier 2019, 85 organisations non-gouvernementales ont appelé les entreprises Amazon, Microsoft et Google à s'engager à ne pas mettre leurs technologies de reconnaissance faciale à disposition des gouvernements (*cf.* not., Le Monde, « Reconnaissance faciale :

Amazon, Microsoft et Google sommés de ne pas vendre leur technologie aux États », 16 janvier 2019).

76. Pourtant, le traitement en l'espèce, alors qu'il concerne un dispositif de reconnaissance faciale, n'est fondé sur aucun cadre juridique précis concernant la reconnaissance faciale, ou de manière plus générale, les données biométriques.

77. Comme cela est renseigné dans la convention d'expérimentation annexé à la Délibération, les seules bases juridiques sont celles du RGPD et de la loi n° 78-17. Ces textes ne constituent en aucun cas un cadre juridique précis, suffisamment clair et accessible au sens de l'article 8 de la CEDH, ce que souligne la CNIL dans son communiqué de presse du 19 septembre 2018.

78. Il en résulte que la délibération doit être annulée, en ce qu'elle prévoit la mise en œuvre d'un traitement entraînant une ingérence dans le droit à la vie privée des personnes concernées qui n'est pas « *prévue par la loi* ».

79. Ce défaut de base légale se double d'une autre erreur de droit, tirée du caractère non déterminé et illégitime du traitement.

S'agissant du caractère non explicite et illégitime du traitement

**80. <u>En deuxième lieu</u>**, la délibération attaquée méconnaît l'article 5 du RGPD, en ce que les finalités avancées pour justifier le traitement litigieux ne sont ni explicites, ni légitimes.

81. L'article 5 du RGPD intitulé « P*rincipes relatifs au traitement des données à caractère personnel* » énonce que :

> « *Les données à caractère personnel doivent être (...) collectées pour des finalités déterminées, explicites et légitimes* ».

82. Le Considérant 39 précise que :

> « *En particulier, les finalités spécifiques du traitement des données à caractère personnel devraient être explicites et légitimes, et déterminées lors de la collecte des données à caractère personnel. Les données à caractère personnel devraient être adéquates, pertinentes et limitées à ce qui est nécessaire pour les finalités pour lesquelles elles sont traitées* ».

83. Dans son avis 03/2013 sur la finalité du traitement, le G29 a ainsi considéré que les finalités du traitement devaient être explicites, c'est à dire clairement indiquées, expliquées ou exprimées. L'objectif de cette obligation est d'assurer que les finalités soient spécifiées sans imprécision ou ambiguïté quant à leur signification ou intention (Opinion n° 03/2013 « *on purpose limitation* », p. 17).

84. Concernant la légitimité de la finalité, le G29 a également considéré que les finalités devaient être conformes à toutes les dispositions applicables concernant les données personnelles (Opinion n° 03/2013 « *on purpose limitation* », p. 20).

85. Concernant le caractère déterminé de la finalité, le Conseil d'État a ainsi prononcé l'annulation une décision administrative n'ayant pas précisé la finalité d'un traitement de données personnelles (*cf.* CE, 9 novembre 2015, n° 383313).

86. Concernant la légitimité de la finalité, le Conseil d'État a jugé que la finalité poursuivi par un dispositif de vidéo-protection urbaine d'une commune qui avait pour objet d'effectuer une lecture automatisée des plaques d'immatriculation des véhicules circulant sur son territoire était illégitime, au motif que cette finalité n'était pas prévue par la loi (*cf.* CE, 27 juin 2016, n° 385091 ; voir dans ce sens également JCL, Fasc. 932 : Données à caractère personnel - Conditions de licéité des traitements de données à caractère personnel, pt. 18).

**87. En l'espèce**, d'abord, la finalité du traitement dont la délibération permet la mise en œuvre n'est ni explicite, ni déterminée.

88. Ainsi, la délibération n°18-893 du 14 décembre 2018 énonce que « *la finalité de cette expérimentation 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 occasionnels), lutter contre l'usurpation d'identité et détecter un déplacement non souhaité* ».

