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

RÉFÉRÉ SUR LE FONDEMENT DE L'ARTICLE L. 521-1 DU CODE DE JUSTICE ADMINISTRATIF

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 M. Bastien Le Querrec, membre du collège solidaire, représentante unique ;**

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.

CONTRE : **La décision prise par la ville de Marseille de mettre en place dans cette ville un dispositif dit de « vidéoprotection intelligente » « d'ici la fin de l'année [2019] », telle que révélée par l'article du journal Télérama du 11 décembre 2019 intitulée « Reconnaissance faciale en France : pourra-t-on y échapper ? ».**

Les exposantes défèrent la décision susvisée à la censure du tribunal administratif de Marseille. Elles en requièrent la suspension immédiate, par les motifs suivants.

FAITS

1. Les associations « La Quadrature du Net » (LQDN) et « Ligue des droits de l'Homme » (LDH), exposantes, sont investies de longue date dans la défense des droits et des libertés, notamment dans l'environnement numérique.

2. Le 31 octobre 2015, la ville de Marseille a publié un avis de marché intitulé « Acquisition d'un dispositif de vidéoprotection intelligente, à Marseille » (*cf.* Pièce n° 1).

3. Le 25 juillet 2016, il a été annoncé sur le site www.francetvinfo.fr, dans un article intitulé « Marseille : des caméras intelligentes », que la ville de Marseille « annonce l'installation d'un système de caméras prédictif, ce qui serait une première dans une grande ville de France »[1]. Il était précisé qu'il s'agissait d'un « logiciel de vidéo surveillance capable de repérer des visages ou d'analyser des allées et venues et de prévenir s'il y a danger ».

4. Le 26 juillet 2016, il était indiqué de la même manière, sur le site www.lepoint.fr, dans un article intitulé « Marseille va s'équiper de caméras prédictives », que « la ville va s'équiper de caméras fonctionnant avec un algorithme d'intelligence artificielle »[2].

5. Le 30 novembre 2018, la ville de Marseille a publié un avis d'attribution du marché intitulé « Dialogue compétitif - acquisition d'un dispositif de vidéoprotection intelligente ». Il y était indiqué que la date de conclusion du marché était le 2 novembre 2018 (*cf.* Pièce n° 2) et que l'entreprise titulaire de ce marché état la société SNEF.

[1] https://www.francetvinfo.fr/faits-divers/criminalite-a-marseille/marseille-des-cameras-intelligentes_1563041.html
[2] https://www.lepoint.fr/high-tech-internet/marseille-va-s-equiper-de-cameras-predictives-26-07-2016-2057208_47.php

Description du dispositif envisagé

6. Le 24 octobre 2019, les exposantes ont eu communication de plusieurs documents contractuels de cet appel d'offre, notamment le « Programme fonctionnel technique » (ci-après « PFT », Pièce n° 3) ainsi que le « Cahier des clauses administratives particulière » (ci-après « CCAP », Pièce n° 4).

7. Le PFT explique que le marché « a pour objet l'acquisition d'un dispositif de VidéoProtection Intelligente (VPI). Son objectif est d'apporter aux opérateurs une aide à l'exploitation de l'outil de vidéoprotection en temps réel et en utilisation différée et de rationaliser le travail de recherche pour optimiser celui du direct » (*cf.* Pièce n° 3, p. 5).

8. Un dispositif de « VidéoProtection intelligente » y est défini comme un « système qui analyse et fusionne les informations provenant de plusieurs capteurs et dont la finalité est de constituer une aide à la décision » (*cf.* Pièce n° 3, p. 6).

9. Plus loin, il est détaillé les fonctions prévues par le déploiement du système dans le cadre de la surveillance en temps réel de l'espace public :

> « La Police Municipale souhaite donc que le système informatique soit capable d'identifier des évènements qui se produisent en temps réel, à l'aide de fonctionnalités, afin d'alerter automatiquement les opérateurs, lesquels pourront réagir en direct et au besoin piloter manuellement d'autres caméras du secteur.
>
> L'attendu de ce projet est d'améliorer l'efficacité du dispositif actuel relativement aux objectifs fixés en termes de fonctionnalités :
>
> - Un traitement automatique des données (valeur ajoutée indépendamment des actions des opérateurs) afin de détecter des anomalies/incidents/faits remarquables)
>
> - Une aide aux opérateurs pour identifier, traiter et suivre des évènements (dont anomalies/ incidents/ faits remarquables)
>
> - La détection d'anomalies non identifiables par un opérateur

- Une aide à la décision

- Un recentrage des opérateurs sur les tâches à valeur ajoutée

- De nouvelles fonctionnalités complémentaires à la sécurité : gestion de l'espace public, analyse des piétons/ véhicules ainsi que des comportements ». (*cf.* Pièce n° 3, p. 12).

10. Il est ensuite énoncé les types d'événements et d'objectifs correspondant à chaque fonctionnalité. Ainsi, une « analyse de scène statique » est mise en œuvre lorsqu'il y a détection d'« objets abandonnées », d'« individus au sol », de « TAG » (comprendre « graffitis »), de « dépose sauvage d'ordure », de « vol/disparation/destruction de mobilier urbain ».

11. Outre la fonctionnalité de « comptage de personnes/véhicules » qui n'est pas détaillée, il est indiqué que le système doit permettre une « détection périmétrique » lors d'un « franchissement de ligne/zone » ou « présences sur zones ». Enfin, l'« analyse de densité de foule » est prévue en cas de « regroupements », d'« attroupement » ou de « surveillance de manifestation sur jauge » (*cf.* Pièce n° 3, p. 13).

12. Plus loin, il est indiqué que, « dans le cadre d'affaires judiciaires », « l'outil doit permettre, après un temps d'analyse de la séquence, de faire des recherches à l'aide de filtres. Les filtres sont : individu (description, avatar, photo), véhicule (type 2 roues, voiture ou camion) » (*cf.* Pièce n° 3, pp. 14 et 15).

13. Enfin, dans le titre « Poste 1 - Fourniture et intégration de fonctionnalités complémentaires », il est indiqué que la ville de Marseille souhaite mettre en place un dispositif de « détection sonore » (explosion, coup de feu, clameur de foule/cris) », de « reconstitution d'évènements (reconstituer le parcours d'un individu ou d'un véhicule à partir des archives de plusieurs caméras) », et de « comportement anormaux » (bagarre/rixe, maraudage, agression) » (*cf.* Pièce n° 3, p. 19).

La mise en place du dispositif

14. Le 18 juin 2019, il était précisé, sur un article du site www.prevention.marseille.fr que « la ville mettra prochainement en place sur son système vidéo des outils d'analyse intelligente permettant d'optimiser les temps de recherche et l'efficacité du visionnage en temps réel (détection de foule, de comportements suspects, détection sonores…) »[3].

