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

TRIBUNAL ADMINISTRATIF

DE

MARSEILLE

MÉMOIRE EN RÉPLIQUE

N° 2009485

POUR : **L'association « La Quadrature du Net » (LQDN)**

CONTRE : **La commune de Marseille**

Table des matières

FAITS

1. Par une requête datée du 3 décembre 2020 et enregistrée sous le n° 2009485, l'association La Quadrature du Net, exposante, a déféré au tribunal de Marseille le contrat, passé entre la commune de Marseille et la société SNEF, portant sur l'acquisition d'un dispositif dit de « vidéoprotection intelligente » et dont la résiliation a été refusée par une décision implicite de la commune de Marseille.

2. Dans cette requête, l'exposante démontrait son intérêt à agir, ainsi que plusieurs moyens d'illégalité de ce contrat. Elle démontrait notamment que le dispositif prévu par le contrat attaqué était disproportionné, souffrait d'un défaut de base légale suffisante et ne respectait pas les conditions propres aux traitements de données biométriques. De plus, elle a également mis en évidence qu'aucune analyse d'impact sur la protection des données (AIPD) n'avait été régulièrement produite et que ce contrat revenait à déléguer à une entreprise privée des missions de police administrative.

3. Par un mémoire en défense daté du 2 août 2021, la commune de Marseille a conclu au rejet de la requête.

4. Par le présent mémoire, l'exposante entend apporter des observations en réplique aux écritures de la commune de Marseille. Il ne remet nullement en cause les moyens et conclusions précédemment articulés, que l'exposante réitère expressément.

DISCUSSION

I. Sur l'intérêt à agir de l'association La Quadrature du Net

5. **En premier lieu**, l'intérêt à agir de l'association est bien acquis.

6. **En droit**, aux termes de l'article 6 § 1 de la Convention européenne des droits de l'homme et des libertés fondamentales (ci-après « CESDH ») :

> « *Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable, par un tribunal indépendant et impartial, établi par la loi, qui décidera, soit des contestations sur ses droits et obligations de caractère civil, soit du bien-fondé de toute accusation en matière pénale dirigée contre elle.* […] »

7. Il ressort de cet article 6 § 1 que l'accès à un tribunal doit être garanti par le droit national.

8. En droit interne, cet accès à un tribunal est permis à « *un tiers à un contrat administratif susceptible d'être lésé dans ses intérêts de façon suffisamment directe et certaine* » par un contrat. Ce tiers peut contester la validité de ce contrat s'il agit dans le délai de deux mois suivant sa passation (*cf.* CE, Ass., 4 avril 2014, *Département de Tarn-et-Garonne*, n° 358994, Rec. p. 70), ou s'il demande la résiliation de ce contrat (*cf.* CE, Sect., 30 juin 2017, *Syndicat mixte de promotion de l'activité transmanche (SMPAT)*, n° 398445, Rec. p. 209).

9. La pierre angulaire de ce système de contestation du contrat repose sur la notion de « *tiers à un contrat administratif susceptible d'être lésé dans ses intérêts de façon suffisamment directe et certaine* ».

10. Le pendant de l'accès par un tiers au juge du contrat, dont l'office est plus large que celui de l'excès de pouvoir, est de ne pouvoir invoquer « *que des vices en rapport direct avec l'intérêt lésé dont ils se prévalent ou ceux d'une gravité telle*

que le juge devrait les relever d'office » (*cf.* CE, Ass., 4 avril 2014, *Département de Tarn-et-Garonne*, préc., cons. 3).

11. Cette évolution de la jurisprudence – et l'ouverture aux tiers du recours en plein contentieux – participe d'une plus grande ouverture de l'accès au juge du contrat avec en contrepartie une restriction des moyens invocables, afin de ne pas remettre en question de façon déraisonnable la sécurité juridique inhérente à la poursuite d'un contrat.

12. **En l'espèce**, l'association La Quadrature du Net est bien recevable à agir en ce qu'elle est lésée dans ses intérêts de façon certaine et directe.