89. Plus loin, il est affirmé que « *cette expérimentation a pour objectif d'évaluer la valeur ajoutée mais aussi les contraintes opérationnelles qu'impliquerait la mise en œuvre d'un dispositif de contrôle d'accès par comparaison faciale, couplé à un dispositif de suivi de trajectoire, au sein d'un lycée. Elle vise notamment à obtenir des éléments pertinents sur l'efficacité des nouveaux dispositifs de comparaison faciale, à éprouver la fiabilité de ces dispositifs dans un espace où circulent de nombreuses personnes, avec des mouvements massifs (heures de rentrée), et à vérifier leur impact sur le fonctionnement général du lycée et sur le respect de la vie privée des personnes concernées* ».

90. Cette finalité est reprise à l'article 2 « *Présentation de l'expérimentation* ».

91. Par ailleurs, la Convention énonce, dans son article 1 « Objet de la Convention » que :

> « *La présente convention d'expérimentation (« Convention ») a pour objet de définir les conditions dans lesquelles CISCO est autorisée à titre temporaire et expérimental à déployer la solution « contrôle d'accès virtuel » dans le Lycée, et la participation de CISCO aux activités pédagogiques associées à cette expérimentation, qui seront mises en œuvre au sein du Lycée. Il s'agit ici d'expérimenter un nouveau dispositif portant sur le déploiement opérationnel de dispositifs de contrôle d'accès biométrique, en vue d'éventuels développements ultérieurs qui seront alors soumis aux règles de publicité et de mise en concurrence en vigueur* ».

92. Plus loin, la convention énonce, dans son article 4, paragraphe b que :

> « *La finalité du traitement est d'apporter une assistance aux agents en charge du contrôle d'accès au lycée et de l'accueil afin de*
> *- prévenir les intrusions de personnes extérieures à l'établissement en luttant contre l'usurpation d'identité ;*
> *- faciliter et réduire la durée des contrôles à l'entrée ;*
> *- orienter les personnes non identifiées en s'assurant leur cheminent vers l'accueil* »

93. Enfin, lors du débat sur l'adoption de cette délibération, le rapporteur, M. Christian Estrosi a énoncé une nouvelle finalité pour cette expérimentation : « *Avec ces deux expériences, une fois que nous l'aurons démontré, nous irons très vite sur la généralisation, à partir du réseau de vidéosurveillance déjà existant, sur lequel il ne nous restera plus qu'à mettre le logiciel qui correspond à l'usage de la reconnaissance faciale par rapport aux caméras déjà installées dans nos établissements scolaires* ».

94. Ainsi, si la Convention énonce dans son article 4 intitulé « Finalité du traitement » que ce dernier a pour objectif d'apporter une assistance aux agents en charge du contrôle d'accès au lycée, il résulte de la délibération et des autres articles de la Convention que le traitement en l'espèce a en réalité pour finalité, comme la notion d'expérimentation le laisse entendre, d'évaluer « *la valeur ajoutée mais aussi les contraintes opérationnelles qu'impliquerait la mise en œuvre d'un dispositif de contrôle d'accès par comparaison faciale, couplé à un dispositif de suivi de trajectoire, au sein d'un lycée* ».

95. La finalité telle qu'indiquée dans le paragraphe correspondant dans la Convention n'est donc pas celle visée par le traitement en l'espèce. Elle n'est donc

pas, contrairement à ce qui est énoncé dans le RGPD et les lignes directrices du G29 clairement indiquée, expliquée ou exprimée mais au contraire imprécise et surtout ambiguë.

**96. Ensuite**, la finalité de l'expérimentation n'est pas légitime car, dans le cadre de l'extension du dispositif à l'ensemble des établissements scolaires de la région, comme cela est prévu par le conseil régional, le consentement des personnes concernées ne pourrait pas être libre au sens du RGPD.

97. En effet, comme renseigné plus haut, la finalité du traitement est d'évaluer la pertinence du dispositif afin de permettre son application dans l'ensemble des établissements scolaires de la région équipées de systèmes de vidéosurveillance.

