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

COUR ADMINISTRATIVE D'APPEL

DE

MARSEILLE

REQUÊTE D'APPEL

POUR : **L'association « La Quadrature du Net » (LQDN), association régie par la loi du 1er juillet 1901 dont le siège social est situé au 115, rue de Ménilmontant à Paris (75020), enregistrée en préfecture de police de Paris sous le numéro W751218406, représentée par [redacted], membre du collège solidaire en exercice.**

CONTRE : **Le jugement n° 2009485 du 2 juin 2023 par lequel le tribunal administratif de Marseille a rejeté la requête présentée par l'association La Quadrature du Net, exposante, tendant, d'une part, à ce qu'il soit mis fin à l'exécution du marché conclu le 2 novembre 2018 entre la commune de Marseille et la société SNEF Service Tertiaire SA ayant notamment pour objet l'acquisition d'un dispositif dit de « vidéoprotection intelligente » et, d'autre part, à ce qu'il soit mis à la charge de la commune de Marseille une somme de 4 096 euros au titre de l'article L. 761-1 du code de justice administrative.**

L'exposante défère le jugement attaqué à la censure de la cour administrative d'appel de Marseille. Elle en requière l'annulation et sollicite qu'il soit fait droit à sa requête présentée devant le tribunal administratif de Marseille par les motifs suivants.

Table des matières

FAITS

1. L'association La Quadrature du Net est investie de longue date dans la défense des droits et des libertés, notamment dans l'environnement numérique, notamment à travers une forte activité de contentieux stratégique.

2. Le 31 octobre 2015, la commune de Marseille a publié un avis de marché intitulé « Acquisition d'un dispositif de vidéoprotection intelligente, à Marseille » (*cf.* pièce n° 5).

3. Le 29 novembre 2018, la commune 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° 6).

4. Par la suite, la requérante a eu communication de plusieurs documents contractuels de ce marché, notamment le Programme fonctionnel technique (PFT), (*cf.* pièce n° 7) ainsi que le Cahier des clauses administratives particulières (CCAP), (*cf.* pièce n° 8).

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° 9).

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 commune de Marseille de mettre en place ce dispositif de « vidéoprotection intelligente » (*cf.* pièce n° 10).

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 administra-

tive (*cf.* pièce n° 11).

8. Par ordonnance du 11 mars 2020, le juge des référés du 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° 12). Puis, par ordonnance du 14 mai 2020, la présidente de la 9e chambre du tribunal administratif de Marseille a rejeté la requête en annulation des associations La Quadrature du Net et Ligue des droits de l'homme (*cf.* pièce n° 13).

9. Le 28 juillet 2020, l'association La Quadrature du Net a donc adressé à la commune de Marseille un courrier par lequel elle lui demandait de résilier le marché public entre conclu entre elle-même et la SNEF conclu le 2 novembre 2018 intitulé « Acquisition d'un dispositif de vidéoprotection intelligente » (*cf.* pièce n° 14). Ce courrier a été remis à la commune de Marseille le 5 août 2020 (*cf.* pièce n° 15). Le silence gardé par la commune de Marseille a laissé naître une décision implicite de refus le 5 octobre 2020.

10. 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 commune 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. Par ailleurs, son objet même – la mise en place d'un traitement de données biométriques sur la voie publique – est illicite.

11. En effet, le contrat prévoit une surveillance de l'ensemble des flux vidéos des caméras de vidéosurveillance qui équipent la commune de Marseille. Le PFT indique que'en février 2018 la commune était équipée de 1 500 caméras, dont plus de 1 000 opérationnelles (*cf.* pièce n° 7, p. 5). Ce chiffre est très probablement plus important aujourd'hui.

12. Par une requête enregistrée le 3 décembre 2020, puis deux mémoires complémentaires, l'association La Quadrature du Net, exposante, a demandé au tribunal

administratif de Marseille qu'il soit mis fin à l'exécution du marché conclu le 2 novembre 2018 entre la commune de Marseille et la société SNEF Service Tertiaire SA ayant notamment pour objet l'acquisition d'un dispositif dit de « vidéoprotection intelligente ».

13. Elle montrait dans sa requête que ce contrat était illégal en ce qu'il déléguait à une personne privée des compétences de police administrative générale, qu'il n'avait fait l'objet d'aucune étude d'impact préalable, qu'il était disproportionné et qu'il ne respectait pas les conditions particulières propres aux traitements de données sensibles, ces différents moyens d'illégalité justifiant, pour des motifs d'intérêt général, la résiliation du contrat litigieux.

14. Par un jugement n° 2009485 du 2 juin 2023 (*cf.* pièce n° 1), le tribunal administratif de Marseille a rejeté la requête de l'exposante. Il a considéré que le contrat ne procéderait pas à une délégation illicite d'une mission de police administrative (pt. 6) et qu'à supposer le dispositif litigieux disproportionné, la poursuite du contrat ne serait pas manifestement contraire à l'intérêt général (pt. 8). Enfin, il s'est borné à considérer, sans mieux s'en expliquer, que les autres moyens de la requérante étaient prétendument inopérants (pt. 9).

15. C'est le jugement attaqué.

DISCUSSION

I. Sur le jugement attaqué

A. En ce qui concerne l'insuffisance de motivation

16. **En premier lieu**, le jugement attaqué est irrégulier en ce qu'il est entaché d'insuffisance de motivation, dès lors que le tribunal a omis de répondre au moyen, pourtant opérant, tiré du non-respect des règles relatives à un traitement de données sensibles. En outre et, en toute hypothèse, le jugement attaqué est irrégulier, en ce que le tribunal a omis d'à tout le moins viser ce moyen, en contradiction avec l'article R. 741-2 du code de justice administrative.

17. En droit, en application d'un principe général rappelé à l'article L. 9 du code de justice administrative, les jugements doivent être motivés.

18. En outre, il résulte du deuxième alinéa de l'article R. 741-2 du code de justice administrative que « [la décision] *contient le nom des parties, l'analyse des conclusions et mémoires ainsi que les visas des dispositions législatives ou réglementaires dont elle fait application.* »

19. Il ressort de ces dispositions que le jugement qui ne fait pas mention des conclusions des parties est irrégulier (*cf.* CE, 10 décembre 1975, *Soriano*, n° 91106, Rec. T. p. 1209), sauf si, à défaut de viser les conclusions, il en a fait l'analyse et y a statué de manière expresse (*cf.* CE, 11 mars 1988, *SARL Jennifer*, n° 44985, Rec. T. p. 963).

20. Par ailleurs, un jugement qui n'a ni visé ni répondu à un moyen, même inopérant, est entaché d'irrégularité (*cf.* CE, 18 juin 1969, *Giaume*, n° 69666, Rec. p. 321).

21. **En l'espèce**, la requérante a, par un mémoire enregistré le 8 décembre 2022, soulevé un nouveau moyen tiré de ce que le contrat litigieux autorisait la

mise en œuvre d'un traitement de données sensibles au sens de l'article 6 de 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 qu'il était donc contraire à ce dernier ainsi qu'à l'article 88 de la loi Informatique et Libertés, éclairé par l'article 10 de la directive UE n° 2016/680 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 »). Or, si le mémoire du 8 décembre 2022 a bien été enregistré et visé, le jugement attaqué ne fait aucune mention de ce moyen.

22. À supposer, pour les seuls besoins de la discussions, que ce moyen ait été inopérant – *quod non* –, le jugement aurait dû *a minima* le viser. Pourtant, si le moyen tiré de ce que le dispositif litigieux constitue un traitement de données biométriques est bien visé, tel n'est pas le cas pour le moyen tiré de ce que le dispositif litigieux constitue un traitement de données sensibles, dont le champ excède largement les seules données biométriques.

23. **Il en résulte que** le jugement attaqué est entaché d'irrégularité.

B. En ce qui concerne l'intérêt général justifiant la résiliation du contrat

24. **En deuxième lieu**, c'est au prix d'une erreur de droit, d'une erreur manifeste d'appréciation, d'une contradiction de motifs et d'une dénaturation des écritures de l'exposante que le jugement retient que la poursuite de l'exécution du contrat à la date du jugement ne serait pas manifestement contraire à l'intérêt général, au motif que l'exécution du contrat serait prétendument suspendue.

25. **En droit**, 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, et ne peut utilement soulever, à l'appui de ses 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 (*cf.* CE, Sect., 30 juin 2017, *Syndicat mixte de promotion de l'activité transmanche (SMPAT)*, n° 398445, Rec. p. 209).