13. L'exposante défend les libertés à l'ère du numérique. Comme rappelé dans sa requête introductive, son intérêt à agir a été reconnu de multiples fois en excès de pouvoir. Le fait que le présent litige soit dirigé contre un contrat – donc qu'il s'agisse de plein contentieux – ne fait néanmoins pas obstacle à ce que l'intérêt à agir de l'exposante soit reconnu.

14. Premièrement, la spécificité du contrat litigieux implique que l'intérêt à agir de l'exposante, y compris en plein contentieux, soit reconnu. En effet, l'objet du contrat en question est d'imposer aux tiers une surveillance, dans l'espace public. Les tiers à ce contrat sont directement et nécessairement concernés par le contrat litigieux, qui aura des conséquences graves sur les libertés fondamentales de toute personne qui circulerait dans la commune de Marseille et devant l'une de ses nombreuses caméras de vidéosurveillance.

15. Deuxièmement, le contrat entre directement dans le champ de l'objet social de l'exposante. Il est certes vrai qu'aucune juridiction n'a eu directement à se prononcer sur la question de l'intérêt à agir d'une association contre un contrat. Toutefois, si la CAA de Lyon a rejeté le recours d'une association parce que le contrat attaqué n'entrait pas dans l'objet social de l'association requérante, elle semble *a contrario* bien admettre un tel recours devant le juge du contrat dans l'hypothèse où le contrat entre dans l'objet social de l'association requérante (*cf.* CAA Lyon, 13 juillet 2022, *Association A Vent Garde*, n° 20LY00422).

16. Troisièmement, ne pas reconnaître l'intérêt à agir de l'exposante, qui dé-

fend les libertés fondamentales de tous et non les intérêts économiques d'une partie privée ou d'un concurrent évincé, la priverait non seulement de son droit à un recours effectif, mais créerait surtout pour une administration une voie – le contrat – lui permettant de mettre en place un dispositif de surveillance de masse tout en échappant à toute sanction.

17. **Il en résulte que** l'association La Quadrature du Net a bien intérêt à agir contre le contrat dont la résiliation a été demandée.

II. Sur la nature précise du dispositif

18. **En deuxième lieu**, le dispositif litigieux consiste bien en une analyse des images de vidéosurveillance, qui est un traitement de données personnelles.

19. **En droit**, il a été rappelé dans la requête introductive et dans le mémoire en défense de la commune de Marseille que l'article 3 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 ») définit la notion de données personnelles comme « *toute information se rapportant à une personne identifiée ou identifiable* », et celle de traitements 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* » (*cf.* requête introductive, §§ 27–28 ; mémoire en défense, §§ 65–68).

20. Le fait qu'un traitement de données personnelles soit ou non effectivement mis en œuvre n'a aucune incidence ni sur la qualification et l'examen dudit traitement lorsqu'il constitue l'objet d'un contrat, ni sur la légalité dudit contrat. C'est donc la nature du dispositif attaqué telle que prévue par l'acte attaqué, et donc le traitement de données tel que décrit dans le contrat, qui doit être examiné pour le présent litige.

21. Par ailleurs, comme rappelé dans la requête introductive (*cf.* requête introductive, § 28), il résulte de la jurisprudence de la CJUE qu'un dispositif de vidéosurveillance est un traitement de données personnelles (*cf.* CJUE, 14 février 2019, *Buivids*, n° C-345/17, pt. 31 ; CJUE, 11 décembre 2014, *Ryneš*, n° C-212/13, pt. 22). Il en va donc naturellement des traitements postérieurs à la captation des images.

22. À ce sujet, le Conseil d'État a jugé qu'un dispositif de floutage d'images postérieurement à la captation des images par drones est un traitement de données personnelles et que le dispositif de captation par drones est indissociable du dispositif de floutage postérieur (*cf.* CE, 22 décembre 2020, *La Quadrature du Net*, n° 446155, Rec. T. ; TA Paris, 28 juin 2022, *La Quadrature du Net*, n° 2017440).

23. **En l'espèce**, la commune de Marseille avance des arguments contradictoires afin de ne pas qualifier l'objet du contrat de traitement de données personnelles.

