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 INTRODUCTIVE D'INSTANCE

POUR : **L'association « La Quadrature du Net » (LQDN), association régie par la loi du 1er juillet 1901 dont le siège social est situé au 60, rue des Orteaux à Paris (75020), enregistrée en préfecture de police de Paris sous le numéro W751218406, représentée par M. Bastien Le Querrec, membre du collège solidaire en exercice.**

CONTRE : **Le contrat conclu par la ville de Marseille avec la société SNEF portant sur l'acquisition d'un dispositif de vidéoprotection intelligente, et dont la résiliation a été refusée par une décision implicite de la ville de Marseille.**

L'exposante défère le contrat attaqué à la censure du tribunal administratif de Marseille. Elle en requiert qu'il soit mis fin à l'exécution de ce contrat, par les motifs suivants.

FAITS

1. L'association « La Quadrature du Net » (LQDN) est investie 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° 3).

3. Le 29 novembre 2018, la ville de Marseille a indiqué sur le site boamp.fr (Bulletin officiel des annonces des marchés publics) que le marché avait été attribué à la société SNEF Service Tertiaire SA. Il y était précisé que la date de conclusion du marché était le 2 novembre 2018 (*cf.* Pièce n° 4).

4. Par la suite, la requérante a eu communication de plusieurs documents contractuels de ce marché, notamment le « Programme fonctionnel technique » (ci-après « PFT », *cf.* Pièce n° 5) ainsi que le « Cahier des clauses administratives particulière » (ci-après « CCAP », *cf.* Pièce n° 6).

5. Le 11 décembre 2019, un article du journal Télérama a indiqué que « *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° 7).

6. Le 17 janvier 2020, l'association La Quadrature du Net et la Ligue des droits de l'Homme ont déposé un recours devant le tribunal administratif de Marseille pour demander l'annulation de la décision prise par la ville de Marseille de mettre en place ce dispositif de « vidéoprotection intelligente » (*cf.* Pièce n° 8).

7. Cette demande était assortie d'une demande de suspension de l'exécution de cette décision, sur le fondement de l'article L. 521-1 du code de justice administrative (*cf.* Pièce n° 9).

8. Le 11 mars 2020, le tribunal administratif de Marseille a rejeté la demande de suspension de la décision. Il a notamment jugé que « *les requérantes ne produisent aucun élément précis, en dehors d'articles de presse et de pièces du marché public signé en 2018, qui suggèrerait qu'aurait été prise une décision distincte de celle autorisant la conclusion ou la signature de ce marché* [...] » (*cf.* Pièce n° 10).

9. Le 14 mai 2020, le tribunal administratif de Marseille a, par ordonnance, rejeté la requête en annulation des associations La Quadrature du Net et Ligue des droits de l'homme (*cf.* Pièce n° 11).

10. Le 28 juillet 2020, l'association La Quadrature du Net a adressé à la ville de Marseille un courrier par lequel elle lui demandait de résilier le marché public entre la ville de Marseille et la SNEF conclu le 2 novembre 2018 intitulé « Acquisition d'un dispositif de vidéoprotection intelligente » (*cf.* Pièce n° 12).

11. Ce courrier a été remis à la ville de Marseille le 5 août 2020 (*cf.* Pièce n° 13). Le silence gardé par la ville de Marseille a laissé naître une décision implicite de refus le 5 octobre 2020.

12. Pourtant, ce contrat est manifestement contraire à l'intérêt général, d'une part, dès lors qu'il permet notamment une surveillance algorithmique automatisée de l'ensemble de la ville de Marseille, et d'autre part, dès lors que cette surveillance algorithmique est manifestement illégale, notamment en ce qu'elle viole les règles garantissant le droit à la vie privée et le droit à la protection des données personnelles.

13. En effet, le contrat prévoit à terme une surveillance sur l'ensemble des flux vidéos des caméras de vidéosurveillance qui équipent la ville de Marseille. Le PFT indique que, en février 2018, la ville était équipée de 1500 caméras, dont plus de 1000 opérationnelles (*cf.* Pièce n° 5, p. 5). Ce chiffre est très probablement plus important aujourd'hui. Ce faisant, comme il sera démontré ci-après, le contrat met donc en place une surveillance biométrique (II) qui est de plus illégale (III).