98. Or, un tel traitement, étendu massivement à tous les lycées des établissements scolaires de la région, serait manifestement illégal au regard du RGPD et de la loi n° 78-17.

99. En effet, selon l'article 9 du RGPD, le traitement de données biométriques, comme le visage, aux fins d'identifier une personne physique de manière unique est interdit, mis à part des cas précis. Parmi ces possibilités, seulement une pourrait concerner le cas d'espèce :

> « *La personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée* ».

100. C'est d'ailleurs cette base légale qui a été choisie pour l'expérimentation, où la participation des élèves serait fondée sur le volontariat et nécessite le consentement des élèves.

101. Ainsi, concernant le consentement, l'article 4, §11, du RGPD exige que, pour être valide, le consentement soit une « *manifestation de volonté, libre, spécifique, éclairée et univoque* ».

102. L'article 7, §4, du RGPD précise que, « *au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat* ».

103. Le Considérant 32 précise que le consentement devra être « *donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant, par exemple au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale* ».

104. Le considérant 42 précise que « *le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice* ».

105. Par ailleurs, le G29 a clairement précisé le sens de ces dispositions dans ses lignes directrices (WP259), expliquant que « *le RGPD prévoit que si la personne concernée n'a pas un véritable choix, se sent contrainte de consentir ou subira des conséquences négatives si elle ne consent pas, alors son consentement n'est pas valide* ».

**106. Au cas présent**, dans le cas où le dispositif de reconnaissance faciale serait appliqué de façon générale et sans exception, comme cela a été affirmé par le rapporteur du projet, dans l'ensemble des établissements scolaires de la région PACA disposant d'un système de vidéosurveillance, il serait alors impossible d'obtenir des élèves et des personnels concernés un consentement libre au sens du RGPD et des lignes directrices du G29.

107. En effet, les élèves de ces établissements ainsi que le personnel ne pourraient pas refuser de se soumettre au dispositif sans subir des conséquences négatives, au sens du RGPD, comme, par exemple, le fait de ne pas être accepté dans l'établissement scolaire. De la même manière, si l'établissement scolaire demande le consentement des élèves au dispositif au travers d'une charte ou du règlement de l'établissement, les élèves n'auront pas le choix de donner leur consentement pour être scolarisés dans ces établissements.

108. Même au cas où un dispositif de contrôle classique était maintenu en parallèle du système de reconnaissance faciale pour les élèves et personnels n'ayant pas donné leur consentement, celui-ci occasionnerait une différence de traitement préjudiciable, puisqu'il occasionnerait pour les personnes concernées des temps d'attente plus importants et/ou des formalités supplémentaires.

109. Or, ces désagréments - renforcés par la baisse tendancielle des « moyens humains disponibles dans les lycées, dans le cadre des plans successifs de réduction des effectifs dans la fonction publique » qu'évoquait le président de Région dans son courrier à la CNIL - auraient nécessairement pour effet d'exercer une contrainte indirecte sur les personnes concernées en vue d'obtenir leur

consentement, faussant de ce fait le caractère libre, explicite et éclairé de ce dernier du fait de l'existence d'un préjudice résultant du refus de la personne concernée.

110. Le consentement, dans le cas d'une mise en place du dispositif dans les lycées concernés ou dans le cas de son extension à l'ensemble des établissement scolaires, ne pourra donc jamais être libre, au sens du RGPD.

111. Concernant les autres possibilités offertes par l'article 9 justifiant le traitement de données biométriques, aucune ne pourrait concerner l'objectif annoncé par la région de faciliter l'entrée des lycéens dans l'établissement scolaire. Il ne s'agit en particulier pas d'un traitement « *nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre* » (§. g), la région ne détaillant en aucun cas en quoi la facilitation de l'accès à l'établissement scolaire pourrait être un motif d'intérêt public important et le traitement n'étant en aucun cas fondé sur une disposition particulière dans l'Union européenne ou en France.

112. Il en résulte que la finalité du traitement est illégitime, et que la délibération autorisant sa mise en œuvre est donc illégale.