15. Enfin, dans un article du 11 décembre 2019 du journal Télérama, intitulé « Reconnaissance faciale en France : pourra-t-on y échapper ? », il est indiqué que « selon nos informations, d'ici la fin de l'année, le CSU phocéen pourra s'appuyer sur un nouveau dispositif de vidéosurveillance intelligente, déployé - pour commencer - sur une cinquantaine de caméras [...] Grâce à cette béquille informatique, les fonctionnaires pourront repérer un objet abandonné, identifier automatiquement une rixe ou suivre le déroulement d'une manifestation, y compris en captant le son alentours. Interrogée, la CNIL n'a jamais entendu parler du projet » (*cf.* Pièce n° 5, p. 5). Cette information a été confirmée aux exposantes le 22 novembre dernier par Caroline Pozmentier, adjointe au maire de Marseille en charge de la sécurité, lors du salon Milipol, qui se tenait à Villepinte (93). Celle-ci a également fait savoir que le prestataire retenu était la société SNEF, sise 87 Avenue des Aygalades dans le 15ème arrondissement de Marseille.

16. Il en résulte que la ville de Marseille a mis en place, dans le courant de la fin de l'année 2019, un dispositif de vidéosurveillance automatisée, dit « vidéoprotection intelligente ».

17. C'est la décision attaquée.

[3] http://prevention.marseille.fr/actualites/remise-de-materiel-la-police-municipale-de-marseille

DISCUSSION

Sur la recevabilité de la présente requête

18. Il convient de relever que les associations exposantes (*i.e.* LQDN et la LDH) sont bien recevables à contester la légalité de la décision attaquée devant le tribunal administratif de Marseille et à en demander la suspension immédiate, sans attendre que le juge du fond se prononce.

En ce qui concerne La Quadrature du Net (LQDN)

19. L'association LQDN est recevable à solliciter la suspension immédiate de la décision attaquée.

20. Aux termes de l'article 3 de ses statuts (*cf.* Pièce n° 6), LQDN est une association constituée conformément à la loi du 1er juillet 1901 qui a notamment pour objet « *la promotion et la défense des droits et des libertés fondamentales dans l'environnement numérique* », et notamment :

> « - la promotion et la défense du droit à l'intimité, à la vie privée, à la protection de la confidentialité des communications et du secret des correspondances et à la protection des données à caractère personnel ;
> - la lutte contre la surveillance généralisée ou politique, d'origine privée ou publique ;
> - la lutte contre l'utilisation d'outils numériques à des fins de surveillance illégitime ; »

21. Il est par ailleurs indiqué que « *La mise en œuvre de cet objet et de ces différents sujets se traduit en pratique par toutes les actions jugées utiles et notamment par (...) la mise en œuvre d'actions juridiques et de contentieux* ».

22. Il est enfin précisé que « *Pour mettre en œuvre ses actions (...) elle jouit de la capacité juridique intégrale reconnue par la loi aux associations et notamment du pouvoir d'ester en justice* ».

23. En autorisant la mise en œuvre d'un traitement de données tel que celui projeté, la décision attaquée affecte directement l'exercice des droits fondamentaux dans l'environnement numérique. En effet, en violant à plusieurs reprises certaines dispositions de la directive de l'Union européenne n° 2016/680 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales » et de la loi n° 78-17 du 6 janvier 1978 « relative à l'information, aux fichiers et aux liberté », tel qu'il sera développé, la décision met particulièrement en danger le droit des personnes concernées au respect de leur vie privée et à la protection contre la surveillance illégitime, que l'association s'est donnée pour mission de protéger.

24. Enfin, LQDN, 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. Elle est régulièrement conduite à défendre les droits et libertés fondamentaux devant le Conseil d'État[4] et le Conseil constitutionnel[5]. LQDN est ainsi partie dans des affaires pendantes devant le Tribunal de l'Union européenne (aff. n° T-738/16), ainsi que 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 (aff. n° C-511/18 et C-512/18). Elle est également partie devant votre tribunal à propos de la délibération prise par le conseil régional PACA concernant la mise en place de portiques de reconnaissance faciale dans deux lycées de la région à Nice et à Marseille[6].

25. En l'espèce, il en résulte que l'intérêt à agir de l'association LQDN est certain.

<u>En ce qui concerne la Ligue des droits de l'Homme (LDH)</u>

[4] 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

[5] 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 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

[6] Affaire enregistrée sous le n° 1901249.

26. L’association LDH est, de même, recevable à solliciter la suspension immédiate de la décision attaquée.

27. Les deux premiers alinéas de l’article 1er des statuts de la LDH (*cf.* Pièce n° 7) énoncent 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 ».

28. 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 ».

29. 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 ».

30. L’intérêt à agir de la LDH est ainsi patent, s’agissant d’une requête visant à solliciter la suspension immédiate d’une décision autorisant la mise en place d’un dispositif de vidéosurveillance automatisée, dit « vidéoprotection intelligente » et visant à installer sur Marseille un système de surveillance algorithmique de l’espace public comprenant notamment un traitement massif de données biométriques.

<u>En ce qui concerne l'acte attaqué</u>

31. L'on sait que « le recours pour excès de pouvoir est recevable dès lors qu'il est dirigé contre un acte administratif, c'est-à-dire une manifestation de volonté unilatérale d'une autorité administrative modifiant l'ordonnancement juridique, quelle que soit la forme que prend cette manifestation » (Gilles Pellissier, « Recours pour excès de pouvoir : conditions de recevabilité », *Répertoire du contentieux administratif*, Dalloz, 2010).

32. Il est par ailleurs acquis qu'une décision administrative susceptible d'un recours juridictionnel et même d'un recours en référé (*cf*. CE, 23 mai 2014, n° 380560) peut notamment être exprimée ou révélée par un communiqué de presse (*cf*. CE, 10 juillet 1992, *Syndicat des médecins libéraux*, n° 105440, Rec. p. 289 ; CE, 25 février 1993, *SIETA*, n° 122993).

33. **En l'espèce**, l'acte attaqué est constitué par la décision prise par la ville de Marseille de mettre en place à Marseille un dispositif dit de « vidéoprotection intelligente » « *d'ici la fin de l'année [2019]* », telle que révélée par l'article de Télérama du 11 décembre 2019 intitulée « Reconnaissance faciale en France : pourra-t-on y échapper ? ».

34. Comme précisé ci-dessus, il est indiqué dans cet article que « *selon nos informations, d'ici la fin de l'année, le CSU phocéen pourra s'appuyer sur un nouveau dispositif de vidéosurveillance intelligente, déployé - pour commencer - sur une cinquantaine de caméras [...] Grâce à cette béquille informatique, les fonctionnaires pourront repérer un objet abandonné, identifier automatiquement une rixe ou suivre le déroulement d'une manifestation, y compris en captant le son alentours. Interrogée, la CNIL n'a jamais entendu parler du projet* » (*cf.* Pièce n° 5, p. 5).

35. Il s'agit donc bien d'une décision administrative qui modifie l'ordonnancement juridique et fait grief aux exposantes dès lors notamment qu'elle met en place un système de vidéosurveillance automatisé sur l'espace public, comprenant un traitement massif de données biométriques, et qui vient ainsi fortement impacter l'exercice des droits et libertés fondamentales protégées par le droit interne et le droit de l'Union européenne.