14. C’est le contrat attaqué.

DISCUSSION

I. Sur l'intérêt à agir de La Quadrature du Net et la recevabilité de son recours

15. **En droit**, le Conseil d'État juge qu'« *un tiers à un contrat administratif susceptible d'être lésé dans ses intérêts de façon suffisamment directe et certaine par une décision refusant de faire droit à sa demande de mettre fin à l'exécution du contrat, est recevable à former devant le juge du contrat un recours de pleine juridiction tendant à ce qu'il soit mis fin à l'exécution du contrat* » (*cf.* CE, Sect., 30 juin 2017, *Syndicat mixte de promotion de l'activité transmanche (SMPAT)*, n° 398445, Rec. p. 209).

16. Il a par ailleurs précisé que « *les tiers ne peuvent utilement soulever, à l'appui de leurs conclusions tendant à ce qu'il soit mis fin à l'exécution du contrat, que des moyens tirés de ce que la personne publique contractante était tenue de mettre fin à son exécution du fait de dispositions législatives applicables aux contrats en cours, de ce que le contrat est entaché d'irrégularités qui sont de nature à faire obstacle à la poursuite de son exécution et que le juge devrait relever d'office ou encore de ce que la poursuite de l'exécution du contrat est manifestement contraire à l'intérêt général* » (Conseil d'État, même décision).

17. À ce titre, en se fondant notamment sur la décision du 3 mars 2006, *Société Oberthur* (*cf.* CE, 3 mars 2006, *Société Oberthur*, n° 287960, Rec. T. p. 1001), la Direction des affaires juridiques (DAJ) du ministère de l'économie rappelle que peuvent être recevables à agir contre un contrat administratif « *les associations de défense d'intérêts collectifs si la lésion des intérêts qu'elles défendent résulte directement du contrat* [...] » (*cf.* DAJ Bercy, « Les recours contentieux liés à la passation des contrats de la commande publique », 1er avril 2019).

18. **En l'espèce**, La Quadrature du Net est une association qui promeut et dé-

fend les libertés fondamentales dans l'environnement numérique. Elle lutte contre la surveillance généralisée, que celle-ci vienne des États ou des acteurs privés, et contre le fichage généralisé.

19. Elle a notamment pour objet, aux termes de l'article 3 de ses statuts, « *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* » et « *la lutte contre l'utilisation d'outils numériques à des fins de surveillance illégitime* » (*cf.* Pièce n° 1).

20. L'exposante a notamment engagé plusieurs actions contentieuses afin de défendre les droits au respect de la vie privée et à la protection des données à caractère personnel devant le Conseil constitutionnel, le Conseil d'État et les autres juridictions administratives, tel que récemment contre des dispositifs de reconnaissance faciale dans des lycées à Nice et à Marseille (*cf.* TA Marseille, 27 février 2020, n° 1901249).

21. Le marché conclu par la ville de Marseille, en ce qu'il prévoit un dispositif de « vidéoprotection intelligente », entraîne un traitement de données personnelles manifestement excessif et disproportionné qui n'a fait l'objet d'aucune étude d'impact et qui n'est fondée sur aucune base légale. En prévoyant la mise en place sur la voie publique d'un tel système de vidéosurveillance algorithmique, le marché conclu par la ville de Marseille avec la société SNEF affecte directement l'exercice des droits fondamentaux dans l'environnement numérique et 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.

22. C'est à ce titre que La Quadrature du Net a demandé à la ville de Marseille de résilier le marché conclu avec la SNEF en ce qu'il ne respectait ni le droit européen ni le droit français concernant le droit à la vie privée et à la protection des données personnelles. La ville de Marseille a, par une décision implicite, refusé de résilier ce marché.