26. **En l'espèce**, c'est à tort que le jugement attaqué retient, pour constater que la poursuite de l'exécution du contrat litigieux ne serait pas manifestement contraire à l'intérêt général, que l'exécution du contrat litigieux « *a, depuis le mois de septembre 2020, été suspendue par la commune au poste n° 2 de la tranche ferme, soit au stade de la conception, dans le cadre d'un moratoire sur le projet global* », et que le dispositif mis en œuvre n'en serait donc « *qu'à une phase de test et de recherche pour laquelle une cinquantaine de caméras fixes ont été installées, lesquelles ne sont pas reliées au réseau principal de vidéoprotection et dont les flux vidéos sont automatiquement effacés dans un délai de dix jours* » (pt. 8).

27. Or, ce faisant, le jugement attaqué, reprenant à son compte les allégations controuvées de la commune sur ce point, opère une contradiction de motifs : la suspension d'un contrat ne peut avoir pour conséquence de laisser perdurer une « *cinquantaine* » de caméras actives, dont les images captées sont pourtant bien traitées par le dispositif litigieux. Bien au contraire, le fait qu'une cinquantaine de caméras soit active montre bien que le contrat n'est nullement suspendu : au mieux, on pourrait considérer que le déploiement de nouvelles caméras aurait été suspendu (ce qu'affirme la commune, mais sans commencement de preuve pour l'étayer), ce qui reste ainsi sans incidence sur les caméras déjà installées, donc sur l'exécution du contrat.

28. L'exposante avait pourtant bien relevé, dans son mémoire en réplique du 5 août 2022 (§§. 23 et s.), cette contradiction manifeste dans les affirmations de la commune. Ainsi, le jugement dénature les écritures de l'exposante lorsqu'il affirme que « *la commune fait valoir, sans être contestée, que le dispositif de "vidéoprotection intelligente" tel qu'il existe actuellement n'est nullement finalisé* » (jugement attaqué, pt. 8, *in medio*).

29. Ainsi, le jugement attaqué ne pouvait, après avoir constaté qu'une cinquan-

taine de caméras étaient toujours mises en œuvre dans l'espace public, considérer l'exécution du contrat suspendue puisque ces caméras, toujours mises en œuvre dans l'espace public, l'étaient uniquement en application du contrat litigieux.

30. Par ailleurs, si seule une cinquantaine de caméras est mise en œuvre, c'est que l'exécution du contrat, bien qu'en cours, n'en est qu'à son commencement. Ainsi, ni l'intérêt général ni le principe de sécurité juridique ne s'opposent à la résiliation d'un contrat qui n'a pas *encore* été exécuté entièrement.

31. **Il en résulte que** le jugement attaqué est entaché d'une erreur de droit, d'une erreur manifeste d'appréciation, d'une contradiction de motifs et d'une dénaturation des écritures de l'exposante en considérant que la poursuite de l'exécution du contrat à la date du jugement ne serait pas manifestement contraire à l'intérêt général en raison de la prétendue suspension de son exécution.

C. En ce qui concerne le caractère illicite de l'objet du contrat litigieux

32. **En troisième lieu**, c'est au prix d'une erreur de droit et d'une erreur manifeste d'appréciation que le jugement attaqué n'a pas soulevé d'office le moyen tiré de l'illicéité de l'objet même du contrat litigieux.

33. **En droit**, le contenu d'un contrat présente un caractère illicite si l'objet même du contrat, tel qu'il a été formulé par la personne publique contractante pour lancer la procédure de passation du contrat ou tel qu'il résulte des stipulations convenues entre les parties qui doivent être regardées comme le définissant, est, en lui-même, contraire à la loi, de sorte qu'en s'engageant pour un tel objet, le cocontractant de la personne publique la méconnaît nécessairement (*cf.* CE, 9 novembre 2018, *Société Cerba et Caisse nationale d'assurance maladie*, n^{os} 420654 et 420663, Rec. p. 407).

34. Ce moyen tiré de l'illicéité de l'objet du contrat est d'ordre public (même décision).

35. **En l'espèce**, l'objet du contrat porte sur la fourniture d'un dispositif de vidéosurveillance algorithmique, c'est-à-dire une analyse automatisée des images

de l'espace public.

36. Comme cela a longuement été décrit et expliqué par l'exposante, ce type de dispositif doit s'analyser comme un traitement de données personnelles, voire d'un traitement de données biométriques ou, à tout le moins, un traitement de données sensibles. Or, un tel traitement de données est, par nature, illégal, de sorte qu'un contrat portant sur la conception et la mise en œuvre de ce type de dispositif porte sur un objet illicite.

37. Si l'exposante n'a pas directement rattaché ses constatations au moyen tiré de l'illicéité du contrat, le tribunal administratif de Marseille aurait dû le soulever d'office. Au contraire, il s'est borné à écarter le moyen tiré de la présence d'un traitement de données biométrique, en le considérant (au demeurant à tort) comme inopérant, alors qu'il avait à sa disposition tous les éléments de faits et de droit, développés par l'exposante dans ses développements sur la qualification juridique des faits, pour constater que le contrat litigieux porte sur un objet manifestement illicite.

38. En particulier, comme souligné par l'exposante dans son mémoire en réplique du 5 août 2022 (*cf.* mémoire en réplique du 5 août 2022, § IV), le dispositif litigieux ne dispose d'aucune base légale, comme a pu le rappeler à de nombreuses reprises la Commission nationale de l'informatique et des libertés (ci-après « la CNIL »). L'autorité expliquait ainsi dans sa position sur les « caméras intelligentes » que « *la CNIL considère que les caméras encadrées par le* [code de la sécurité intérieure] *ne sont pas* de facto *"autorisées" à utiliser des technologies de vidéo "augmentée" y compris pour les finalités ayant permis leur implantation : le législateur n'a entendu encadrer par le* [code de la sécurité intérieure] *que des dispositifs de vidéo "simples", qui ne captent pas le son et ne sont pas équipés de traitements algorithmiques d'analyse automatique* » (*cf.* pièce n° 19, pt. 4.1).

39. **Il en résulte que** c'est au prix d'une erreur de droit et d'une erreur manifeste d'appréciation que le jugement attaqué n'a pas soulevé d'office le moyen tiré de l'illicéité de l'objet même du contrat litigieux.

D. En ce qui concerne la délégation de compétence d'une autorité publique à une personne de droit privé

40. **<u>En quatrième lieu</u>**, c'est au prix d'une erreur manifeste d'appréciation que le jugement attaqué a considéré que le traitement litigieux ne déléguerait pas au prestataire une compétence ne pouvant légalement appartenir qu'à autorité publique.

41. **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* ».

42. 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.* »

43. 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* […] » (*cf.* Cons. const., 10 mars 2011, n° 2011-625 DC, *Loi d'orientation et de programmation pour la performance de la sécurité intérieure*, cons. 19).

44. 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, p. 10).

45. Ainsi, 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.

46. **En l'espèce**, c'est à tort que le jugement attaqué retient, pour écarter le moyen tiré de la délégation de compétence d'une autorité publique à une personne de droit privée, que « *le logiciel ou les agents de la société cocontractante* [n']*apprécient* [pas] *si les faits survenus sur la voie publique constituent une atteinte à l'ordre public ou une infraction pénale* » (pt. 6).

47. En effet, comme cela avait pourtant été souligné par l'exposante, le dispositif litigieux vise, précisément, à analyser ce qui se passe sur l'espace public pour détecter de potentiels troubles à l'ordre public. La décision finale est donc influencée par le dispositif attaqué et c'est même son objet : pour ne pas avoir à analyser humainement toutes les situations, cette analyse est confiée au traitement litigieux.

48. Le dispositif litigieux consiste très certainement en un algorithme dit de « *machine learning* ». Pendant une première période d'apprentissage, l'algorithme s'adapte à partir d'un jeu de données dont la nature (présence d'un trouble à l'ordre public ou absence de trouble à l'ordre public) est connue. Une fois cet apprentissage jugé suffisant par le responsable de traitement, l'algorithme est chargé de déterminer, à partir des situations apprises pendant la phase d'apprentissage, la nature d'un nouveau jeu de données (c'est-à-dire de déterminer si ces nouvelles données constituent ou non un trouble à l'ordre public, sans, cette fois-ci, que le résultat ne soit connu). Le résultat de la deuxième phase dépend donc nécessairement de la première phase d'apprentissage.

49. Ainsi, c'est bien le concepteur des algorithmes d'analyse qui détermine ce que constituera un trouble à l'ordre public ou, au contraire, ce qui ne constituera pas un tel trouble, dès lors que c'est lui, et lui seul, qui, d'une part, détermine les images qui servent à l'apprentissage et, d'autre part, maîtrise le code source du dispositif.