Sur les conditions fixées par l'article L. 521-1 du code de justice administrative

L'urgence, au sens de l'article L.521-1 du code de justice administrative, est caractérisée

36. Aux termes du 1er alinéa de l'article L. 521-1 du code de justice administrative :

> « *Quand une décision administrative, même de rejet, fait l'objet d'une requête en annulation ou en réformation, le juge des référés, saisi d'une demande en ce sens, peut ordonner la suspension de l'exécution de cette décision, ou de certains de ses effets, lorsque l'urgence le justifie et qu'il est fait état d'un moyen propre à créer, en l'état de l'instruction, un doute sérieux quant à la légalité de la décision.* »

37. La condition d'urgence, à laquelle est subordonnée le prononcé d'une mesure de suspension, est regardée comme remplie lorsque la décision administrative contestée préjudicie de manière suffisamment grave et immédiate soit à un intérêt public, soit à la situation du requérant ou aux intérêts qu'il entend défendre (*cf.* not. CE sect. 19 janvier 2001, *Confédération nationale des radios libres*, n° 228815, Rec. p. 29).

38. Il appartient au juge des référés d'apprécier concrètement, compte tenu des justifications fournies par le requérant, si les effets de la décision administrative contestée sont de nature à caractériser une urgence justifiant que, sans attendre le jugement de la requête au fond, l'exécution de la décision soit suspendue (*cf.* not. CE sect. 28 février 2001, *Préfet des Alpes-Maritimes et société Sud-Est Assainissement*, n° 229562, Rec. p. 109).

39. **En l'espèce,** le préjudice grave et immédiat causé par la décision attaquée aux intérêts qu'entendent défendre les exposantes caractérise l'urgence au sens de l'article L. 521-1 du code de justice administrative.

40. Comme précisé ci-dessus, la décision prise par la ville de Marseille produit des effets hautement préjudiciables, ces derniers étant d'ores-et-déjà constitués et se manifestent dès-à-présent, avant que toute intervention du juge du fond soit

raisonnablement envisageable. Il s'agit d'une décision mettant en place sur la voie publique un système de vidéosurveillance algorithmique, impliquant un traitement massif de données biométriques, dit « vidéoprotection intelligente », y compris en temps réel. Ce dispositif a été mis en place dans les toutes dernières semaines de l'année 2019.

41. L'atteinte engendrée par cette décision aux intérêts que les exposantes entendent défendre, c'est-à-dire la protection des droits et libertés fondamentales, parmi lesquels la protection des données à caractère personnel, est à la fois **grave**, eu égard au traitement massif de données personnelles et notamment de données biométriques, sur la voie publique et **immédiate**, dès lors que, selon l'article du journal Télérama, elle est aujourd'hui déjà en vigueur et que ces effets délétères sont déjà en train de se produire.

42. Il n'est dès lors pas raisonnablement contestable qu'en l'espèce une situation d'urgence, au sens de l'article L.521-1 du code de justice administrative est constituée.

43. **En outre, il existe plusieurs moyens de nature à faire naître, à tout le moins, un doute sérieux sur la légalité de la décision attaquée**

<u>Sur les moyens propres à faire naître un doute sérieux sur la légalité de la décision attaquée</u>

<u>En ce qui concerne le droit applicable</u>

<u>S'agissant de l'applicabilité de la directive n° 2016/680 dite « directive police-justice »</u>

44. La directive n° 2016/680 du 27 avril 2016 dite « directive police-justice » s'applique, selon ses deux premiers articles, à tout traitement de données « *effectué par les autorités compétentes* » aux « *fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces* ».

45. De la même manière, il est précisé que « *la présente directive s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier* ».

46. Les dispositions de la « directive police-justice » ont été partiellement transposées dans la loi n° 78-17 du 6 janvier 1978 modifiée, dans son titre III intitulé : « Dispositions applicables aux traitements relevant de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil ».

47. Il convient par ailleurs de noter que l'article 251-1 du code de la sécurité intérieure dispose que :

> « *Les enregistrements visuels de vidéoprotection répondant aux conditions fixées aux articles L. 251-2 et L. 251-3 sont soumis aux dispositions du présent titre,* ***à l'exclusion de ceux qui sont utilisés dans des traitements automatisés*** *ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques, qui sont soumis à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* ».

48. **En l'espèce**, il ne fait aucun doute au vu de la description du dispositif mis en place par la décision attaquée que ce dispositif inclut des traitements automatisés.

49. Les articles L. 251-2 et L. 251-3 ne sont donc pas applicables en l'espèce, et c'est donc bien la loi n° 78-17 du 6 janvier 1978 modifiée qui s'applique à ces traitements.

50. En outre, concernant la finalité du traitement autorisé par la décision attaquée, celle-ci ressort clairement du PFT : « *La Police Municipale souhaite donc que le systèmes informatique soit capable d'identifier des événements qui se produisent en temps réel ».* L'objectif concret est *« d'apporter aux opérateurs une aide*

l'exploitation de l'outil de vidéoprotection en temps réel, à l'aide de fonctionnalités, afin d'alerter automatiquement les opérateurs, lesquels pourront réagir en direct ». L'objectif final allégué est de « *contribuer à une meilleure sécurisation de l'espace public* ».

51. Parmi les fonctionnalités données en exemples, le PFT vise la lutte contre certaines infractions, dont la « *dépose sauvage d'ordures* », le « *vol/disparition/destruction de mobilier urbain* », la détection sonore d'« *explosion, coup de feu* » ou la détection de « *comportement anormaux : bagarre / rixe, maraudage, agression* »

52. Ainsi, la décision attaquée autorise une autorité compétente à réaliser un traitement automatisé pour lutter contre des infractions et, plus largement, contre des menaces à la sécurité publique.

53. **En conclusion**, la décision attaquée doit respecter la « directive police-justice », telle que transposée dans la loi n° 78-17 du 6 janvier 1978.

<u>En ce qui concerne la nature biométrique de certaines des données traitées</u>

54. L'article 3§13, de la directive police-justice définit les « données biométriques » comme « *les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son* ***identification unique*** ».

55. La notion d'« *identification unique* » n'implique pas nécessairement de révéler l'état civil d'une personne mais, plus largement, de pouvoir individualiser une personne au sein d'un groupe, généralement afin de lui appliquer des mesures spécifiques.

56. Le Comité européen de la protection des données (CEPD, qui réunit l'ensemble des « CNIL » européennes) l'a encore récemment rappelé dans son projet de lignes directrices du 10 juillet 2019 sur le traitement de données personnelles par des appareils vidéos (*cf.* « *Guidelines 3/2019 on processing of personal data through video devices* »[7]).

[7] https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-32019-processing-personal-data-through-video_fr

57. Au point 81, le CEPD donne l'exemple concret d'un traitement permettant de suivre le trajet d'une personne entre plusieurs zones à partir de ses caractéristiques physiques, et sans que cela n'implique de pouvoir en connaître l'état civil. Il s'agit bien ici pour le Comité d'un traitement de données biométriques :

> « *L'article 9 est applicable dans le cas où le responsable du traitement procède au stockage des données biométriques (..) dans le but d'identifier une personne de manière unique. Dans le cas où un responsable du traitement souhaite détecter les personnes qui pénètrent à nouveau dans la zone ou dans une autre zone (...), la finalité serait alors l'identification unique d'une personne physique, ce qui signifie que l'opération relèverait dès le départ de l'article 9 (...). Étant donné que le dispositif utilise des caractéristiques physiques pour détecter des personnes physiques spécifiques revenant dans le champ de la caméra (comme les visiteurs d'un centre commercial) et les suivre, ce dispositif constituerait une méthode d'identification biométrique car il vise la reconnaissance par le recours à un traitement technique spécifique* » (EDPB, Projet de lignes directrices 3/2019, point 81, p. 16 - traduction libre non officielle)

58. **En l'espèce**, une partie du dispositif envisagé prévoit que « *l'outil doit permettre après un temps d'analyse de la séquence, de faire des recherches à l'aide de filtres. Les filtres sont : individu (description, avatar, photo) (...)* » (*cf.* Pièce n° 3, p. 14 et 15).