23. **Il en résulte que** l'association a sans conteste intérêt à agir contre la déci-

sion de refus implicite de la ville de Marseille refusant de prononcer la résiliation du contrat conclu avec la société SNEF portant sur l'acquisition d'un dispositif de vidéoprotection intelligente.

24. **Elle est également recevable à demander la résiliation de ce contrat**, dès lors qu'elle est lésée dans ses intérêts de façon suffisamment directe et certaine par la décision implicite de la ville de Marseille refusant de faire droit à sa demande de mettre fin à l'exécution du contrat litigieux.

25. Les moyens articulés ci-après démontrent, d'une part, que la ville de Marseille était tenue de mettre fin à l'exécution du contrat litigieux du fait de dispositions législatives applicables à ce contrat (*i.e.* notamment la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci après « loi Informatique et Libertés ») et, d'autre part, que la poursuite de l'exécution de ce contrat est manifestement contraire à l'intérêt général, au sens de la jurisprudence de Section *SMPAT* du 20 juin 2017.

II. Sur la qualification juridique des faits

26. Le marché conclu par la ville de Marseille avec la société SNEF met en place une chaîne de traitements de données personnelles, et plus particulièrement de données sensibles.

27. **En droit**, aux termes du 1 de l'article 3 de la directive 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 (ci-après directive « police-justice »), une donnée personnelle est définie comme « *toute information se rapportant à une personne identifiée ou identifiable* ». Une personne identifiable est une personne qui peut être « *identifiée, directement ou indirectement, notamment par référence à* […] *un ou plusieurs éléments spécifiques propres à son identité physique, physiologique,* […] *culturelle ou sociale* ». Ces mêmes articles définissent un traitement de données personnelles comme « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés*

[…] *telles que la collecte, l'enregistrement* […]*, la consultation, l'utilisation, la communication par transmission* […] *l'effacement*».

28. Ainsi, selon la jurisprudence de la Cour de justice de l'Union européenne, l'image d'une personne enregistrée par une caméra constitue une « *donnée à caractère personnel* », dès lors qu'elle permet d'identifier la personne concernée (*cf*. CJUE, 14 février 2019, *Buivids*, n° C-345/17, pt. 31 ; CJUE, 11 décembre 2014, *Ryneš*, n° C-212/13, pt. 22). Par suite, dès lors qu'il est possible de voir ou d'entendre la personne sur la vidéo en cause, les images des personnes ainsi enregistrées constituent des données personnelles (*cf*. arrêt, *Buivids*, préc., pt. 32).

29. **En droit**, toujours, il existe au sein de ces données une sous-catégorie de données dites « sensibles », qui comprend notamment, selon l'article 6 de la loi Informatique et Libertés, les données qui « *révèlent* […] *les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique* », ou bien « *des données biométriques aux fins d'identifier une personne physique de manière unique* ». L'article 10 de la directive « police-justice » reprend cette même définition.

30. La notion de données biométriques est détaillée par l'article 3 de la directive « police-justice » comme désignant des données « *résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales* ». Le Comité européen de la protection des données (ci-après « CEPD »), autorité européenne chargée de garantir l'application effective des règles européennes en matière de données personnelles, détaille le traitement de données biométriques comme étant un « *traitement technique spécifique* » des données se rapportant « *aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique* » dans le but précis « *d'identifier une personne physique de manière unique* » (CEPD, « Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo », point 76, *cf*. Pièce n° 15). Si l'approche du CEPD concerne le réglement n° 2016/679, dit règlement général sur la protection des données (ci-après « RGPD »), elle est bien entendu applicable *mutatis mutandis* à la directive « police-justice », cette dernière reprenant exactement les mêmes définitions que le RGPD.

31. À ce titre, la notion d'« identification unique » n'implique pas nécessaire-

ment 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.