113. De plus, la délibération attaquée est entachée d'une autre erreur de droit, tirée du caractère non adéquat, non pertinent et excessif du traitement qu'elle autorise.

S'agissant de l'absence de caractère adéquat et pertinent, et du caractère manifestement excessif de la collecte des données litigieuse

**114. <u>En troisième lieu</u>**, la délibération attaquée méconnaît l'article 5 du RGPD dès lors que les données collectées et faisant l'objet d'un traitement ne sont ni adéquates, ni pertinentes et, en tout état de cause, manifestement excessives au regard des finalités pour lesquelles elles sont collectées et traitées.

115. L'article 5 du RGPD intitulé « *Principes relatifs au traitement des données à caractère personnel* » énonce que :

> « *Les données à caractère personnel doivent être (...) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* ».

116. A ce titre le Considérant 39 du Règlement énonce que :

« *Les données à caractère personnel ne devraient être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens* »

117. L'article 6 de la loi n° 78-17 dispose que :

« *Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes : (...) 3° [Les données] sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs* ».

118. A ce titre, la CNIL a, à de nombreuses reprises, considéré que la mise en œuvre d'un traitement de données biométriques au sein d'un établissement scolaire afin de contrôler l'accès des élèves à cet établissement ou à un service de cet établissement était excessive au regard de la finalité poursuivie.

119. Ainsi :

- Concernant la constitution d'une base de données biométriques reposant sur la reconnaissance automatique des empreintes digitales et conditionnant l'accès des élèves à la cantine de l'établissement, la CNIL a notamment considéré que « *la constitution de bases de données biométriques y compris d'empreintes digitales peut être justifiée dans certaines circonstances particulières où l'exigence de sécurité et d'identification des personnes est impérieuse, sa mise en œuvre dans un collège, à l'égard notamment de mineurs et aux seules fins de contrôler l'accès à la cantine scolaire est excessive au regard de la finalité poursuivie* » (Délibération n°00-015 du 21 mars 2000 portant avis sur le traitement automatisé d'informations nominatives, mis en œuvre par le collège Jean Rostand de Nice, destiné à gérer à la cantine scolaire par la connaissance des empreintes digitales) ;

- Concernant un dispositif de reconnaissance des empreintes digitales afin de contrôler l'accès à l'établissement par les élèves, la CNIL a notamment considéré que : « *En l'espèce, l'objectif poursuivi par le lycée maritime de Boulogne – Le Portel tendant au contrôle de l'accès à l'établissement et de la présence des élèves, s'il est légitime, n'est pas associé à un fort impératif de sécurité justifiant la conservation dans une base de données des empreintes digitales des élèves et des personnels concernés. La Commission observe que le dispositif n'a pas pour objet le contrôle de l'accès d'un nombre limité de personnes à une zone bien déterminée représentant ou contenant un enjeu majeur dépassant l'intérêt strict de l'organisme. Elle relève également qu'un dispositif reposant sur l'utilisation d'une carte, sans recours à la biométrie, permettrait d'atteindre les objectifs poursuivis par le lycée maritime avec un niveau suffisant de sécurité par rapport aux enjeux. En conséquence, le traitement pris dans son ensemble n'apparaît ni adapté ni proportionné du point de vue de la protection des données personnelles* »

(Délibération n°2008-178 du 26 juin 2008 refusant la mise en œuvre par le lycée maritime de Boulogne – Le Portel d'un traitement de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès des élèves et des personnels à l'établissement) ;