59. Ces filtres renvoient explicitement à des données physiques et physiologiques dont le caractère biométrique ne fait aucun débat.

60. Une autre partie du dispositif envisagé consiste en « *un traitement automatique de données* » visant à détecter des « *anomalies/incidents/faits remarquables* » afin « *d'alerter automatiquement les opérateurs* ». Les « anomalies » ou « incidents » mentionnés sont notamment la présence d'un « individu au sol », de « TAG », du « vol/disparation/destruction de mobilier urbain ». Le projet mentionne également la « détection sonore » et la « reconstitution d'évènements » pour « le parcours d'un individu » ou la détection de « comportements anormaux » comme les « bagarre / rixe, maraudage, agression » (*cf.* Pièce n° 3, p. 12, 13 et 19).

61. On en comprend que le responsable du traitement définit et enregistre, au sein du traitement, certaines caractéristiques propres à tel ou tel comportement qu'elle souhaite détecter. Ensuite, le traitement analyse les caractéristiques comportementales de l'ensemble des personnes filmées par les caméras affectées au dispositif. Le traitement fait remonter une alerte lorsque, au sein de ce groupe, il est parvenu à individualiser de façon unique une personne dont les caractéristiques *comportementales* correspondent à celles enregistrées et recherchées par la police. Le but de l'alerte est de permettre à la police de prendre une mesure spécifique à l'égard de la personne signalée, telle qu'orienter d'autres caméras pour la suivre en temps réel ou envoyer des agents l'interpeller.

62. De plus, il n'est pas interdit que l'alerte transmette aux agents des caractéristiques *visuelles* permettant de retrouver eux-mêmes la personne. Il est même très probable que ce soit le cas en pratique, puisque cela permettra de faciliter grandement la prise de mesures à l'égard des personnes individualisées par le traitement algorithmique. Qu'il s'agisse de caractéristiques physiques ou physiologiques (*i.e.* âge, taille, corpulence, genre) ou comportementales (*i.e.* couleur des habits, position, démarche), il s'agit encore de permettre à la police d'individualiser une personne de façon unique au sein des autres personnes présentes sur le lieu où la mesure doit être prise.

63. Il en résulte que la police enregistre, au sein du traitement, certaines caractéristiques propres à tel ou tel comportement qu'elle souhaite détecter. Il peut s'agir de caractéristiques comportementales générales (*i.e.* présence du corps au sol, mouvements rapides considérés comme suspects, *etc*.) ou de caractéristiques physiques, physiologiques ou comportementales individualisantes *via* l'application de « filtres » (*i.e.* description, avatar, photo, son de la voix, etc.) permettant de retrouver des données vidéos liées à l'individu en question. À partir de ces données, le traitement automatisé analyse les caractéristiques de l'ensemble des personnes filmées par les caméras affectées au dispositif. **Le traitement peut ensuite faire remonter une alerte lorsqu'il a repéré des caractéristiques comportementales générales correspondent à celles renseignées par la police, ou qu'il a repéré des personnes correspondant aux caractéristiques individualisantes recherchées.** Dans chacun des deux cas, le but du dispositif est bien de permettre à la police de prendre une mesure spécifique à l'égard des personnes détectées, par exemple pour orienter d'autres caméras afin de suivre en temps réel son parcours ou envoyer des agents pour que ces derniers procèdent à une interpellation.

64. S'agissant du cas des alertes déclenchées par la détection de caractéristiques comportementales « générales », il n'est pas exclu que l'alerte automatique liée au dispositif attaqué puisse transmettre aux agents des caractéristiques physiques permettant de retrouver eux-mêmes la personne (*i.e.* photos, description, etc.). Il est même très probable que ce soit le cas en pratique, puisque plusieurs solutions technologiques intègrent ces fonctionnalités dans le but de faciliter la prise de mesures à l'égard des personnes repérées individuellement par le traitement algorithmique. Qu'il s'agisse de caractéristiques physiques ou physiologiques (*i.e.* âge, taille, corpulence, genre) ou comportementales (*i.e.* couleur des habits, position, démarche), il s'agit encore de permettre à la police d'individualiser une personne de façon unique au sein des autres personnes présentes sur le lieu où la mesure doit être prise.

65. Quant aux fonctionnalités de suivi des individus et de reconstitutions a posteriori de leurs parcours, elles impliquent bien que les services de police puissent demander au logiciel de retrouver un individu identifié sur des images enregistrées. Une telle fonctionnalité correspond donc également à un traitement de données biométriques à fin d'identification d'une personne.

66. **En conclusion**, par le fonctionnement même du traitement qui conduit à l'alerte, mais aussi probablement par les informations transmises par l'alerte, la décision attaquée autorise un traitement de données biométriques - un traitement de caractéristiques comportementales, et aussi de caractéristiques physiques et physiologiques, permettant d'identifier une personne de façon unique.

<u>En ce qui concerne l'illégalité externe de la décision attaquée</u>

67. La décision est illégale en ce 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 et qu'elle n'a donné lieu à aucune consultation préalable de l'autorité de contrôle.

68. L'article 27 de la « directive police-justice », intitulé « Analyse d'impact relative à la protection des données » dispose que

> « *1. Lorsqu'un type de traitement, en particulier par le recours aux 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 les libertés des personnes physiques, les États membres prévoient que le responsable du traitement effectue préalablement au traitement une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

2. L'analyse visée au paragraphe 1 contient au moins une description générale des opérations de traitement envisagées, une évaluation des risques pour les droits et libertés des personnes concernées, les mesures envisagées pour faire face à ces risques, les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect de la présente directive, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes touchées. »

69. L'article 28 de la même directive intitulé « Consultation préalable de l'autorité de contrôle » dispose que :

« *Les États membres prévoient que le responsable du traitement ou le sous-traitant consulte l'autorité de contrôle préalablement au traitement des données à caractère personnel qui fera partie d'un nouveau fichier à créer :*

a) lorsqu'une analyse d'impact relative à la protection des données, telle qu'elle est prévue à l'article 27, indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque ; ou

b) lorsque le type de traitement, en particulier, en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées. »

70. Ces obligations sont transposées à l'article 90 de la loi « Informatique et libertés » du 6 janvier 1978 qui dispose que :

« *Si le traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, notamment parce qu'il porte sur des données mentionnées*

au I de l'article 6, le responsable de traitement effectue une analyse d'impact relative à la protection des données à caractère personnel.

Si le traitement est mis en œuvre pour le compte de l'Etat, cette analyse d'impact est adressée à la Commission nationale de l'informatique et des libertés avec la demande d'avis prévue à l'article 33.

Dans les autres cas, le responsable de traitement ou son sous-traitant consulte la Commission nationale de l'informatique et des libertés préalablement à la mise en œuvre du traitement de données à caractère personnel, qui se prononce également dans les délais prévus à l'article 34 :

1° Soit lorsque l'analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable de traitement ne prenait pas de mesures pour atténuer le risque ;

2° Soit lorsque le type de traitement, en particulier en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées ».