32. Au point 82 de ces mêmes lignes directrices, 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 l'autorité d'un traitement de données biométriques :

> « *Toutefois, l'article 9* [du RGPD et, *mutatis mutandis*, l'article 10 de la directive « police-justice »] *s'applique si le responsable du traitement conserve des données biométriques* [...] *afin d'identifier une personne de manière unique. Si un responsable du traitement souhaite détecter une personne concernée qui pénètre à nouveau dans l'espace surveillé ou dans une autre zone* [...] *la finalité serait alors d'identifier de manière unique une personne physique, ce qui signifie que l'opération relèverait d'emblée de l'article 9* [...] . *Dès lors que le système se fonde sur l'analyse de caractéristiques physiques pour détecter des personnes spécifiques qui entrent dans le champ de la caméra (comme les visiteurs d'un centre commercial) et les suivre, il constitue une méthode d'identification biométrique, car il vise la reconnaissance par l'utilisation d'un traitement technique spécifique.* » (CEPD, lignes directrices 3/2019, point 82, p. 16, *cf.* Pièce n° 15)

33. **En l'espèce**, le marché conclu par la ville de Marseille 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° 5, p. 14 et 15).

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

35. 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* » (graffitis), du « *vol / disparation / destruction de mobilier urbain* ». Le marché public 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° 5, p. 12, 13 et 19).

36. On en comprend que la ville de Marseille veut définir et enregistrer, 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. 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 sur place.

37. De plus, il n'est pas exclut que l'alerte transmette aux agents des caractéristiques visuelles permettant de retrouver eux-même 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 (âge, taille, corpulence, genre) ou comportementales (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.

38. Par ailleurs, dans une affaire n° 2001080, la requérante avait demandé au tribunal administratif de Marseille, sur le fondement de l'article L. 521-1 du code de justice administrative, de suspendre la décision de la ville de Marseille de mettre en place un dispositif de vidéosurveillance automatisé. Si le juge des référés a considéré la requête irrecevable car dirigée contre un acte détachable du contrat attaqué aujourd'hui dans la présente requête, il relevait bien la présence d'un dispositif « *d'analyse de données biométriques permettant d'identifier les personnes dont l'image serait captée par les caméras* » (TA Marseille, 11 mars 2020, n° 2001080, pt. 5, *cf.* Pièce n° 10).

39. **En conclusion**, de par le fonctionnement même du traitement qui conduit à l'alerte, mais aussi probablement de par les informations transmises par l'alerte, le contrat conclu entre la ville de Marseille et la société SNEF met en place un traitement non seulement de données personnelles, mais encore — parce qu'il est permis d'identifier une personne de façon unique — de données personnelles sensibles.

III. Sur les moyens propres à conduire à ce qu'il soit mis fin au contrat attaqué

40. Le contrat, en ce qu'il permet une surveillance constante de l'espace public par un procédé algorithmique automatique et qu'il est manifestement contraire aux règles sur la protection des données personnelles, porte une atteinte particulièrement grave à l'intérêt général.

41. Le contrat est manifestement illégal en ce qu'il a été conclu en l'absence d'analyse d'impact (A) et prévoit un traitement de données personnelles manifestement disproportionné (B). Il ne respecte pas non plus les conditions de légalité d'un traitement de données sensibles (C) et entraîne la délégation de missions de police administrative à une personne privée (D).

A. En ce qui concerne l'absence d'analyse d'impact finalisée avant la conclusion du marché

42. **En droit**, l'article 90 de la loi Informatique et Libertés prévoit que, si un 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* » et adresse cette analyse à la CNIL « *si le traitement est mis en œuvre pour le compte de l'État* ». L'article 27 de la directive « police-justice » précise que cette étude d'impact est requise pour les traitements qui sont réalisés « *en particulier par le recours à de nouvelles technologies* ».

43. 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 « *trois types de traitements* [sont] *susceptibles de présenter un risque élevé* » et nécessitent donc une analyse d'impact, dont « *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* ».

44. 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 Groupe de travail Article 29 sur la protection des données (organe, précurseur du CEPD, consultatif européen indépendant sur la protection des données et de la vie privée, ci-après « G29 ») 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* » (*cf.* Pièce n° 16, p. 4).

45. 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* » (*cf.* Pièce n° 16, p. 17).

46. **En l'espèce**, comme exposé ci-dessus, le dispositif attaqué prévoit l'instal-

lation 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 » (Pièce n° 5, p. 5).