50. Comme l'avait rappelé l'exposante devant le tribunal administratif de Marseille, le degré d'importance du dispositif litigieux dans la prise de décision est par ailleurs très élevé puisque le contrat litigieux mettant en place une surveillance algorithmique vise à « *rationaliser le travail de recherche pour optimiser celui du direct* » (*cf.* pièce n° 7, p. 5). La commune de Marseille admettait par ailleurs dans son mémoire en défense qu'une analyse exclusivement humaine des images de vidéosurveillance n'est pas compatible avec le nombre de caméras (*cf.* mémoire en défense du 2 août 2021, § 4).

51. Enfin, le dispositif litigieux ne constitue pas une aide à toutes les décisions : dans beaucoup de cas c'est le dispositif seul qui prend une décision, sans contrôle humain. En effet, alors que dans le cas où le dispositif litigieux estime que la situation analysée constitue un trouble à l'ordre public une personne humaine vérifiera le résultat, une telle vérification humaine est totalement absente dans le cas où le dispositif litigieux estime que la situation analysée ne constitue pas un trouble à l'ordre public.

52. Or, décider de ce qui ne relève pas d'un trouble à l'ordre public est aussi important que de décider de ce qui en relève : le dispositif litigieux peut, seul et sans contrôle, décider qu'un comportement analysé ne pose pas de problème et, en n'émettant pas d'alerte, aboutir à l'absence de mesure sur le terrain.

53. **Il en résulte que** c'est à tort que le jugement attaqué a considéré que le contrat litigieux ne constituait pas une délégation de compétence d'une autorité publique à une personne de droit privé.

54. Partant, le jugement attaqué ne pourra qu'être annulé.

II. Sur le fond de l'affaire

A. En ce qui concerne l'intérêt à agir de La Quadrature du Net et la recevabilité de son recours

55. D'emblée, il convient de rappeler que l'intérêt à agir de La Quadrature du Net est acquis.

56. **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).

57. 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* » (même décision).

58. 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).

59. En ce qui concerne les associations de défense d'intérêts généraux, la cour administrative de Nantes a par exemple jugé que des associations de défense des

milieux aquatiques justifient d'un intérêt suffisamment direct et certain à contester des conventions de concession d'utilisation du domaine public maritime pour des projets éoliens *offshore* dans la mesure où ces projet faisaient peser des effets sur l'environnement (*cf.* CAA Nantes, 3 avril 2018, *Association de protection du site des Petites Dalles et autres*, n° 17NT01735).

60. **En l'espèce**, La Quadrature du Net est une association qui promeut et défend 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.

61. 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° 3).

62. 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).

63. Le marché conclu par la commune 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 commune 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.

64. C'est à ce titre que La Quadrature du Net a demandé à la commune 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 commune de Marseille a, par une décision implicite, refusé de résilier ce marché.

65. Par ailleurs, l'intérêt à agir de La Quadrature du Net était reconnu par Mme la rapporteure publique du tribunal administratif de Marseille Célie Simeray dans ses conclusions dans la présente affaire (*cf.* pièce n° 2).

66. *A contrario*, une lecture trop restreinte de l'intérêt à agir dans la présente affaire aurait pour conséquence de priver de tout recours une association de défense des libertés contre un contrat portant sur un dispositif de surveillance des tiers, alors qu'un tel dispositif, s'il n'avait pas fait l'objet d'une contractualisation, aurait pu être attaqué par la voie de l'excès de pouvoir avec une demande d'abrogation de la décision. Ce serait aller frontalement à l'encontre de l'article 6 § 1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après « CESDH ») que de considérer que le recours à un contrat pour prévoir un dispositif de surveillance de tiers fermerait la possibilité de contester cette surveillance.

67. **Il en résulte que** l'association requérante a sans conteste intérêt à agir contre la décision de refus implicite de la commune de Marseille refusant de prononcer la résiliation du contrat conclu avec la société SNEF portant sur l'acquisition d'un dispositif de vidéoprotection intelligente.

68. **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 commune de Marseille refusant de faire droit à sa demande de mettre fin à l'exécution du contrat litigieux, et que celui-ci porte sur un objet illicite.

69. Les moyens articulés ci-après démontrent, d'une part, que la commune 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 Informatique et Libertés et, d'autre part, que la poursuite de l'exécution de ce contrat est manifeste-

ment contraire à l'intérêt général, au sens de la jurisprudence de Section *SMPAT* du 20 juin 2017.

B. En ce qui concerne la qualification juridique des faits

1. Quant au traitement de données biométriques

70. Le marché conclu par la commune de Marseille avec la société SNEF met en place une chaîne de traitements de données personnelles, et plus particulièrement de données biométriques.

71. **En droit**, aux termes du 1 de l'article 3 de la 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*».

72. 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).

73. Par ailleurs, 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 », et dont le traitement est par principe interdit. L'article 10 de la directive « police-justice » reprend cette même définition.

74. 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 le « CEPD »), autorité européenne chargée de garantir l'application effective des règles européennes en matière de données personnelles, détaille, dans ses lignes directrices, 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* » (*cf*. pièce n° 17, pt. 74). Si l'approche du CEPD concerne le règlement UE n° 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après « RGPD »), elle est bien entendu applicable *mutatis mutandis* à la directive « police-justice », cette dernière reprenant exactement les mêmes définitions que le RGPD.

75. Trois conditions sont donc nécessaires, au sens de l'article 3 de la directive « police-justice » et 6 de la loi Informatique et Libertés, pour qu'un dispositif puisse être qualifié de traitement de données biométriques : il faut qu'il y ait un traitement spécifique, qui analyse des caractéristiques physiques, physiologiques ou comportementales des personnes, et qui vise à identifier ces dernières de manière unique.

76. Un traitement technique spécifique s'entend comme incluant tout type d'algorithme ou programme informatique qui serait appliqué aux flux vidéo pour isoler, caractériser, segmenter ou encore rendre apparente une information relative à une personne physique filmée. Ce traitement peut également consister à extraire du flux vidéo, même *a posteriori*, des données biométriques de cette personne.

77. En ce qui concerne l'analyse des caractéristiques physiques ou physiologiques, celles-ci peuvent se rapporter au corps d'une personne filmée au sens large, tels que des visages, des silhouettes ou toute caractéristique isolée du corps, telle la couleur des cheveux, la couleur des yeux, la forme du visage, la taille, le poids,

l'âge. Les données comportementales, quant à elles, visent toute information relative à l'action du corps dans l'environnement et l'espace. Pourront être qualifiés de biométriques un vêtement ou accessoire porté par la personne à un instant *t*, un geste, une expression d'émotion, une direction de déplacement, une position dans l'espace et le temps (assis, debout, statique, allure de la marche, *etc*.).

78. En ce qui concerne l'identification unique, celle-ci 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. Au point 82 de ses 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.* » (*cf*. pièce n° 17, pt. 82)

79. À cet égard, une telle interprétation de la définition de « *traitement biométrique* » est partagée par le Défenseur des droits dans son enquête sur la « *Perception du développement des technologies biométriques en France* » publiée en octobre 2022 (*cf*. pièce n° 23).

80. Ainsi, en introduction, le Défenseur des droits rappelle que les technologies biométriques sont définies comme « *des technologies dont le fonctionne-*

ment consiste à collecter des caractéristiques corporelles spécifiques à chaque personne dans le but d'authentifier, d'identifier ou d'évaluer les individus. Au sens du droit des données personnelles, ces caractéristiques constituent des données biométriques lorsqu'elles font l'objet de traitements spécifiques permettant d'établir l'identification des individus de manière unique. À l'heure où les traitements de données issues du corps humain se multiplient, la présente étude d'opinion aborde ces technologies au sens large, en en dégageant trois finalités principales : l'authentification, l'identification et l'évaluation » (*cf.* pièce n° 23, p. 2).

81. L'autorité estime que les données biométriques doivent, au sens du droit européen des données personnelles – RGPD ou directive « police-justice » qui partagent les mêmes définitions –, également s'entendre comme l'évaluation des personnes à partir du moment où les données traitées pour cette évaluation sont « *des données corporelles et/ou issues de systèmes biométriques* », et que le traitement vise à « *Identifier ou déduire des émotions, des traits de personnalité ou des intentions (on parle alors de systèmes de "reconnaissance des émotions")* », ou bien à « *Inscrire la ou les personnes visées dans des catégories spécifiques, par exemple de sexe, d'âge, de couleur de cheveux, de couleur des yeux, d'origine ethnique ou d'orientation sexuelle ou politique en vue de prendre des mesures spécifiques (on parle alors de systèmes de "catégorisation")* » (*cf.* pièce n° 23, p. 3).