71. Dans sa délibération n° 2018-326 du 11 octobre 2018 portant adoption de lignes directrices sur les analyses d'impact relatives à la protection des données (AIPD), la CNIL rappelle que le règlement donne « *trois types de traitements susceptibles de présenter un risque élevé* » et nécessitant une analyse d'impact, dont « *l'évaluation systématique et approfondie d'aspects personnels fondée sur un traitement automatisé et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire* », « *le traitement à grande échelle de données sensibles ou relatives à des condamnations pénales et des infractions* » et « *la surveillance systématique à grande échelle d'une zone accessible au public* ».

72. La CNIL précise que « *le CEPD a identifié neuf critères permettant de caractériser un traitement susceptible d'engendrer un risque élevé* », dont « *croisement ou combinaison de données* », « *surveillance systématique de personnes* » et « *utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles* ».

73. La CNIL considère, par ailleurs, que « *de manière générale, qu'un traitement qui rencontre au moins deux des critères mentionnés ci-dessus doit faire l'objet d'une AIPD* ».

74. Elle ajoute qu'« *[u]ne AIPD faisant apparaître des risques résiduels élevés malgré les mesures envisagées par le responsable de traitement concerné doit être transmise à la CNIL dans les conditions prévues par l'article 36 du RGPD* ».

75. 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 de l'article 29 sur la protection des données, dit « G29 », 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).

76. 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* ».

77. Il en résulte qu'une analyse d'impact et une consultation préalable d'une autorité de contrôle sont nécessaires avant la mise en œuvre d'un traitement ayant recours à de nouvelles technologies étant susceptible d'engendrer un risque élevé pour les

droits et les libertés des personnes physiques. De telles obligations sont d'autant plus nécessaires lorsque les données concernées sont des données biométriques et lorsque le traitement concerne la surveillance à grande échelle d'une zone accessible au public.

78. **En l'espèce**, comme exposé ci-dessus, le dispositif attaqué prévoit l'installation d'un dispositif de vidéosurveillance dit « intelligent ». Plus précisément, le dispositif correspond à un système de « *VidéoProtection Intelligente (VPI)* », son objectif étant « *d'apporter aux opérateurs une aide à l'exploitation de l'outil de vidéoprotection en temps réel et en utilisation différée et de rationaliser le travail de recherche pour optimiser celui du direct* » (*cf.* Pièce n° 3, p. 5).

79. Il est ainsi précisé que « *la police municipale souhaite donc que le système informatique soit capable d'identifier des évènements qui se produisent en temps réel, à l'aide de fonctionnalités, afin d'alerter automatiquement les opérateurs, lesquels pourront réagir en direct et au besoin piloter manuellement d'autres caméras du secteur* » (*cf.* Pièce n° 3, p. 12).

80. A ce titre, le dispositif prévoit notamment « *un traitement automatique des données (...) afin de détecter des anomalies/incidents/faits remarquables* » pouvant consister en l'analyse « d'individu au sol », « comptage de personnes », « détection périmétrique de franchissement de ligne/zone » (*cf.* Pièce n° 3, p. 13).

81. Il permet par ailleurs de « *repérer des visages ou d'analyser des allées et venues et de prévenir s'il y a danger* » (www.francetvinfo.fr, « Marseille : des caméras intelligentes », 25 juillet 2016)[8] et d'« *analyser et fusionner les informations provenant de plusieurs capteurs et dont la finalité est de constituer une aide à la décision* » (*cf.* Pièce n° 3, p. 6).

82. La décision attaquée met donc en œuvre un traitement ayant recours à de nouvelles technologies. Ce traitement, mis en œuvre dans l'espace public à Marseille, permet l'évaluation systématique et approfondie d'aspects personnels fondée sur un traitement automatisé et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire.

[8] https://www.francetvinfo.fr/faits-divers/criminalite-a-marseille/marseille-des-cameras-intelligentes_1563041.html

83. Il concerne également le traitement à grande échelle de données sensibles ou relatives à des condamnations pénales et des infractions et la surveillance systématique à grande échelle d'une zone accessible au public. Il permet également un croisement ou une combinaison de données, une surveillance systématique de personnes et comprend l'utilisation de nouvelles solutions technologiques ou organisationnelles.

84. Enfin, comme précisé plus haut, il s'agit notamment d'un traitement de données biométriques.

85. Il en résulte qu'une analyse d'impact et une consultation préalable de la CNIL étaient obligatoires avant la mise en œuvre du dispositif.

86. Or, comme précisé ci-dessus, il a été publié, le 18 juin 2019, sur le site www.prevention.marseille.fr que « *la ville mettra prochainement en place sur son système vidéo des outils d'analyse intelligente permettant d'optimiser les temps de recherche et l'efficacité du visionnage en temps réel (détection de foule, de comportements suspects, détection sonores…*) »[9]. Le 29 novembre 2018, la ville de Marseille a également publié un avis d'attribution du marché.

87. Cela signifie que l'appel d'offres détaillé ci-dessus a été pourvu, et la mise en place du dispositif parachevé.

88. Les requérantes ont interrogé la ville de Marseille et la CNIL sur l'état d'avancement de l'installation du projet ainsi que sur la communication de l'étude d'impact dont le caractère obligatoire a été exposé précédemment. Aucune réponse n'a malheureusement été obtenue à ce jour (*cf.* Pièce n° 8).

89. Cela étant, dans l'article du 11 décembre 2019 du journal Télérama, intitulé « Reconnaissance faciale en France : pourra-t-on y échapper ? », il est indiqué que « *Interrogée, la CNIL n'a jamais entendu parler du projet.* » (*cf.* Pièce n° 5, p. 5).

90. Ainsi, en contrariété avec ce qui est prévu dans la directive « police-justice », la loi n° 78-17 et dans les lignes directrices qui énoncent que l'étude doit « être lancée le plus tôt possible dans le cycle de conception du traitement », aucune étude

[9] http://prevention.marseille.fr/actualites/remise-de-materiel-la-police-municipale-de-marseille

d'impact ni consultation préalable de l'autorité de contrôle n'a été réalisée au moment du déploiement du dispositif.

91. Or, cette étude d'impact aurait dû permettre d'évaluer, comme cela est détaillé dans la directive « police-justice », la nécessité du traitement et les risques qu'il contient pour la vie privée des personnes se déplaçant dans la ville de Marseille ainsi que les mesures appropriées à mettre en place pour la protection des personnes concernées.

92. En outre, l'absence de l'étude d'impact a non seulement nuit à l'information de la population mais a aussi nécessairement, eu égard notamment aux développements ci-dessous concernant l'illégalité du traitement, influé sur la décision prise par le conseil municipal, 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).

93. Conformément aux motifs développés ci-dessous, une telle étude d'impact aurait conduit la ville de Marseille à notamment constater l'absence de toute nécessité de ce traitement ainsi, que les nombreux risques qu'il emporte pour la protection de la vie privée des personnes circulant sur la voie publique.

94. **Il en résulte que** la décision attaquée est illégale en ce qu'elle autorise la mise en œuvre d'un traitement de données, notamment de données biométriques, au travers d'un système de vidéosurveillance automatisée alors qu'aucune étude d'impact n'a été réalisée au moment de son adoption et qu'aucune consultation préalable de l'autorité de contrôle n'a été conduite.