47. 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* » (Pièce n° 5, p. 12).

48. À 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* » (Pièce n° 5, p. 13).

49. Il permet par ailleurs de « *repérer des visages ou d'analyser des allées et venues et de prévenir s'il y a danger* » (francetvinfo.fr, « Marseille : des caméras intelligentes », 25 juillet 2016) et d'« *analyser et fusionner les informations provenant de plusieurs capteurs et dont la finalité est de constituer une aide à la décision* » (Pièce n° 5, p. 6).

50. 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.

51. 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 combinaison de données, une surveillance systématique de personnes et comprend l'utilisation innovante de nouvelles solutions technologiques ou organisationnelles.

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

53. Il en résulte qu'une analyse d'impact était obligatoire « *le plus tôt possible dans le cycle de conception du traitement* ». C'est d'ailleurs également l'avis de la CNIL qui, dans un document obtenue par la requérante, a souligné à la ville de Marseille que « *de par son ampleur et ses conditions d'exploitation, le traitement vidéoprotection de la ville de Marseille apparaît devoir faire l'objet d'une AIPD* » (*cf.* Pièce n° 14, p. 1).

54. Or, il a été publié, le 18 juin 2019, sur le site « 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…)* ». Le 29 novembre 2018, la ville de Marseille a également publié un avis d'attribution du marché.

55. Il ressort par ailleurs des documents obtenus par la requérante concernant les échanges entre la ville de Marseille et la CNIL que, au 28 septembre 2020, l'analyse d'impact transmise par la ville de Marseille à la CNIL n'était en aucun cas finalisée, et les éléments qui y étaient contenus étaient loin d'être satisfaisants pour l'autorité de protection de la vie privée. Celle-ci considère en effet que, concernant cette analyse :

> « *Une première analyse du document a permis de relever un certain nombre de points de fonds et de méthode pour lesquels des précisions et compléments doivent être apportés par le responsable de traitement. Ces éléments sont indispensables aux fins, d'une part, de parvenir à une compréhension précise du dispositif envisagé et, d'autre part, de pouvoir délivrer un retour adapté* » (*cf.* Pièce n° 14).

56. Cela signifie que le contrat a été conclu, et la mise en place du dispositif engagée sans qu'aucune étude d'impact finalisée n'ait été réalisée.

57. 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.

58. 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, Ass. 23 décembre 2011, *Danthony*, n° 335033, Rec. p. 649 ; voir dans ce sens également : CE, 14 octobre 2011, *Société Ocréal*,n° 323257, Rec. T. p. 734).

59. Conformément aux motifs développés ci-dessous, un 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.

60. **Il en résulte** que le contrat conclu est illégal en ce qu'il a été conclu et est mis en œuvre alors qu'aucune étude d'impact n'a été encore réalisée.

B. En ce qui concerne le caractère excessif et inadéquat du traitement en litige

61. Le contrat 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.

62. **En droit**, 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* ».

63. À ce titre, le considérant 26 de cette même directive énonce qu'« *il 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 ».

64. L'article 4 de la loi Informatique et 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* ».

65. Dans une affaire concernant l'installation de portiques de reconnaissance faciale dans deux lycées, la CNIL a déjà souligné qu'un « *traitement de données* [sensibles] *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* » (courrier adressé le 25 octobre 2019 au président de la région Provence-Alpes-Côte d'Azur par la CNIL).

66. Elle précisait qu'en l'espèce la finalité de sécurisation et de fluidification des entrées au sein des lycées « *peut incontestablement être raisonnablement atteinte par d'autres moyens* ». Elle en déduisait 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* ».

67. **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.

68. **En l'espèce**, les documents contractuels énoncent 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 L. 2212-2 du code général des collectivités territoriales.

69. 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. 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* » (Pièce n° 5, p. 12).

70. 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* » (Pièce n° 5, p. 14).

71. 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 les « *objets abandonnés* », les « *individu au sol* », les « *TAG* » (graffitis), la « *dépose sauvage d'ordures* », le « *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 par ailleurs indiqué que le dispositif doit permettre une analyse de séquences vidéos par filtres et que « *les filtres sont : individu (description, avatar, photo)* » (Pièce n° 3, p. 12, 13 et 19).