82. Le Défenseur des droits donne ainsi les exemples suivants (même pièce) :

> « *Parmi les services que certaines entreprises affirment pouvoir proposer aujourd'hui, on peut citer l'analyse de la nervosité d'un candidat ou d'une candidate dans le cadre d'une procédure de recrutement, la détection de comportements dits anormaux afin de lutter contre les vols dans les supermarchés, ou encore l'analyse des réactions de consommateurs à la présentation de biens ou de services afin notamment de leur proposer de la publicité ciblée.* »

83. De manière plus générale, il explique que « *les technologies d'évaluation dites également d'analyse (on parle également de vidéo "intelligente" ou "augmentée")* » sont des dispositifs d'évaluation et sont donc, à ce titre, des traitements de données biométriques (même pièce).

84. **En l'espèce**, le traitement litigieux est bien, au sens de l'article 2 de la directive « police-justice », un traitement de données biométriques au sens où il s'agit d'un traitement technique spécifique portant sur les caractéristiques physiques, physiologiques ou comportementales d'une personne physique permettant ou confirmant son identification unique.

85. **Premièrement**, le traitement mis en œuvre par la commune de Marseille consiste à détecter des « *évènements* » vis-à-vis d'individus, tel que le franchissement d'une zone, un dessin de tag, un regroupement (*cf.* pièce n° 7, p. 13) et à appliquer des filtres sur des individus (*cf.* pièce n° 7, p. 15) en ce qui concerne la tranche ferme. La tranche conditionnelle ajoute à ces paramétrages le suivi de « *parcours* » de personnes, des « *bagarres* », « *maraudage* » ou encore des « *rixes* » (*cf.* pièce n° 7, p. 19).

86. Ces opérations sont spécifiques en ce qu'elles ont été conçues pour poursuivre un objectif spécifique (isoler ou repérer une personne de façon unique ; *cf. infra*) et interviennent en addition du traitement général qui consiste à filmer l'espace public.

87. **Deuxièmement**, le traitement litigieux concerne l'analyse des caractéristiques physiques, physiologiques ou comportementales des personnes.

88. En effet, concernant la tranche ferme, les paramétrages impliquent que :

— pour repérer la « *destruction de mobilier urbain* », le logiciel doit être programmé pour la détection d'un mouvement d'un corps prédéfini (corps en train de donner des coups par exemple), soit une **donnée comportementale** ;
— pour analyser un « *tag* », le logiciel détecte l'action d'un corps en train de dessiner près d'un mur ou de manipuler une bombe de peinture par exemple, ce qui est également une **donnée comportementale** prédéfinie ;
— pour détecter le « *franchissement d'une zone* » ou la « *présence dans une zone* », le logiciel doit repérer une direction et/ou la position d'une personne physique par rapport à un critère préétabli (un périmètre ou un lieu), soit, à nouveau, une **donnée comportementale** ;
— pour repérer un « *individu au sol* », le logiciel recherche une position particulière du corps, soit à nouveau une **donnée comportementale**, ce que

la commune concède elle-même (*cf.* mémoire en défense, § 85) ;

— enfin, le filtre « *individu* » prévu pour les usages de police judiciaire implique que les agents de la commune pourront paramétrer le logiciel pour retrouver un individu en particulier à partir d'informations préalables. Ces dernières sont des informations relatives au physique ou à la physiologie de la personne recherchée (par exemple des cheveux noirs, une petite taille, etc.) ou son comportement (par exemple un manteau vert, une démarche rapide.). Dans tous les cas, il s'agit de **données biométriques**.

89. Concernant la tranche conditionnelle :

— la « *reconstitution d'un parcours d'un individu à partir des archives de plusieurs caméras* » implique, de la même manière que le filtre, de paramétrer le logiciel pour que soient repérées certaines informations physiques ou comportementales relatives à l'individu que l'on souhaite trouver dans le flux d'image, soit des **données biométriques** ;

— la détection de « *bagarres* », « *rixes* » et « *agressions* » implique de reconnaître un type de mouvement en particulier ou l'interaction de plusieurs types de silhouettes, soit des **données comportementales** ;

— la détection de maraudage nécessite de reconnaître un comportement statique ou encore allant dans une direction ou à une allure particulière, soit à nouveau une **donnée comportementale**.

90. **Troisièmement**, le dispositif litigieux prévoit l'identification unique des personnes en ce que l'objectif du dispositif est de détecter des « *anomalies / incidents / faits remarquables* » afin « *d'alerter automatiquement les opérateurs* ». Peu importe qu'une action humaine intervienne en parallèle comme l'évoque la commune, l'objectif principal des opérations demandées au dispositif litigieux est d'individualiser une personne physique en réunissant des éléments la concernant afin de la reconnaître et/ou diriger une action ciblée sur cette personne .

91. En effet, afin de détecter un comportement qui s'étend ou se répète dans le temps (tels que le maraudage, une action sur du mobilier urbain, une course, une chute, etc.) le système doit distinguer en continu une même personne sur plusieurs images du flux vidéo. Il doit être capable de la « reconnaître » d'une image à l'autre,

sans quoi le comportement ne pourra être caractérisé. Pour ce faire, le système attribue à la personne une identité unique qui n'est pas son état civil mais se compose de l'empreinte numérique d'une ou plusieurs de ses caractéristiques physiques, physiologiques ou comportementales. Par exemple, le système va devoir utiliser l'empreinte numérique associée à une personne qui a dessiné un tag pour reconnaître ce comportement dans les minutes qui suivent la détection.

92. De plus, une fois que le système litigieux a détecté un comportement (que ce comportement soit instantané ou étaler dans le temps), il va généralement chercher à le signaler aux agents humains en encadrant la personne concernée sur leur moniteur vidéo, sur la base de l'empreinte numérique. Cette simple opération, consistant à isoler une personne de façon graphique et unique sur différentes images, implique aussi que le système litigieux confère à la personne une identité unique composée des différentes caractéristiques qui permettent de la « reconnaître » sur le flux vidéo.

93. La fonction de « reconnaissance » est probablement la plus flagrante concernant le suivi d'une personne dans la rue qui est prévu dans la tranche ferme (à travers le paramètre de filtre) et dans la tranche conditionnelle. Ici, le système capture d'abord une première image de la personne, qui n'est alors pas « connue » de lui. À partir de cette première image, il extrait l'empreinte de différentes caractéristiques propres à la personne afin de lui conférer une identité unique. Cette identité unique lui permet ensuite de « reconnaître » la personne sur les images prises ultérieurement, notamment par d'autres caméras.

94. Par ailleurs, en matière de police administrative, la finalité globale du système litigieux n'est pas tant de détecter des comportements que de permettre à des agents humains de réaliser *in fine* certaines actions spécifiques en réaction à ces comportements. Cette finalité consiste à réprimer, éloigner ou mettre en garde les auteurs des comportements jugés indésirables.

95. Tel est précisément l'objectif du système mis en place par la commune de Marseille qui est décrit de la façon suivante dans le PFT au § 7.1.2.1 (*cf.* pièce n° 7, p. 12) :

« *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 (coordination des secours, intervention des équipages terrain, etc…). Il est donc nécessaire que la solution logicielle permette d'effectuer de façon autonome cette visualisation.

La Police Municipale souhaite donc que le système informatique soit capable d'identifier des événements 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. »

96. Pour intervenir ou décider d'une action, les agents doivent être capables d'identifier chaque personne de façon unique parmi les nombreuses autres personnes présentes sur les lieux où le comportement détecté est survenu. Concrètement, le dispositif litigieux et/ou les agents qui consultent les flux vidéo doivent transmettre aux agents sur le terrain une série de caractéristiques physiques, physiologiques et comportementales qui leur permettront de « reconnaître » de façon unique la personne afin d'exercer sur elle l'action ciblée appropriée, peu importe que son état civil soit connu.

97. Par exemple, un agent sur le terrain pourrait recevoir l'ordre de verbaliser un homme d'une trentaine d'années portant une capuche noire et des chaussures rouges et que le dispositif litigieux aura détecté comme venant de dessiner sur un mur. Dans ce contexte, le dispositif litigieux aura transmis à l'agent les informations nécessaires pour que celui-ci puisse identifier de façon unique dans l'espace public la personne ayant réalisé le comportement reproché afin d'exercer sur elle une action ciblée. Sans cette identification préalable, aucune action n'est possible.

98. Ainsi, chacune des deux fonctions du système attaqué (reconnaître et exercer une action ciblée) implique l'identification unique d'une personne.

99. Au demeurant, 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 commune 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° 12).

100. **Il en résulte que**, 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 commune 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 biométriques.

2. Quant au traitement, à tout le moins, de données sensibles

101. Le dispositif litigieux constitue également, à tout le moins, un traitement de données sensibles de manière générale.

102. **En droit**, comme indiqué précédemment, l'article 10 de la directive « police-justice » et 6 de la loi Informatique et Libertés encadrent strictement le traitement des données dites sensibles. Cet article 10 de la directive « police-justice » interdit « *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* ».