- Concernant un dispositif de reconnaissance de données biométriques afin de contrôler l'accès à un service de restauration scolaire, la CNIL a notamment considéré que *: « L'avantage escompté de la mise en œuvre du dispositif proposé est donc de faciliter la gestion de la cantine, en évitant notamment les inconvénients que peut comporter l'utilisation d'un badge (perte, détérioration, oubli...). Le collège ATURRI, récemment ouvert, voit aussi un intérêt de principe à faire usage des nouvelles technologies. (...) La Commission constate que la reconnaissance du réseau veineux des doigts de la main constitue une technique biométrique plus précise et plus fiable que celle du seul contour de la main. Même si le réseau veineux des doigts de la main ne présente pas, en l'état actuel de la technique, la caractéristique de pouvoir être capturé à l'insu des personnes concernées, toute possibilité de détournement ou de mauvais usage (faille de sécurité, détournement de finalité par le responsable de traitement ou par un tiers...) fait peser un risque sérieux sur l'intégrité et la protection des données biométriques personnelles des utilisateurs qui, de surcroît, s'agissant des élèves, sont des mineurs. Par ailleurs, la Commission relève que la finalité poursuivie pourrait être atteinte par d'autres moyens comme le badge remis à chaque utilisateur ou la technique biométrique du contour de la main. Dès lors, elle considère que le recours à un élément propre à l'identité physique des élèves et aussi fiable que le réseau veineux des doigts de la main aux seules fins d'accéder à un service de restauration scolaire n'est pas pertinent, adéquat et non excessif au regard de la finalité poursuivie* » (Délibération n°2011-147 du 19 mai 2011 refusant la mise en œuvre par le collège ATURRI d'un traitement de données reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle d'accès au service de restauration scolaire).

- Concernant un dispositif de reconnaissance de données biométriques afin de contrôler l'accès à la bagagerie des élèves, la CNIL a notamment considéré que : « *la Commission relève que la finalité poursuivie pourrait être atteinte par d'autres moyens comme un badge remis à chaque utilisateur. Dès lors, elle considère que le recours à un élément propre à l'identité physique des élèves et aussi fiable que le réseau veineux des doigts de la main aux seules fins d'accéder à un service à la bagagerie des élèves et au portillon intérieur n'est pas pertinent, adéquat et non excessif au regard de la finalité poursuivie. Par conséquent, la Commission n'autorise pas le lycée LES IRIS à mettre en œuvre un traitement de données à caractère personnel reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle d'accès à la bagagerie des élèves et au portillon intérieur* » (Délibération n°2011-388 du 1er décembre 2011 refusant la mise en œuvre par le lycée LES IRIS d'un traitement de données reposant sur la

reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle d'accès à la bagagerie des élèves et au portillon intérieur) ;

120. Il est ainsi considéré que :

> « *Il ressort surtout de l'ensemble de ces décisions que les juridictions et la CNIL effectuent un contrôle très attentif de l'application du principe de proportionnalité. De telle sorte qu'elles sanctionnent systématiquement les cas dans lesquels le responsable dont le traitement est mis en cause n'établit pas la preuve certaine que les moyens auxquels il a recours pour le mettre en œuvre sont absolument indispensables et ne se limitent pas seulement à être utiles ou à simplifier sa gestion du traitement* » (Romain Perray, Lexis Nexis, JCL Communication / Fasc. 932 : Données personnelles, §. 36).

121. Il en résulte que pour déterminer le caractère adéquat, pertinent et non excessif d'un traitement de données biométriques, il convient notamment de prendre en compte le caractère nécessaire du dispositif (par exemple, si la finalité poursuivie pouvait être atteinte par d'autres moyens moins invasifs), le cadre dans lequel il est installé (la CNIL apporte un attention particulière aux dispositifs biométriques concernant des mineurs), la possibilité de détournement ou de mauvais usage du dispositif, ou, enfin, la nature des données traitées (par exemple, la CNIL considère que le réseau veineux des doigts de la main est un élément propre à l'identité physique des élèves et nécessite donc un contrôle d'autant plus strict).

**122. En l'espèce**, comme rappelé précédemment, le dispositif en l'espèce concerne notamment la mise en œuvre d'un traitement de reconnaissance faciale à l'entrée d'un établissement scolaire afin « *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 occasionnels), lutter contre l'usurpation d'identité et détecter un déplacement non souhaité* ».