24. **D'une part**, elle se contente d'affirmer qu'« *une cinquantaine de caméras fixes* » sont déployées (*cf.* mémoire en défense, § 28), sans donner aucun chiffre exact alors que la commune, en tant que responsable de traitement, connaît précisément le nombre et les caractéristiques des caméras composant le dispositif litigieux.

25. Par ailleurs, c'est bien volontairement que la commune de Marseille entretient le flou sur son dispositif. En effet, par lettre recommandée avec accusé de réception en date du 14 février 2022 et reçue le 21 février dernier (*cf.* pièce n° 17), l'exposante a demandé au maire de Marseille, en application du livre troisième du code des relations entre le public et l'administration, la communication du nom des logiciels utilisés dans le cadre du contrat faisant l'objet du présent litige, ainsi que leurs manuels d'utilisation. Cette demande de communication de documents administratifs est restée sans réponse, caractérisant le choix de la commune de Marseille de faire preuve du moins de transparence possible sur le dispositif attaqué, au mépris du droit à la communication de documents administratifs.

26. **D'autre part**, la commune prétend que le logiciel d'analyse d'images objet du marché devrait être dissocié du système de vidéosurveillance au prétexte que le parc de caméras aurait été installé antérieurement à la conclusion du marché. La commune se permet alors, à tort, de définir le système litigieux comme se limitant

à « *offrir un moyen d'appui à l'exécution matérielle des missions que poursuivent les services de police* » (*cf.* mémoire en défense, § 79). Cette interprétation, qui consiste à séparer les équipements et leur utilisation, est erronée tant juridiquement que techniquement, la captation d'images et le logiciel les analysant étant exploités comme un tout.

27. En effet, premièrement, au paragraphe 6.1 du Programme fonctionnel technique (PFT), il est expressément écrit que la tranche ferme prévoit le « *déploiement de la solution* » (*cf.* pièce n° 5, p. 10). Cette prestation est décrite au paragraphe 7.1.2.4 du même document comme comprenant (*cf.* pièce n° 5, p. 15) :

— « *L'intégration de la solution au système d'information vidéoprotection existant*
— *L'adaptation, au besoin, du système d'information existant en coordination avec l'intégrateur : prise en charge par le titulaire du marché VPI des modifications à apporter au SI existant afin d'intégrer les solutions.*
— *Des phases de test afin de valider entre autre la conformité des outils par rapport au besoin et le bon fonctionnement de la solution en conditions d'exploitation.*
— *La fourniture des licences*
— *Le déploiement et le paramétrage des outils sur les caméras en fonction des fonctionnalités souhaitées par les opérateurs* »

28. C'est donc bien évidemment l'ensemble du dispositif technique qui est concerné par le marché, de sa conception à sa mise en place, en passant par son adaptation au dispositif de vidéosurveillance existant.

29. Deuxièmement, lors d'un premier recours en excès de pouvoir dirigé par la requérante contre l'exécution de ce marché, le tribunal administratif de Marseille a déclaré la requête irrecevable parce que dirigée contre le contrat lui-même (*cf.* TA Marseille, ord., 11 mars 2020, *La Quadrature du Net et autre*, n° 2001080).

30. Il en résulte que c'est bien le dispositif présenté par le marché public consistant en la mise en place d'un dispositif de traitement de données d'images de vidéosurveillance qui doit être pris en compte pour l'analyse requise par le présent litige.

31. Au surplus, la commune concède elle-même l'existence d'un traitement de données personnelles lorsqu'elle affirme de pas ignorer « *que la mise en œuvre du logiciel projeté puisse constituer un traitement de données personnelles* » (*cf.* mémoire en défense, § 73), cette constatation l'ayant conduit à mener une AIPD dont il sera discuté *infra*.