103. Cette définition est identique à celle du 1. de l'article 9 du RGPD et s'inscrit dans la continuité du 1. de l'article 8 la directive 95/46/CE.

104. La Cour de Justice de l'Union européenne (CJUE) a, dans un arrêt de grande chambre rendu le 1er août 2022 (*cf.* CJUE, gr. ch., 1er août 2022, *OT c. Vyriausioji tarnybinės etikos komisija*, aff. C-184/20), précisé la notion de donnée

sensible à l'aune de la directive 95/46/CE et du RGPD. Son raisonnement est, *mutatis mutandis*, parfaitement applicables à la définition de données sensibles de la directive « police-justice » et de la loi Informatique et Libertés.

105. Dans cet arrêt, la Cour a ainsi expliqué que les notions de « *catégories particulières de données à caractère personnel* » et de « *données sensibles* » doivent être interprétées de façon large au regard, d'une part, de la prise en compte de l'objectif du RGPD et de la directive 95/46/CE qui « *est de garantir un niveau élevé de protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel les concernant* » et, d'autre part, au regard de la « *nature particulière des données sensibles qui nécessitent une protection accrue* » (§§ 125–126).

106. Elle retient une définition large de la notion de données sensibles, notamment en raison de « *l'objectif de la directive 95/46 et du RGPD* [...] *qui est de garantir un niveau élevé de protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel les concernant* » (§ 125). Elle considère donc que les données personnelles susceptibles de dévoiler, même de manière indirecte, des informations sensibles concernant une personne physique doivent être considérées comme des données sensibles (§ 127).

107. Surtout, la Cour retient de cette interprétation large que les traitements portant sur des données qui, prises indépendamment, ne sont pas sensibles mais qui, par leur recoupement avec d'autres données qui ne sont pas sensibles, peuvent malgré tout révéler des informations sensibles sur les personnes concernées, relèvent de l'article 9 du RGPD (et, *mutatis mutandis*, de l'article 10 de la directive « police-justice »). La Cour précise également que ce recoupement entre données qui ne sont pas sensibles n'a pas à être fait par le traitement lui-même : dans le cas jugée, la CJUE a considéré que la seule publication d'informations sur des personnes qui, recoupées (par le public, par exemple), permettent de « *divulguer indirectement l'orientation sexuelle d'une personne physique* », constitue un traitement de données sensibles.

108. Autrement dit, un traitement de données sensibles est constitué dès lors que sont traitées des données qui, une fois recoupées (par le traitement lui-même ou par un tiers), sont susceptibles de révéler des informations sensibles, même si, par

elles mêmes, ces données sont dépourvues de sensibilité.

109. **En l'espèce**, pour la tranche ferme du contrat, les paramétrages impliquent que le filtre « *individu* » permet aux agents de la commune de retrouver un individu en particulier à partir d'informations préalables (*cf.* pièce n° 7, pp. 14–15). Ainsi, cette fonctionnalité implique que seront traitées des informations relatives au physique ou à la physiologie de la personne recherchée (par exemple des cheveux noirs, une petite taille, *etc*.) ou son comportement (par exemple un manteau vert, une démarche rapide ou lente, *etc*.).

110. À supposer, pour les seuls besoins de la discussions, que ces données ne soient pas, prises individuellement, des données sensibles – *quod non* –, leur recoupement (par le traitement lui-même ou l'agent qui effectuera les paramétrages pour retrouver la personne) permet de révéler des informations sensibles sur les personnes concernées. En particulier, les données ainsi recoupées permettent *a minima* de révéler « *l'origine raciale ou ethnique* », voire « *la santé* », « *la vie sexuelle ou l'orientation sexuelle* » des personnes concernées, par exemple si la personne porte des vêtements marquant une appartenance politique, ou si sa démarche indique un problème de santé.

111. Pour la tranche conditionnelle, les données de « *reconstitution d'un parcours d'un individu à partir des archives de plusieurs caméras* », de détection de « *bagarres* », « *rixes* », « *agressions* » ou de « *maraudage* » (*cf.* pièce n° 7, p. 19), impliquent notamment d'isoler une personne du reste de la foule puis de catégoriser son comportement.

112. Or, à supposer ici encore, pour les seuls besoins de la discussions, que ces données ne soient pas, prises individuellement, des données sensibles – *quod non* –, elles permettent, par leur recoupement, de révéler des informations sensibles sur la personne concernée. Ce recoupement permet notamment de révéler les individus avec qui la personne concernée serait en contact ou les lieux fréquentés. Or, la connaissance du graphe social [1] d'une personne ou les lieux fréquentés permet sans aucun doute de révéler « *les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale* », ou « *la vie sexuelle ou l'orientation*

1. Un graphe social est la représentation logique des relations qu'entretient une personne. Il permet de représenter avec qui une personne est en relations, et à quel niveau d'intensité. Source : `https://en.wikipedia.org/wiki/Social_graph`.

sexuelle », par exemple si la personne concernée fréquente un local syndical, un bar LGBT, ou encore rencontre une personnalité politique.

113. **Il en résulte que**, l'analyse et la reconnaissance – par le traitement litigieux – de certaines données comportementales, physiques ou physiologiques, et de façon générale les données relatives aux corps et à la localisation des personnes filmées, dès lors qu'elles sont recoupées avec d'autres informations, peuvent révéler l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale ou encore des données concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne physique. Le traitement litigieux doit donc être interprété comme un traitement de données sensibles au sens de l'article 6 de la loi Informatique et Libertés et 10 de la directive « police-justice ».

C. En ce qui concerne les moyens propres à conduire à ce qu'il soit mis fin au contrat attaqué

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

115. Le contrat est manifestement illégal en ce que son objet est illicite (1), qu'il a été conclu en l'absence d'analyse d'impact (2) et prévoit un traitement de données personnelles manifestement disproportionné (3). Il ne respecte pas non plus les conditions de légalité d'un traitement de données sensibles (4) et entraîne la délégation de missions de police administrative à une personne privée (5).

1. Quant à l'illicéité de l'objet du contrat

116. **<u>En premier lieu</u>**, le contrat litigieux est illégal en ce que son objet est illicite car dépourvu de toute base légale.

117. **En droit**, le contenu d'un contrat présente un caractère illicite si l'ob-

jet même du contrat, tel qu'il a été formulé par la personne publique contractante pour lancer la procédure de passation du contrat ou tel qu'il résulte des stipulations convenues entre les parties qui doivent être regardées comme le définissant, est, en lui-même, contraire à la loi, de sorte qu'en s'engageant pour un tel objet, le cocontractant de la personne publique la méconnaît nécessairement (*cf.* CE, 9 novembre 2018, *Société Cerba et Caisse nationale d'assurance maladie*, préc., Rec. p. 407).

118. Par ailleurs, aux termes de l'article 8 de la CESDH, intitulé « *Droit au respect de la vie privée et familiale* » :

> « *1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.*
>
> *2. 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.* »

119. La Cour européenne des droits de l'homme (ci-après « CEDH ») 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 CESDH « *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.* CEDH, 25 mars 1983, *Silver et autres c. Royaume-Uni*, n° 5947/72, §§ 85–88).

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

> « *Les mots* "prévue par la loi" *veulent d'abord que la mesure incrimi-*

née 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.* CEDH, 12 juin 2014, *Fernandez Martinez c. Espagne*, n° 56030/07, § 117)

121. 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).

122. 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.

123. Cette exigence de la CESDH est reprise en substance par l'article 4 de la directive « police-justice » et 4 de la loi Informatique et Libertés. Aux termes du 1. de l'article 4 de la directive « police-justice », « *les États membres prévoient que les données à caractère personnel sont : a) traitées de manière licite et loyale ;* [...] ». La loi Informatique et Libertés reprend ce critère en exigeant à son article 4 que « *les données à caractère personnel doivent être : 1° Traitées de manière licite, loyale et, pour les traitements relevant du titre II, transparente au regard de la personne concernée ;* [...] ».

124. La définition de la licéité est donnée à l'article 8 de la directive « police-justice » :

« *1. Les États membres prévoient que le traitement n'est licite que si et dans la mesure où il est nécessaire à l'exécution d'une mission effectuée*

par une autorité compétente, pour les finalités énoncées à l'article 1er, paragraphe 1, et où il est fondé sur le droit de l'Union ou le droit d'un État membre.

2. Une disposition du droit d'un État membre qui réglemente le traitement relevant du champ d'application de la présente directive précise au moins les objectifs du traitement, les données à caractère personnel devant faire l'objet d'un traitement et les finalités du traitement. »

125. L'article 5 de la loi Informatique et Libertés reprend une définition similaire à celle de la directive « police-justice ».