123. Par ailleurs, il est énoncé dans la Convention, dans son article 4, paragraphe b que :

> « *La finalité du traitement est d'apporter une assistance aux agents en charge du contrôle d'accès au lycée et de l'accueil afin de*
> *- prévenir les intrusions de personnes extérieures à l'établissement en luttant contre l'usurpation d'identité ;*
> *- faciliter et réduire la durée des contrôles à l'entrée ;*

*- orienter les personnes non identifiées en s'assurant leur cheminent vers l'accueil* »

124. Comme indiqué précédemment, la finalité réelle du traitement critiqué en l'espèce n'est pas et ne peut pas être « *d'apporter une assistance aux agents en charge du contrôle d'accès au lycée et de l'accueil* » mais d'évaluer l'efficience du traitement pendant l'expérimentation en vue d'éventuels développements ultérieurs.

125. Dans le cas où la finalité réelle du traitement serait d'apporter une assistance aux agents chargés du contrôle d'accès au lycée, alors le traitement en l'espèce serait en tout état de cause inadéquat car limité à une très faible partie des lycéens, c'est à dire seulement ceux ayant donné volontairement leur consentement au traitement, ce qui ne pourrait en aucun cas constituer une assistance aux agents en charge du contrôle.

126. Il en résulte que le traitement ne serait pas pertinent par rapport à la finalité envisagée.

**127. En tout état de cause**, le traitement est de toute évidence excessif par rapport à la finalité envisagée. Il s'agit d'un dispositif de reconnaissance faciale, donc d'un traitement de données biométriques, concernant des mineurs et conditionnant leur accès à l'entrée de l'établissement.

128. Il n'est ainsi indiqué dans la délibération que les éléments suivants : « *Depuis novembre 2015, le Ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche a transmis une série de consignes à appliquer dans les établissements scolaires* » et « *l'authentification 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* ».

129. Dans la Convention, il est par ailleurs indiqué que :

> « *Le dispositif biométrique s'impose afin de pouvoir authentifier de manière forte les personnes identifiées par un dispositif classique (porteur de badge, d'un document...). 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. 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 occasionnels) ;*
*- Lutter contre l'usurpation d'identité ;*
*- Détecter un déplacement non souhaité* » (Convention, p. 3).

130. Aucun de ces éléments ne permet de justifier la nécessité d'un traitement de données biométriques de reconnaissance faciale sur des lycéens.

131. Ni la région ni les lycées concernés n'apportent, contrairement à ce qui est prévu dans le RGPD, d'éléments précis et factuels qui permettraient de déterminer qu'aucun autre moyen n'aurait permis de parvenir à l'objectif visé. Une mise en œuvre du dispositif aurait nécessité des analyses présentant plusieurs dispositifs pour l'entrée des lycéens dans l'établissement et montrant, pour chacun d'eux, notamment son coût et son efficacité. Seule une telle analyse aurait permis de démontrer la nécessité du dispositif de reconnaissance faciale.

132. N'ayant pas démontré cette nécessité, un traitement de données biométriques, en particulier concernant le visage des personnes concernées, sur des mineurs, est évidemment non adéquat et excessif par rapport à la finalité envisagée.

133. **A tous égards,** l'annulation de la délibération est inéluctable.

**<u>Sur l'application de l'article L. 761-1 du code de justice administrative</u>**

134. Compte tenu des frais qu'ils ont été contraints d'engager pour assurer la défense de leurs intérêts dans cette procédure, les exposants demandent qu'une somme 1 024 euros soit mise à la charge de la région PACA sur le fondement des dispositions de l'article L. 761-1 du code de justice administrative.

**PAR CES MOTIFS** et tous autres à déduire, produire ou suppléer au besoin même d'office, les exposants concluent qu'il plaise au tribunal administratif de Marseille :

**ANNULER** la délibération n° 18-893 du 14 décembre 2018 du conseil régional de Provence-Alpes-Côte d'Azur, avec toutes conséquences de droit ;

**METTRE A LA CHARGE** de la région Provence-Alpes-Côte d'Azur la somme de 1 024 euros, en application des dispositions de l'article L. 761-1 du code de justice administrative.

Fait à Paris, le 14 février 2019

**ALEXIS FITZJEAN Ó COBHTHAIGH**
***Avocat au Barreau de Paris***