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

S'agissant du défaut de base légale du traitement autorisé par la décision attaquée

95. **En premier lieu**, la décision attaquée méconnaît l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

96. 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* »

97. 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* » (*cf.* Cour EDH, 25 mars 1983, *Silver et autres c. Royaume-Uni,* n° 5947/72, §§. 85 à 88).

98. 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* » (*cf.* Cour EDH, 12 juin 2014, *Fernandez Martinez c. Espagne*, n° 56030/07, §. 117).

99. 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).

100. 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.

101. Sur son site Web, à la page intitulée « Vidéoprotection : quelles sont les dispositions applicables ? », la CNIL considère que les systèmes de vidéoprotection mis en place sur la voie publique par les autorités publiques pour prévenir des atteintes à la sécurité sont régies par les conditions prévues par l'article L. 251-2 du code de la sécurité intérieure. La CNIL qualifie de « classiques » ces systèmes de vidéoprotection, puisqu'ils ne « *recourent pas à une technologie innovante* ».

102. Il en résulte, *a contrario*, qu'un système qui agrémenterait la captation de la voie publique par une couche applicative ou algorithmique mettant en œuvre un traitement de données supplémentaire, et plus intrusif car automatisé, ne pourra être qualifié de « classique » et devra répondre à un encadrement législatif distinct. Un tel cadre juridique dédié à la vidéosurveillance dite « intelligente » est à ce jour inexistant.

103. À ce titre, dans un courrier du 25 octobre 2019 adressé à la métropole de Saint-Etienne, la CNIL émet un avertissement concernant un dispositif de captation et d'analyse de sons émis sur la voie publique.

104. Elle y affirme notamment que « *quel que soit le régime applicable, il apparaît en tout état de cause que, compte tenu des risques qu'il induit pour les libertés, le recours au dispositif de captation et d'analyse des sons de l'espace public ne saurait trouver un fondement suffisant dans les dispositions législatives d'ordre général de la loi de 1978 ou dans le seul pouvoir réglementaire de la commune de Saint- Étienne ou de Saint-Etienne Métropole. Seule une loi spécifique, adaptée aux caractéristiques techniques et aux enjeux en question, serait de nature à fournir un encadrement adéquat aux traitements envisagés, au titre des "garanties*

fondamentales accordées aux citoyens pour l'exercice des libertés publiques" mentionnée à l'article 34 de la Constitution ».

105. Elle poursuit et décrit que « l*e dispositif de captation et d'analyse de sons de l'espace public dont la mise en œuvre est envisagée, en ce qu'il repose sur une captation continue, systématique et indifférenciée des sons dans l'espace public et peut dès lors capter des conversation privées, apparaît comporter des risques substantiels pour les libertés individuelles, notamment le droit au respect à la vie privée consacré par l'article 2 de la Déclaration des Droits de l'Homme et du Citoyen et par l'article 8 de la Convention européenne de sauvegarde des droits de l'Homme* ».

106. La CNIL insiste sur le fait que « *le couplage même non automatisé, avec le dispositif de vidéoprotection - qui, pour sa part, avait justifié une intervention spécifique du législateur - conduit à renforcer l'intrusivité du système et le niveau de surveillance dont fait l'objet la population vivant, circulant ou travaillant dans la zone concernée. Ce risque d'atteinte au droit au respect à la vie privée est d'autant plus important qu'aucune garantie technique ou juridique ne permet de prévenir, de manière suffisante, une écoute en direct des sons ou un enregistrement de ceux-ci* ».

107. Il en résulte qu'un dispositif de vidéosurveillance ayant recours à une technologie innovante, permettant notamment le traitement de données biométriques à des fins d'individualisation et le couplage avec un système de captation sonore, présente des risques d'atteinte au droit au respect de la vie privée et nécessite un cadre juridique précis, spécifique et adapté.

108. **En l'espèce**, le système de vidéoprotection mis en place par la ville de Marseille repose sur une combinaison de technologies inédite.

109. En effet, le système de vidéoprotection « *analyse et fusionne les informations provenant de plusieurs capteurs et dont la finalité est de constituer une aide à la décision* » (*cf.* Pièce n° 3, p. 6). Plus précisément, le projet de vidéoprotection doit mettre en place :

> « *-un traitement automatique des données (valeur ajoutée indépendamment des actions des opérateurs) afin de détecter des anomalies/incidents/faits remarquables*

- une aide aux opérateurs pour identifier, traiter et suivre des événements (dont anomalies/incidents/faits remarquables)
- la détection d'anomalies non identifiables par un opérateur
- une aide à la décision
- un recentrage des opérateurs sur les taches à valeur ajoutée
- de nouvelles fonctionnalités complémentaires à la sécurité : gestion de l'espace public, analyse des piétons/véhicules ainsi que des comportements » (*cf.* Pièce n° 3, p. 12).

110. De plus, les fonctionnalités complémentaires prévoient notamment la « détection sonore », la « reconstitution d'évènements » ou encore la détection des « comportements anormaux » (*cf.* Pièce n° 3, p. 19).

111. La description de l'appel d'offre démontre donc que le système mis en place par la ville de Marseille dépasse largement les fonctionnalités classiques de « vidéoprotection » prévues par le code de sécurité intérieure. En particulier, les fonctionnalités d'analyse des images et des sons prévues dans le dispositif permettent une surveillance active et automatisée de l'ensemble de la population circulant sur la voie publique, grâce à une aide algorithmique et le traitement de données personnelles, notamment biométriques.

112. Il en résulte que ce système crée de nouvelles ingérences dans le droit à la vie privée des personnes vivant, circulant ou travaillant dans la zone couverte par la vidéoprotection automatisées, et ce, en l'absence de toute base légale spécifique.

S'agissant du caractère excessif et l'absence de caractère adéquat et pertinent du traitement

113. **En deuxième lieu**, le traitement attaqué méconnaît l'article 4 de la « directive police-justice » 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.

114.L'article 4 de la « directive police-justice » dispose que :

« *Les États membres prévoient que les données à caractère personnel sont (...) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées* ».

115.A ce titre, le Considérant 26 de la directive énonce qu'« *[i]l convient notamment de veiller à ce que les données à caractère personnel collectées ne soient pas excessives, ni conservées pendant une durée excédant celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Les données à caractère personnel ne devraient être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens* ».

116.L'article 4 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dispose que « *les données à caractère personnel doivent être (..) Adéquates, pertinentes et, au regard des finalités pour lesquelles elles sont traitées, limitées à ce qui est nécessaire et (...) [pour les traitements relevant de la "directive police-justice"] non excessives* ».

117.Dans son courrier adressé le 25 octobre 2019 à M. Renaud Muselier, président de la région Provence-Alpes-Côte d'Azur, concernant l'installation de portiques de reconnaissance faciale dans deux lycées de la région, la CNIL souligne que le « *traitement de données doit être proportionné, en termes d'impact pour les droits et libertés des personnes, par rapport à la finalité qu'il poursuit et ne porter que sur des données « nécessaire » pour atteindre cette finalité. Il incombe d'ailleurs au responsable de traitement d'évaluer la nécessité et la proportionnalité du traitement envisagé en tenant le plus grand compte de la nature des données traitées, du contexte de sa mise en œuvre et des risques qu'il représente pour les droits et libertés des personnes concernées* ».