126. La CNIL considère par ailleurs que les dispositions du code de la sécurité intérieure ne concernent pas les dispositifs d'analyses algorithmiques d'images issues des systèmes de vidéosurveillance mis en place sur la voie publique par une autorité publique. Autrement dit, il n'existe aucune base légale pour un traitement de données personnelles consistant en l'analyse des images de caméras autorisées en application du code de la sécurité intérieure : « *la CNIL considère que les caméras encadrées par le* [code de la sécurité intérieure] *ne sont pas* de facto *"autorisées" à utiliser des technologies de vidéo "augmentée" y compris pour les finalités ayant permis leur implantation : le législateur n'a entendu encadrer par le* [code de la sécurité intérieure] *que des dispositifs de vidéo "simples", qui ne captent pas le son et ne sont pas équipés de traitements algorithmiques d'analyse automatique* » (*cf.* pièce n° 19, pt. 4.1).

127. À l'occasion du contrôle d'un dispositif d'analyse automatisé d'images par la ville de Valenciennes, la CNIL estimait déjà que les traitements des images de vidéosurveillance ne relèvent pas des dispositions du code de la sécurité intérieure, mais bien de la loi Informatique et Libertés et de la directive « police-justice », donc que le code de la sécurité intérieur n'était pas une base légale pour ce genre de dispositifs. L'autorité écrivait ainsi que « *les traitements en question apparaissent devoir relever de la directive "police justice" du 27 avril 2016 et des textes pris pour sa transposition (titres I et III de la loi n° 78-17 du 6 janvier 1978 modifiée) en ce que, d'une part, les finalités poursuivies ont trait à la prévention et la détection des infractions pénales, et d'autre part, les traitements sont mis en œuvre par le maire qui constitue une "autorité compétente" au sens de l'article 87 de la loi du 6*

janvier 1978 modifiée, ce dernier disposant de prérogatives de puissance publique dans l'exercice de ses missions de police municipale » (*cf.* pièce n° 20, p. 2). Cette interprétation est applicable, *mutatis mutandis*, à tout dispositif d'analyse algorithmique des images.

128. De plus, les dispositifs biométriques doivent également répondre à une obligation renforcée de base légale. Aux termes de l'article 10 de la directive « police-justice », de tels traitements ne sont possibles, entre autres, que « *lorsqu'ils sont autorisés par le droit de l'Union ou le droit d'un État membre* ». Cette exigence est reprise par l'article 88 de la loi Informatique et Libertés, qui précise qu'un traitement de données biométriques n'est possible que « *s'il est autorisé par une disposition législative ou réglementaire* ».

129. **En l'espèce**, comme démontré ci-avant, le dispositif litigieux consiste en un traitement de données personnelles, dont des données biométriques ou, à tout le moins, de données sensibles.

130. Le dispositif litigieux excède largement les fonctionnalités classiques de vidéosurveillance prévues par le code de sécurité intérieure. En particulier, les fonctionnalités d'analyse des images 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.

131. Ce faisant, un tel traitement de données doit reposer sur une base légale spécifique.

132. En matière de police administrative, le dispositif n'est pourtant prévu par aucune base légale, ainsi que l'a rappelé la CNIL dans sa position sur la « vidéosurveillance intelligente » (*cf.* pièce n° 19, pt. 4.1) et dans un courrier à la commune de Valenciennes concernant un dispositif similaire (*cf.* pièce n° 20, p. 2).

133. Par ailleurs, si l'article 10 de la loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions a donné une base légale pour certains dispositifs de vidéosurveillance algorithmique utilisés pour des missions de police administrative, cette base légale ne couvre aucunement le dispositif prévu dans le contrat litigieux, dans la mesure où ne

seront autorisés par cette loi que certains dispositifs dont l'élaboration et l'exploitation seront de la responsabilité de l'État et non des communes. Bien au contraire, cette loi démontre que ce type de dispositifs ne dispose d'aucune base légale dans la mesure où le législateur n'a voulu autoriser des dispositifs de vidéosurveillance algorithmique que dans certains cas seulement, sous le contrôle de l'État.

134. En matière de police judiciaire, le dispositif souffre également d'une absence base légale. Dans ses écritures devant le tribunal administratif de Marseille, la commune de Marseille affirmait, à tort, que le dispositif litigieux aurait comme base légale l'article 60-1 du code de procédure pénale. Pour rappel, aux termes du premier alinéa de cet article :

> « *Le procureur de la République ou l'officier de police judiciaire ou, sous le contrôle de ce dernier, l'agent de police judiciaire ou, dans le cas prévu au 3° de l'article 21-3, l'assistant d'enquête peut, par tout moyen, requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des informations intéressant l'enquête, y compris, sous réserve de l'article 60-1-2, celles issues d'un système informatique ou d'un traitement de données nominatives, de lui remettre ces informations, notamment sous forme numérique, le cas échéant selon des normes fixées par voie réglementaire, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel.* [...] »

135. Il ressort de cet article qu'une commune est seulement autorisée à communiquer les images de vidéosurveillance qu'elle détient, sur réquisition de l'autorité judiciaire. Cette communication n'implique donc aucunement une recherche par filtres, ni humaine, ni algorithmique, qui relève de missions de police judiciaire qu'une commune ne détient pas. En pratique, lorsqu'une telle réquisition est exigée par l'autorité judiciaire, une commune doit seulement fournir les images qu'elle détient, indépendamment de son contenu. L'analyse des images – et la détermination de l'utilité ou non pour l'enquête – ne sera pas faite par la commune mais par l'autorité judiciaire elle-même. Il ne peut en aller autrement sans que la commune ne s'arroge des pouvoirs de police judiciaire qu'elle ne détient légalement pas.

136. **Il en résulte que**, le dispositif litigieux ne disposant pas de base légale,

ni en police administrative, ni en police judiciaire, le contrat litigieux porte sur un objet manifestement illicite. La résiliation du contrat litigieux est, de ce seul chef, acquise.

2. Quant à l'absence d'analyse d'impact finalisée avant la conclusion du marché

137. **En deuxième lieu**, la poursuite du contrat litigieux est manifestement contraire à l'intérêt général dans la mesure où le dispositif ainsi mis en œuvre n'a fait l'objet d'aucune analyse d'impact sur la protection des données (AIPD) en violation de l'article 90 de la loi Informatique et Libertés.

138. **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* ».

139. 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* ».

140. Enfin, dans ses « Lignes directrices concernant l'AIPD et la manière de déterminer si le traitement est susceptible d'engendrer un risque élevé aux fins du règlement (UE) 2016/679 » (*cf.* pièce n° 18), 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° 18, p. 4).

141. 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° 18, p. 17).

142. **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* » (pièce n° 7, p. 5).

143. 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° 7, p. 12).

144. 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° 7, p. 13).

145. Il permet d'« *analyser et fusionner les informations provenant de plusieurs capteurs et dont la finalité est de constituer une aide à la décision* » (pièce n° 7, p. 6).

146. 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.

147. 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.

148. Enfin, comme précisé ci-avant, il s'agit notamment d'un traitement de données biométriques ou, à tout le moins, de données sensibles.

149. 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 commune 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° 16, p. 1).

150. Or, il ressort des documents obtenus par la requérante que, au 28 septembre 2020, l'analyse d'impact transmise par la commune 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° 16).

151. Par ailleurs, la CNIL affirmait également dans un courrier adressé à l'exposante daté du 30 octobre 2020 avoir « *d'ailleurs appelé la ville de Marseille à compléter l'AIPD portant sur le projet précité* », l'autorité ne disposant pas « *d'une version définitive et complète de l'AIPD* » (*cf.* pièce n° 22).

152. Cela signifie que le contrat a été conclu, puis le dispositif mis en place, sans qu'aucune AIPD finalisée n'ait été réalisée. À ce jour, le dispositif litigieux est toujours mis en œuvre sans qu'aucune AIPD finalisée n'ait été produite et transmise à la CNIL.

153. 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 commune de Marseille ainsi que les mesures appropriées à mettre en place pour la protection des personnes concernées.

154. 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).

155. Conformément aux motifs développés ci-dessous, un telle étude d'impact aurait conduit la commune 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.

156. **Il en résulte** que la poursuite de l'exécution du contrat est manifestement

contraire à l'intérêt général dans la mesure où aucune étude d'impact n'a été encore réalisée.

3. Quant au caractère excessif et inadéquat du traitement en litige

157. **En troisième lieu**, la poursuite du contrat litigieux est manifestement contraire à l'intérêt général en ce que le dispositif ainsi mis en œuvre méconnaît l'article 8 de la CESDH, l'article 4 de la loi Informatique et Libertés, lu à la lumière de 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.

158. **En droit**, comme rappelé ci-avant, l'article 8 de la CESDH proclame le droit à la vie privée.