72. 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* » (Pièce n° 3, p. 12).

73. Il n'est par ailleurs 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 Informatique et Libertés, aucun élément précis ou factuel qui permettrait de déterminer qu'aucun autre moyen n'aurait permis de parvenir à l'objectif visé.

74. **Il en résulte que** le contrat attaqué met en place un traitement de données qui n'est ni adéquat, ni nécessaire, et manifestement excessifs par rapport à la finalité envisagé.

C. En ce qui concerne le non-respect des conditions de légalité d'un traitement de données biométriques

75. Le contrat attaqué est illégal en ce qu'il met en place un traitement de données biométriques sans respecter les conditions de légalité d'un tel traitement.

76. **En droit**, la loi Informatique et Libertés, transposant l'article 10 de la directive « police-justice », dispose à son article 88 que le traitement de données sensibles « *est possible uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et 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* ».

77. Le G29, dans son « *avis sur certaines questions clés de la directive (UE) 2016/680* » du 29 novembre 2017, exige « *de prévoir des motifs précis et particulièrement solides* » pour justifier les traitements de données biométriques ou d'autres données sensibles, afin notamment « *d'évaluer et de démontrer si la finalité du traitement (par ex. une enquête pénale) ne peut être atteinte dans le cadre d'un traitement qui affecte moins les droits et les libertés de la personne concernée* ». Autrement dit, pour satisfaire le critère de « *nécessité absolue* », il ne doit exister absolument aucun traitement de données qui, ne traitant aucune donnée sensible, permettrait de poursuivre la même finalité.

78. **En l'espèce**, comme indiqué ci-dessus, il ne fait aucun doute que le contrat conclu par la ville de Marseille concerne la mise en place d'un traitement de données biométriques.

79. En premier lieu, de par le fonctionnement même du traitement qui conduit à l'alerte, mais aussi probablement de part les informations transmises lorsque des alerte sont générées par le dispositif à destination des opérateurs humains, le contrat prévoit un traitement de données biométriques car ayant trait aux caractéristiques physiques, physiologiques ou comportementales, ou permettant d'identifier une personne de façon unique.

80. En second lieu, 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)* [...] » (Pièce n° 5, p. 19).

81. Il en résulte que le dispositif concernant le traitement de données biométriques, il était nécessaire que son responsable, la ville de Marseille, en prouve la nécessité absolue, ainsi que l'existence de garanties appropriées pour les droits et libertés des personnes concernées, ainsi que l'existence d'une disposition législative ou réglementaire ou l'objectif de protection des « *intérêts vitaux d'une personne physique* ».

82. Aucun élément n'est apporté par la ville de Marseille pour justifier de ces éléments. Comme établi précédemment, la ville de Marseille n'a, à aucun moment, démontré la nécessité du traitement, encore moins la « *nécessité absolue* » de ce dis-

positif par rapport à d'autres moyens, notamment humains. L'appel d'offre n'aborde à aucun moment l'existence de garanties appropriées au nouveau type de dispositif de vidéosurveillance automatisée.

83. **Il en résulte que** le contrat met en place un traitement de données sensibles sans nécessité absolue ni garanties appropriées.

D. En ce qui concerne la délégation de missions de police administrative à une personne privée

84. Le contrat est illégal en ce qu'il délègue inconstitutionnellement à une personne privée des compétences de police administrative générale.

85. **En droit**, 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* ».

86. 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'un des articles prévoyait que « *les salariés du délégataire privé pussent visionner les images prises par l'autorité publique sur la voie publique.* »

87. 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* [...] » (Décision n° 2011-625 DC du 10

mars 2011, Considérant 19).

88. 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).

89. **Il en résulte** qu'un contrat prévoyant la mise en œuvre d'un dispositif déléguant à une personne privée une mission de surveillance générale de la voie publique est illégal et doit être résilié.