118.Elle précise qu'en l'espèce que la finalité de sécurisation et de fluidification des entrées au sein des lycées « *peut incontestablement être raisonnablement atteinte par d'autres moyens* ». Elle en déduit que « *les dispositifs de reconnaissance faciale envisagés (...) ne sont pas conformes aux principes de proportionnalité et de minimisation des données posés, dans la continuité de la loi du 6 janvier 1978, par le RGPD* ».

119.Il en résulte que pour déterminer le caractère adéquat, pertinent et non excessif d'un traitement de données, 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), du contexte de sa mise en œuvre et des risques qu'il représente pour les droits et libertés des personnes concernées, la possibilité de détournement ou de mauvais usage du dispositif, ou, enfin, la nature des données traitées.

120.**En l'espèce**, l'appel d'offre énonce que le système a pour but d'aider la police municipale dans l'exploitation de la vidéoprotection de la ville, dans le cadre des dispositions de l'article L. 2212-1 et 2 du code général des collectivités territoriales.

121.Deux besoins principaux sont distingués en fonction du mode d'exploitation, la surveillance en direct de l'espace public et l'exploitation en différé dans le cadre d'affaires judiciaires.

122.Tout d'abord, la surveillance de l'espace public est justifiée par le fait que :

> « *Les opérateurs ne peuvent pas visualiser l'ensemble des flux. Dès lors, si un fait remarquable se produit dans le champ de vision d'une caméra non visualisée, les opérateurs n'en sont pas avertis et ne peuvent pas traiter en direct l'événement (...). La Police Municipale souhaite donc que le système informatique soit capable d'identifier des évènements qui se produisent en temps réel, à l'aide de fonctionnalités, afin d'alerter automatiquement les opérateurs, lesquels pourront réagir en direct et au besoin piloter manuellement d'autres caméras du secteur* » (*cf.* Pièce n° 3, p. 12).

123.Ensuite, pour l'exploitation en différé, il est expliqué que « *Les vidéos peuvent être réquisitionnées. La recherche d'évènements à posteriori est une tâche complexe et chronophage. La Police Municipale souhaite se munir d'outils informatiques permettant d'améliorer à la fois la durée et la pertinence des recherches sur archives* » (*cf.* Pièce n° 3, p. 14).

124.C'est au titre de ces deux objectifs que le dispositif prévoit le traitement d'un grand nombre de données, notamment biométriques. Comme rappelé ci-dessus, le dispositif prévoit la détection par « *traitement automatique de données* » de plusieurs « *anomalies / incidents / faits remarquables* » dont « *objets abandonnés* », « individu au sol », « TAG », « dépose sauvage d'ordures »,

« *vol/disparition/destruction de mobilier urbain* ». Le dispositif prévoit également le « *comptage de personnes/véhicules* », « *l'analyse de densité de foule : regroupements, attroupement, surveillance de manifestation* », la « détection sonore » (explosion, coup de feu, clameur de foule), la « reconstitution d'évènements » (reconstituer le parcours d'un individu ou d'un véhicule à partir des archives de plusieurs caméras) et la détection de « comportements anormaux (bagarre / rixe, maraudage, agression) ». Il est par ailleurs indiqué que le dispositif doit permettre une analyse de séquences vidéos par filtres et que « les filtres sont : individu (description, avatar, photo) » (*cf.* Pièce n° 3, p. 12, 13 et 19).

125. Il n'est à aucun moment indiqué en quoi un tel traitement de données, pratiqué sur l'espace public à Marseille, est adéquat, pertinent et manifestement non-excessif par rapport à l'objectif poursuivi, c'est-à-dire strictement nécessaire au regard de la finalité. La ville de Marseille n'apporte ainsi, contrairement à ce qui est requis par la « directive police-justice » et par les dispositions de la loi n° 78-17, aucun élément précis ou factuel qui permettrait de déterminer qu'aucun autre moyen n'aurait permis de parvenir à l'objectif visé.

126. Au contraire, la ville de Marseille se borne à indiquer que le dispositif ne constitue qu'une « aide » apportée à la police municipale, et que « l'attendu de ce projet est d'améliorer l'efficacité du dispositif actuel ».

127. **Il en résulte que**, la ville de Marseille n'ayant pas démontré la nécessité des traitements induits par le dispositif de vidéosurveillance « intelligente », ces traitements sont non adéquats et excessifs par rapport à la finalité envisagé.

S'agissant du non-respect des conditions de légalité d'un traitement de données biométriques

128. **En troisième lieu**, la décision est illégale en ce qu'elle met en place un dispositif entraînant notamment le traitement de données biométriques sans respecter les conditions de légalité d'un tel traitement.

129. L'article 10 de la directive « police-justice » intitulé « *Traitement portant sur des catégories particulières de données à caractère personnel* » indique que :

> « *Le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions*

politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, et le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique est autorisé uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et uniquement:

a) lorsqu'ils sont autorisés par le droit de l'Union ou le droit d'un État membre;

b) pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique; ou

c) lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée ».

130. Par ailleurs, l'article 88 de la loi n° 78-17 prévoit de la même façon que « *Le traitement de données mentionnées au I de l'article 6 est possible uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et soit s'il est autorisé par une disposition législative ou réglementaire, soit s'il vise à protéger les intérêts vitaux d'une personne physique, soit s'il porte sur des données manifestement rendues publiques par la personne concernée* ».

131. Il en résulte que le traitement de données biométriques n'est possible qu'en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et soit s'il est autorisé par une disposition législative ou réglementaire, soit s'il vise à protéger les intérêts vitaux d'une personne physique, soit s'il porte sur des données manifestement rendues publiques par la personne concernée.

132. **En l'espèce**, comme indiqué ci-dessus, il ne fait aucun doute que la décision attaquée concerne la mise en place d'un traitement de données, notamment de données biométriques.

133. *Premièrement*, par le fonctionnement même du traitement qui conduit à l'alerte, mais aussi par les informations transmises lorsque des alertes sont générées par le

dispositif à destination des opérateurs humains, la décision attaquée autorise un traitement de données biométriques - un traitement de caractéristiques physiques, physiologiques ou comportementales, permettant d'identifier une personne de façon unique.

134.*Deuxièmement*, de manière encore plus explicite, la description du dispositif prévoit que « *l'outil doit permettre après un temps d'analyse de la séquence, de faire des recherches à l'aide de filtres. Les filtres sont : individu (description, avatar, photo) (...)* » (*cf.* Pièce n° 3, p. 19).

135.Dès lors que le dispositif concerne un **traitement de données biométriques**, il était nécessaire que son responsable, la ville de Marseille, prouve la *nécessité absolue* de recourir à une telle technologie, ainsi que l'existence de garanties appropriées pour les droits et libertés des personnes concernées, de même que l'existence d'une base légale ou l'objectif de protection des « intérêts vitaux d'une personne physique ».

136.Or, la ville de Marseille n'a, à aucun moment, démontré la nécessité de mettre en place et recourir à un tel traitement, encore moins la *nécessité absolue* de ce dispositif par rapport à d'autres moyens, notamment humains. L'appel d'offres n'aborde à aucun moment l'existence de garanties appropriées au nouveau type de dispositif de vidéosurveillance automatisée. Enfin, l'appel d'offre mentionne les dispositions du code de la sécurité intérieure qui, comme vu précédemment, ne sont pas applicables à ce nouveau type de vidéosurveillance.