159. L'article 4 de la directive « police-justice » dispose quant à lui 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* ». Cette exigence est reprise par le 3° de l'article 4 de la loi Informatique et Libertés qui exige que « *Les données à caractère personnel doivent être :* […] *3° 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* ».

160. À ce titre, le considérant 26 de la directive « police-justice » 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* ».

161. 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 » (*cf.* pièce n° 21).

162. 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* ».

163. Plus topique encore, le juge des référés du tribunal administratif de Montreuil, saisi de la légalité d'un dispositif d'analyse automatisée d'images et de sons à des fins de lutte contre la fraude aux examens, a considéré que « *la vérification automatisée de l'identité du candidat, l'analyse continue de son visage filmé, l'analyse continue de son regard, l'accès à l'ensemble des données stockées sur son ordinateur, la captation et l'analyse automatisée de l'environnement sonore et visuel* [...] [porte] *une atteinte excessive au droit à la protection des données personnelles que les candidats tirent du règlement général sur la protection des données* » (*cf.* TA Montreuil, ord., 14 décembre 2022, [redacted], n° 2216570, pt. 8). Cette constatation est, *mutatis mutandis*, applicable à la directive « police-justice ».

164. Ainsi, 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.

165. **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 commune, dans le cadre des dispositions de l'article L. 2212-1 et L. 2212-2 du code général des collectivités territoriales.

166. 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° 7, p. 12).

167. 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° 7, p. 14).

168. C'est au titre de ces deux objectifs que le dispositif prévoit le traitement d'un grand nombre de données, notamment biométriques. 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° 5, pp. 12–13 et 19).

169. La commune 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° 5, p. 12).

170. Il n'est par ailleurs à aucun moment indiqué en quoi un tel traitement de données, pratiqué sur l'espace public à Marseille, serait adéquat, pertinent et manifestement non-excessif par rapport à l'objectif poursuivi, c'est-à-dire strictement nécessaire au regard de la finalité. La commune 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.

171. **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. Partant, son exécution porte atteinte aux droits de toute personne qui serait filmée par une des caméras du dispositif ; la poursuite de l'exécution du contrat irait donc manifestement à l'encontre de l'intérêt général.

4. Quant au non-respect des conditions de légalité d'un traitement de données sensibles

172. **En quatrième lieu**, le contrat litigieux porte sur un objet illicite et la poursuite de son exécution va manifestement à l'encontre de l'intérêt général dans la mesure où est mis en œuvre un dispositif illégal, en ce qu'il met en place un traitement de données biométriques ou, à tout le moins, un traitement de données sensibles, en violation des articles 6 et 88 de la loi Informatique et Libertés, lus à la lumière des article 8 et 10 de la directive « police-justice ».

173. **En droit**, l'article 8 de la directive « police-justice » précise ce qu'il faut entendre par licéité du traitement :

« *1. Les États membres prévoient que le traitement n'est licite que si et dans la mesure où il est nécessaire à l'exécution d'une mission effectuée par une autorité compétente, pour les finalités énoncées à l'article 1er, paragraphe 1, et où il est fondé sur le droit de l'Union ou le droit d'un État membre.*

2. Une disposition du droit d'un État membre qui réglemente le traitement relevant du champ d'application de la présente directive précise au moins les objectifs du traitement, les données à caractère personnel devant faire l'objet d'un traitement et les finalités du traitement. »

174. En matière de données personnelles, la CJUE rappelle systématiquement que la directive 95/46/CE « *vise à garantir un niveau élevé de protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel* » (*cf.* CJUE, gr. ch., 13 mai 2014, *Google Spain SL et Google Inc.*, aff. C-131/12, pt. 66 ; CJUE, 11 décembre 2014, *Ryneš*, préc., pt. 27 ; CJUE, gr. ch., 5 juin 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, aff. C-210/16, pt. 26). La Cour applique ce cadre méthodologique strict également au RGPD (*cf.* CJUE, 6 octobre 2020, *La Quadrature du Net e.a.*, aff. C-511/18, C-512/18 et C-520/18, pt. 207 ; CJUE, gr. ch., 1er août 2022, *Vyriausioji tarnybinės etikos komisija*, aff. C-184/20, pt. 61 ; CJUE, gr. ch., 16 juillet 2020, *Facebook Ireland et Schrems*, aff. C-311/18, pt. 101). Ce cadre doit également être appliqué, *mutatis mutandis*, à la directive « police-justice », ces textes partageant les mêmes définitions et principes.

175. Par ailleurs, ce contrôle de proportionnalité se retrouve renforcé lorsque des données sensibles sont traitées. Ainsi, aux termes de l'article 88 de la loi Informatique et Libertés :

« *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 per-*

sonne concernée. »

176. Les articles 88 et 6 de la loi Informatique et Libertés sont issus de la transposition de l'article 10 de la directive « police-justice », aux termes duquel :

> « *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.* »

177. Il ressort de l'article 88 de la loi Informatique et Libertés, lu à la lumière de l'article 10 de la directive « police-justice », que le contrôle de proportionnalité d'un traitement de données sensibles est renforcé. N'est plus seulement exigée une simple « nécessité », mais désormais une « nécessité absolue ».

178. La CJUE a récemment précisé, à l'occasion de son arrêt *Ministerstvo na vatreshnite raboti* (*cf.* CJUE, 26 janvier 2023, aff. C-205/21), le cadre d'interprétation de l'exigence de « nécessité absolue ». Loin d'être un simple effet de style, l'exigence de « nécessité absolue » renforce les conditions à respecter pour qu'un traitement de données sensibles soit licite :

> « *117.* […] *ainsi qu'il résulte des termes mêmes dans lesquels elle est énoncée à l'article 10 de la directive 2016/680, l'exigence selon laquelle le traitement de telles données est autorisé "uniquement en cas de nécessité absolue" doit être interprétée comme définissant des conditions renforcées de licéité du traitement des données sensibles, au regard de celles qui découlent de l'article 4, paragraphe 1, sous b) et c), et de l'article 8, paragraphe 1, de cette directive, lesquelles se réfèrent seulement à la "nécessité" d'un traitement de données relevant, de manière générale, du champ d'application de ladite directive.*
>
> *118. Ainsi, d'une part, l'emploi de l'adverbe "uniquement" devant l'expression "en cas de nécessité absolue" souligne que le traitement de catégories particulières de données, au sens de l'article 10 de la directive 2016/680, ne pourra être considéré comme nécessaire que dans un nombre limité de cas. D'autre part, le caractère "absolu" de la nécessité d'un traitement de telles données implique que cette nécessité soit appréciée de manière particulièrement rigoureuse.* »

179. Dans son arrêt, la CJUE rappelle que la « nécessité » doit déjà s'interpréter de manière rigoureuse, donc que l'exigence de « nécessité absolue » est encore plus stricte (*ibid.*, pt. 126) :

> « […] *il doit être rappelé, ainsi qu'il ressort du considérant 26 de la directive 2016/680, que l'exigence de nécessité est remplie lorsque l'objectif poursuivi par le traitement de données en cause ne peut raisonnablement être atteint de manière aussi efficace par d'autres moyens moins attentatoires aux droits fondamentaux des personnes concernées, en particulier aux droits au respect de la vie privée et à la protection des données à caractère personnel garantis par les articles 7 et 8 de la Charte* […]. »

180. Ainsi, pour que l'exigence de « nécessité absolue » au sens de l'article 10 de la directive « police-justice » soit remplie, la CJUE exige, *premièrement*, que les finalités du traitement soient particulièrement précises (*ibid.*, pts. 122–124). Elle a notamment indiqué que « *les finalités du traitement de* [données sensibles] *ne*

sauraient être désignées dans des termes à caractère trop général, mais requièrent d'être définies de manière suffisamment précise et concrète pour permettre d'évaluer la "nécessité absolue" dudit traitement » (*ibid*., pt. 124).

181. *Deuxièmement*, la CJUE exige une rigueur toute particulière dans l'appréciation du principe de minimisation des données lorsque sont traitées des données personnelles sensibles (*ibid*., pts. 125–127). Ce principe de minimisation des données renforcé s'apprécie au regard des finalités ainsi précisées du dispositifs : la Cour exige notamment du responsable du traitement « *de s'assurer que cet objectif ne peut pas être satisfait en ayant recours à des catégories de données autres que celles énumérées à l'article 10 de la directive 2016/680* » (*ibid*., pt. 126). Elle impose également au responsable de traitement « *qu'il soit tenu compte de l'importance particulière de l'objectif qu'un tel traitement vise à atteindre* » (*ibid*., pt. 127) dans le sens où seul un objectif important pourra justifier le traitement de telles données. Elle précise ainsi qu'« *Une telle importance peut s'apprécier, entre autres, en fonction de la nature même de l'objectif poursuivi, notamment du fait que le traitement sert un objectif concret en lien avec la prévention d'infractions pénales ou de menaces contre la sécurité publique présentant un certain degré de gravité, la répression de telles infractions ou la protection contre de telles menaces, ainsi qu'à la lumière des circonstances spécifiques dans lesquelles ce traitement est effectué.* » (*ibid*.)