90. **En l'espèce,** concernant le contrat conclu entre la ville de Marseille et la SNEF, 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 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* [...] » (Pièce n° 5, p. 12).

91. 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* » (Pièce n° 5, p. 12).

92. 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 et 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 » (Pièce n° 5, p. 22).

93. Comme rappelé à plusieurs reprises ci-dessus, le dispositif prévoit ensuite un très large nombres de traitements de données personnelles effectués par la « *solution logicielle* » dont l'« *analyse de scènes statiques* », le « *comptage de personnes / véhicules* », la « *détection périmétrique* », « *l'analyse de densité de foule* », la recherche et l'analyse de séquence de vidéos à l'aide de filtres.

94. Ainsi, le contrat attaqué 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 la 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 générer une alerte et déclencher la surveillance active d'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, et concernant des évènements que l'opérateur lui-même n'aurait pas pu remarquer. Il lui reviendra également, à travers le dispositif qu'elle a conçu et mis en œuvre, de procéder à des mission de gestion de la voie publique et d'analyse et de comptage des piétons.

95. **Il en résulte que** le contrat attaqué est illégal en ce qu'il entraîne la délégation à une personne privée de compétences de police administrative générale inhérentes à l'exercice de la force publique.

96. **En conclusion**, le contrat attaqué porte une atteinte particulièrement grave à l'intérêt général en ce qu'il met en place une surveillance algorithmique automatisée de l'espace public marseillais, surveillance qui est illégale.

97. À tous égards, la résiliation immédiate du contrat s'impose.

PAR CES MOTIFS, l'association La Quadrature du Net, exposante, conclut qu'il plaise au tribunal de :

METTRE FIN A L'EXECUTION du marché conclu le 2 novembre 2018 entre la ville de Marseille et la société SNEF Service Tertiaire SA ayant notamment pour objet l'acquisition d'un dispositif dit de "vidéoprotection intelligente" ;

METTRE À LA CHARGE de la ville de Marseille une somme de 4 096 euros, en application de l'article L. 761-1 du code de justice administrative.

Fait à Paris, le 3 décembre 2020

Alexis FITZJEAN Ó COBHTHAIGH
Avocat au Barreau de Paris

BORDEREAU DES PRODUCTIONS

Pièce n° 1 : Statuts de l'association « La Quadrature du Net » ;

Pièce n° 2 : Pouvoir spécial ;

Pièce n° 3 : Avis de marché n° 15-165192, intitulé « Acquisition d'un dispositif de vidéoprotection intelligente, à Marseille », diffusé le 31 octobre 2015 ;

Pièce n° 4 : Avis n° 18-165285, diffusée le 30 novembre 2018 ;

Pièce n° 5 : Programme technique fonctionnel final ;

Pièce n° 6 : Cahier des Clauses Administratives Particulières ;

Pièce n° 7 : Article de M. Olivier Tesquet, « Reconnaissance faciale : pourra-t-on y échapper ? », Télérama, 11 décembre 2019 ;

Pièce n° 8 : Recours de La Quadrature du Net et de la Ligue des droits de l'Homme déposé devant le tribunal administratif de Marseille le 17 janvier 2020 ;

Pièce n° 9 : Recours en référé-suspension de La Quadrature du Net et de la Ligue des droits de l'Homme déposé devant le tribunal administratif de Marseille le 17 janvier 2020 ;

Pièce n° 10 : Décision de rejet du 11 mars 2020 du tribunal administratif de Marseille ;

Pièce n° 11 : Ordonnance du tribunal administratif de Marseille du 14 mai 2020 ;

Pièce n° 12 : Courrier du 28 juillet 2020 adressé par l'association La Quadrature du Net à la ville de Marseille ;

Pièce n° 13 : Preuves de la distribution du courrier à la ville de Marseille le 3 août 2020 ;

Pièce n° 14 : Courriers envoyés par la CNIL à la ville de Marseille en octobre 2020 ;

Pièce n° 15 : EDPB, Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo

Pièce n° 16 : Groupe de travail « Article 29 » sur la protection des données, 4 avril 2017, *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*.