137.**Il en résulte** que la décision de mise en place d'un tel traitement est illégale.

Sur la délégation à une personne privée des compétences de police administrative générale

138.**En quatrième lieu**, l'article 12 de la Déclaration des Droits de l'Homme et du Citoyen de 1789 prévoit que :

> « *La garantie des droits de l'Homme et du Citoyen nécessite une force publique : cette force est donc instituée pour l'avantage de tous, et non pour l'utilité particulière de ceux auxquels elle est confiée* ».

139. Dans sa décision n° 2011-625 DC du 10 mars 2011, le Conseil Constitutionnel a analysé la constitutionnalité d'une disposition de la loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI). L'une de ses dispositions prévoyait que les salariés du délégataire privé pouvaient visionner les images prises par l'autorité publique sur la voie publique. Il ne s'agissait plus ici de permettre des systèmes de vidéoprotection privée mais des systèmes de vidéoprotection publique avec visionnage des images par des agents d'opérateurs privés.

140. Le Conseil Constitutionnel a considéré que :

> « *(…) en autorisant toute personne morale à mettre en œuvre des dispositifs de surveillance au-delà des abords « immédiats » de ses bâtiments et installations et en confiant à des opérateurs privés le soin d'exploiter des systèmes de vidéoprotection sur la voie publique et de visionner les images pour le compte de personnes publiques, les dispositions contestées permettent d'investir des personnes privées de missions de surveillance générale de la voie publique ; que chacune de ces dispositions rend ainsi possible* ***la délégation à une personne privée des compétences de police administrative générale inhérentes à l'exercice de la « force publique » nécessaire à la garantie des droits*** *; que, par suite, doivent être déclarés contraires à la Constitution le douzième alinéa du 1° ainsi que les b) et c) du 2° de l'article 18 ; que, par voie de conséquence, le premier alinéa du 1° de l'article 18 de la loi déférée doit conduire à remplacer le seul premier alinéa du II de l'article 10 de la loi du 21 janvier 1995 par les dix alinéas prévus par ce 1°* » (Décision n° 2011-625 DC du 10 mars 2011, pt. 19).

141. Il est ainsi indiqué dans le « commentaire autorisé » de la décision que « *Le Conseil a jugé que chacune des dispositions en cause conduisaient à déléguer une mission de surveillance générale de la voie publique et que, par conséquent, elles méconnaissaient l'exigence, résultant de l'article 12 de la Déclaration des droits de l'homme et du citoyen de 1789, selon laquelle la garantie des droits est assurée par une « force publique »* » (Commentaire de la décision n° 2011-625 DC du 10 mars 2011, p. 10).

142.**Il en résulte** qu'une décision mettant en œuvre un dispositif déléguant à une personne privée une mission de surveillance générale de la voie publique est illégale et même inconstitutionnelle et doit donc être immédiatement suspendue.

143.**En l'espèce**, il est prévu dans le PFT que les opérateurs ne pouvant pas « visualiser l'ensemble des flux » et ne pouvant pas « traiter en direct l'évènement », il serait nécessaire « que la solution logicielle permette d'effectuer de façon autonome cette visualisation ». De manière encore plus précise, il est indiqué que « la police municipale souhaite donc que le système informatique soit capable d'identifier des évènements qui se produisent en temps réel, à l'aide de fonctionnalités, afin d'alerter automatiquement les opérateurs, lesquels pourront réagir en direct (...) » (*cf.* Pièce n° 3, p. 12).

144.Le dispositif prévoit encore un « un traitement automatique des données (...) afin de détecter des anomalies/incidents/faits remarquables », une « aide aux opérateurs pour identifier, traiter et suivre des évènements », la « détection d'anomalies non identifiables par un opérateur », « une aide à la décision », et de nouvelles « fonctionnalités complémentaires à la sécurité » dont la « gestion de l'espace public » et l' « analyse des piétons/véhicules ainsi que des comportements » (*cf.* Pièce n° 3, p. 12).

145.Dans la partie intitulée « Poste 2 - Fourniture et intégration d'une solution globale fonctionnelle », il est prévu que le titulaire du marché « installe les différents composants de sa solution dans les serveurs puis réalises les différentes installations » et « réalise ensuite les paramétrages spécifiques de l'ensemble de la plateforme et des algorithmes adéquats sur les flux dont la ville de Marseille et le titulaire ont défini un objectif de VPI » (*cf.* Pièce n° 3, p. 22).

146.Comme rappelé à plusieurs reprises ci-dessus, le dispositif prévoit ensuite un très grand nombre de traitement de données personnelles effectuées par la « solution logicielle » dont l'« analyse de scènes statiques », le « comptage de personnes/véhicules », la « détection périmétrique », « l'analyse de densité de foule », ainsi que la recherche et l'analyse de séquence de vidéos à l'aide de filtres.

147.Ainsi, la décision attaquée prévoit la délégation au titulaire du marché, en l'espèce, la société SNEF, d'un grand nombre de pouvoirs de surveillance de la voie publique et de pouvoirs de police administrative. Il est en effet indiqué que le paramétrage des algorithmes sera fait par l'entreprise privée titulaire du marché qui se voit donc déléguer des compétences de caractérisation d'évènements

pouvant engendrer une alerte et déclencher la surveillance active effectuée par des « opérateurs humains ». Il reviendra ainsi à la solution logicielle de l'entreprise privée d'identifier, de catégoriser et de générer des alertes sur certains évènements ayant lieu sur la voie publique, et cela de manière automatique, à propos des évènements que l'opérateur lui-même n'aurait pas pu remarquer. Il lui reviendra également, à la société privée, à travers le dispositif qu'elle a conçu et mis en œuvre pour le compte de la ville, de procéder à des missions de gestion de la voie publique et d'analyse et de comptage des piétons.

148. **Il en résulte que** la décision est illégale et même inconstitutionnelle en ce qu'elle entraîne la délégation à une personne privée de compétences de police administrative générale inhérentes à l'exercice de la force publique.

149. Il ressort de tout ce qui précède qu'il existe plusieurs moyens propres à faire naître, à tout le moins, un doute sérieux sur la légalité de la décision attaquée.

150. **A tous égards, la suspension s'impose.**

Sur l'application de l'article L. 761-1 du code de justice administrative

151. Compte tenu des frais qu'elles ont été contraintes 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 ville de Marseille sur le fondement des dispositions de l'article L. 761-1 du code de justice administrative.

PAR CES MOTIFS, les exposantes concluent qu'il plaise au tribunal administratif de Marseille :

SUSPENDRE l'exécution de la décision prise par la ville de Marseille de mettre en place un dispositif de « vidéoprotection intelligente » « d'ici la fin de l'année [2019] », telle que révélée par l'article de *Télérama* du 11 décembre 2019 intitulée « Reconnaissance faciale en France : pourra-t-on y échapper ? », jusqu'à ce qu'il soit statué au fond sur la légalité de cette décision ;

METTRE A LA CHARGE de la ville de Marseille une somme de 1 024 euros, en application des dispositions de l'article L. 761-1 du code de justice administrative.

Fait à Paris, le 17 janvier 2019

ALEXIS FITZJEAN Ó COBHTHAIGH
Avocat au Barreau de Paris