32. Par ailleurs, si la tranche ferme du contrat définit le traitement de données mis en place par la commune, la tranche conditionnelle, même non-affermie, précise quant à elle les évolutions du dispositif litigieux. Le fait que la tranche conditionnelle n'ait pas été affermie et que le dispositif litigieux tel que mis en place dans l'espace public marseillais ne comporte pas de caractéristiques issues de la tranche conditionnelle est sans incidence sur l'illégalité du contrat attaqué (v., pour une analogie avec un décret et les modalités de son exécution, CE, 27 mars 2020, *Association CRPA et autres*, n° 431350, Rec. T., pt. 13 ; CE, 18 octobre 2018, *La Quadrature du Net et autres*, n° 406347, pt. 22).

33. **En conclusion**, le contrat porte bien sur un traitement de données personnelles qui, de surcroît, est déjà partiellement mis en œuvre par la ville de Marseille.

III. Sur la qualification juridique du dispositif en traitement de données biométriques

34. **En troisième lieu**, le dispositif litigieux consiste bien en un traitement de données biométriques.

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

36. **En l'espèce**, la commune de Marseille mobilise les trois critères précités de façon erronée pour exclure la qualification de données biométriques. Or, une exacte application de cette définition au dispositif attaqué, notamment au regard de la doctrine et de la jurisprudence, doit conduire à rejeter les développements de la

commune de Marseille.

37. Il sera donc étudié successivement les critères de définition d'une donnée biométrique, à savoir la présence d'un traitement technique spécifique (A) portant sur les caractéristiques physiques, physiologiques ou comportementales d'une personne physique (B) permettant ou confirmant son identification unique (C).

A. En ce qui concerne la présence d'un traitement technique spécifique

38. **Premièrement**, le dispositif litigieux comporte bien un traitement technique spécifique.

39. **En droit**, 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.

40. **En l'espèce**, 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° 5, p. 13, cité au pt. 18 du mémoire en défense de la commune) et à appliquer des filtres sur des individus (*cf.* pièce n° 5, p. 15, cité au pt. 19 du mémoire en défense de la commune) 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° 5, p. 19, cité au pt. 21 du mémoire en défense de la commune).

41. 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.

42. **En conclusion**, l'ensemble des fonctionnalités prévues dans le dispositif

attaqué, aussi bien par la tranche ferme que par la tranche conditionnelle, consistent donc bien en la mise en en œuvre de traitements techniques spécifiques.

B. En ce qui concerne l'analyse des caractéristiques physiques, physiologiques ou comportementales des personnes

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

44. **En droit**, les informations physiques ou physiologiques 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.

45. Les données comportementales 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.).

46. **En l'espèce**, contrairement à ce qu'affirme la commune de Marseille, le paramétrage du dispositif en cause implique un traitement de ces données.

47. 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**.

48. 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**.

49. **Il en résulte qu'**il ne fait aucun doute que le dispositif attaqué, à la fois dans sa tranche ferme et sa tranche conditionnelle, vise à traiter les données physiques, physiologiques et comportementales des personnes filmées dans l'espace public.

C. En ce qui concerne l'identification unique des personnes

50. **Troisièmement**, le dispositif litigieux prévoit l'identification unique des personnes.

51. **En droit**, contrairement à ce que prétend au prix d'une erreur de droit la commune de Marseille, l'identification unique ne vise pas à authentifier l'identité ou l'état civil d'une personne. Comme cela a été déjà rappelé dans la requête introductive, le Comité Européen de la Protection des Données (CEPD, ou EDPB) a apporté des précisions quant à cette notion d'identification unique qui implique, plus largement, de pouvoir individualiser une personne au sein d'un groupe ou de l'environnement filmé (*cf.* requête introductive §32).

52. **En l'espèce**, 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 (1) et/ou diriger une action ciblée sur cette personne (2).

1. S'agissant de la reconnaissance des personnes

53. 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.

54. De plus, une fois que le système litigieux a détecté un comportement (que

ce comportement soit instantané ou non), 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.

55. 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.

2. S'agissant de l'action ciblée sur les personnes

56. 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.

57. 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° 5, 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. »

58. 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.

59. 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.