182. C'est ainsi que, en appliquant ce cadre méthodologique d'interprétation de la notion de « nécessité absolue », la CJUE a considéré qu'« *une législation nationale qui prévoit la collecte systématique des données biométriques et génétiques de toute personne mise en examen pour une infraction intentionnelle poursuivie d'office est, en principe, contraire à l'exigence énoncée à l'article 10 de la directive 2016/680, selon laquelle le traitement des catégories particulières de données visées à cet article doit être autorisé "uniquement en cas de nécessité absolue".* » (*ibid*., pt. 128) Elle a considéré qu'une législation qui « *est susceptible de conduire, de manière indifférenciée et généralisée, à la collecte des données biométriques et génétiques de la plupart des personnes mises en examen dès lors que la notion d'"infraction pénale intentionnelle poursuivie d'office" revêt un caractère particulièrement général et est susceptible de s'appliquer à un grand nombre d'infractions pénales, indépendamment de leur nature et de leur gravité* » (*ibid*., pt. 129).

183. Appliqué au cas d'une collecte de données biométriques pour toute per-

sonne mise en examen dont la Cour était saisie, elle considère que la circonstance selon laquelle le traitement de données sensibles est limité au cas « *des personnes pour lesquelles il existe des motifs sérieux de croire qu'elles ont commis une infraction pénale* » n'est pas suffisante pour que l'exigence de « nécessité absolue » du traitement soit remplie (*ibid*., pt. 130). La CJUE relève que, dans ce cas de collecte systématiques de données biométriques de personnes mises en examen, « *il pourra se produire des cas où la collecte* [de ces données] *n'obéira à aucune nécessité concrète aux fins de la procédure pénale en cours* » (*ibid*., pt. 131) alors qu'il aurait fallu, pour qu'une telle collecte de données biométriques soit absolument nécessaire, déterminer les cas de collecte « *au regard de l'ensemble des éléments pertinents, tels que, notamment, la nature et la gravité de l'infraction présumée pour laquelle elle est mise en examen, les circonstances particulières de cette infraction, le lien éventuel de ladite infraction avec d'autres procédures en cours, les antécédents judiciaires ou le profil individuel de la personne en cause* ».

184. **En l'espèce**, comme indiqué ci-avant, le dispositif litigieux mis en œuvre par le contrat attaqué constitue un traitement de données biométriques ou, à tout le moins, un traitement de données sensibles. Or, la nécessité absolue de ce traitement fait manifestement défaut au regard de la jurisprudence précitée de la CJUE.

185. Premièrement, en ce qui concerne les finalités du dispositif, celles-ci ne sont pas suffisamment définies. La commune se contente ainsi, dans les documents du marché public, de présenter son dispositif comme une « *aide aux opérateurs pour identifier, traiter et suivre des évènements* », une « *aide à la décision* », un outil offrant des « *fonctionnalités complémentaires à la sécurité* » (pièce n° 7, p. 12). Comme rappelé ci-avant, elle 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° 5, p. 12). Or, une aide est une notion bien trop large, qui ne permet aucunement d'évaluer en quoi le traitement serait strictement nécessaire.

186. Deuxièmement, en ce qui concerne le principe de minimisation des données, le contrat litigieux ne prévoit aucun critère qui permettrait de limiter les atteintes aux droits fondamentaux. Aussi, le fait que la commune affirme que seule une cinquantaine de caméras est actuellement déployée est sans incidence sur le respect du principe de minimisation des données dans la mesure non seulement où rien, dans le contrat, n'encadre les lieux où sont installées de nouvelles caméras au

dispositif litigieux, mais encore où, dès aujourd'hui avec la cinquantaine de caméras déjà mises en œuvre, n'importe quelle personne passant devant une des cinquante caméras verra ses données personnelles traitées sans que la pertinence de ce traitement n'ait été évaluée.

187. **Il en résulte que** le dispositif mis en œuvre constitue un traitement de données personnelles biométriques ou, à tout le moins, sensibles, alors même que sa « nécessité absolue » fait défaut. Partant, l'objet même du contrat est illicite et la poursuite de son exécution aurait comme conséquence d'imposer aux personnes ainsi filmée un traitement illégal et forcé de leurs données personnelles sensibles, ce qui est manifestement contraire à l'intérêt général.

5. Quant à la délégation de missions de police administrative à une personne privée

188. **En cinquième lieu**, le contrat litigieux est illégal en ce qu'il délègue inconstitutionnellement à une personne privée des compétences de police administrative générale.

189. Comme rappelé ci-avant en ce qui concerne le jugement attaqué, le contrat litigieux procède bien à une délégation de compétence d'une autorité publique à une personne de droit privé (*cf.* « En ce qui concerne la délégation de compétence d'une autorité publique à une personne de droit privé », pp. 11 et s.).

190. **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.

**

191. **En conclusion**, le contrat attaqué porte une atteinte particulièrement grave et manifeste à l'intérêt général en ce qu'il met en place une surveillance algorithmique, automatisée et illégale, de l'espace public marseillais. Ce faisant, n'importe

quelle personne filmée par le dispositif litigieux verra ses données traitées, en violation de ses droits.

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

PAR CES MOTIFS, l'association La Quadrature du Net, exposante, conclut qu'il plaise à la cour administrative d'appel de Marseille :

ANNULER le jugement attaqué, avec toutes conséquences de droit ;

FAIRE DROIT aux demandes que l'exposante a présentées devant le tribunal administratif de Marseille et, notamment, **METTRE FIN À L'EXÉCUTION** du marché conclu le 2 novembre 2018 entre la commune 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 commune de Marseille une somme de 6 144 euros, en application de l'article L. 761-1 du code de justice administrative.

Fait à Toulouse, le 3 août 2023

Alexis FITZJEAN Ó COBHTHAIGH
Avocat au Barreau de Paris

BORDEREAU DES PRODUCTIONS

Pièce n° 1 : Jugement n° 2009485 du tribunal administratif de Marseille du 2 juin 2023 (jugement attaqué) et courrier de notification du jugement ;

Pièce n° 2 : Conclusions de Mme la rapporteure publique du tribunal administratif de Marseille Célie Simeray dans l'affaire n° 2009485 ;

Pièce n° 3 : Statuts de l'association « La Quadrature du Net » ;

Pièce n° 4 : Pouvoir spécial ;

Pièce n° 5 : Avis de marché n° 15-165192, intitulé « Acquisition d'un dispositif de vidéoprotection intelligente, à Marseille », diffusé le 31 octobre 2015 ;

Pièce n° 6 : Avis n° 18-165285, diffusée le 30 novembre 2018 ;

Pièce n° 7 : Programme fonctionnel technique final ;

Pièce n° 8 : Cahier des clauses administratives particulières ;

Pièce n° 9 : Article de M. Olivier Tesquet, « Reconnaissance faciale : pourra-t-on y échapper ? », Télérama, 11 décembre 2019 ;

Pièce n° 10 : 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° 11 : 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° 12 : Ordonnance de rejet du référé-suspension du 11 mars 2020 du tribunal administratif de Marseille ;

Pièce n° 13 : Ordonnance du tribunal administratif de Marseille du 14 mai 2020 ;

Pièce n° 14 : Courrier du 28 juillet 2020 adressé par l'association La Quadrature du Net à la commune de Marseille ;

Pièce n° 15 : Preuves de la distribution du courrier à la commune de Marseille le 3 août 2020 ;

Pièce n° 16 : Courriers envoyés par la CNIL à la commune de Marseille en octobre 2020 ;

Pièce n° 17 : EDPB, Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo, version 2.1, 26 février 2020, URL : `https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_fr.pdf` ;

Pièce n° 18 : 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* ;

Pièce n° 19 : CNIL, Caméras dites « intelligentes » ou « augmentées » dans les espaces publics : position sur les conditions de déploiement ;

Pièce n° 20 : Avertissement de la CNIL à la commune de Valenciennes pour son dispositif d'analyse automatisée des images de vidéosurveillance ;

Pièce n° 21 : Courrier adressé le 25 octobre 2019 au président de la région Provence-Alpes-Côte d'Azur par la CNIL ;

Pièce n° 22 : Courrier de la CNIL adressé le 30 octobre 2020 à l'exposante concernant l'AIPD du dispositif de vidéosurveillance algorithmique de Marseille.

Pièce n° 23 : Enquête du Défenseur des droits « Perception du développement des technologies biométriques en France – Entre manque d'information et demande d'encadrement », octobre 2022.