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

61. **En conclusion**, une correcte analyse de la définition de données biométriques à travers la caractérisation des trois éléments exposés ci-dessus permet de qualifier le dispositif attaqué, à la fois dans sa tranche ferme et sa tranche conditionnelle, de traitement de données biométriques.

IV. Sur l'absence de base légale

62. **En quatrième lieu**, le dispositif litigieux est contraire à l'article 8 de la CESDH, à la lecture combinée des articles 4 et 8, et 10 de la directive « police-justice », et à la lecture combinée des articles 4 et 5, et 88 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 »), en ce qu'il prévoit une atteinte au droit à la vie privée qui n'est pas prévue par la loi.

63. **En droit**, 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.* »

64. 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).

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

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

66. 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).

67. 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.

68. 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 ;* [...] ».

69. 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. »

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

71. La Commission nationale de l'informatique et des libertés (ci-après « 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° 18, pt. 4.1).

72. 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° 19, p. 2). Cette interprétation est applicable, *mutatis mutandis*, à tout dispositif d'analyse algorithmique des images.

73. **En droit**, toujours, 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* ».

74. **En l'espèce**, comme démontré dans la requête introductive et développé *supra* (*cf.* III. « Sur la qualification juridique du dispositif en traitement de données biométriques »), le dispositif litigieux consiste en un traitement de données personnelles, dont des données biométriques.

75. Le dispositif litigieux dépasse 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.

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

77. En matière de police administrative, le dispositif n'est pourtant prévu par aucune base légale. Il en va de même en matière de police judiciaire.

78. Dans son mémoire en défense, la commune de Marseille se méprend gravement sur le sens à donner à ces exigences et affirme, 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 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.* [...] »

79. 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 s'arroge des pouvoirs de police judiciaire qu'elle ne détient pas.

80. **Il en résulte que** le dispositif litigieux ne dispose pas de base légale, ni en police administrative, ni en police judiciaire.

V. Sur le caractère disproportionné du traitement

81. **En cinquième lieu**, le contrat attaqué est contraire à l'article 4 de la directive « police-justice » et à l'article 4 de la loi Informatique et Libertés en ce qu'il met en œuvre un traitement de données personnelles disproportionné.

82. **En droit**, comme démontré ci-avant (*cf.* II. « Sur la nature précise du dispositif ») et dans la requête introductive (*cf.* requête introductive, §§ 61 et s.), puisque le traitement mis en œuvre par le dispositif litigieux est un traitement de données, l'article 4 de la directive « police-justice », transposé à l'article 4 de la loi Informa-

tique et Libertés, conditionne sa légalité à une exigence de proportionnalité.

83. Ainsi, le Conseil d'État exige que la nécessité d'un dispositif de surveillance par drones soit démontré par le responsable de traitement (*cf*. CE, 22 décembre 2020, *La Quadrature du Net*, préc., pt. 11) :

> « *Eu égard au nombre important de personnes susceptibles de faire l'objet des mesures de surveillance litigieuses et à l'atteinte qu'elles sont susceptibles de porter à la liberté de manifestation et alors que le ministre n'apporte pas d'élément de nature à établir que l'objectif de garantie de la sécurité publique lors de rassemblements de personnes sur la voie publique ne pourrait être atteint pleinement, dans les circonstances actuelles, en l'absence de recours à des drones, la condition d'urgence doit être regardée comme remplie*. »

84. Pour des dispositifs de vidéosurveillance « classique », c'est-à-dire des dispositifs ne traitant pas des biométriques car relevant exclusivement des articles L. 251-1 et suivants du code de la sécurité intérieure, le juge administratif exige que ce genre de dispositif soit proportionné (*cf*. CAA Nantes, 9 novembre 2018, *Commune de Ploërmel*, n° 17NT02743, pt. 5) :

> « *La mise en œuvre de tels systèmes de surveillance doit être assortie de garanties de nature à sauvegarder l'exercice des libertés individuelles. Dès lors leur autorisation suppose qu'une telle mesure soit nécessaire et proportionnée à la préservation de l'ordre public.* »

85. Pour juger que le dispositif n'était en l'espèce pas nécessaire, la Cour administrative d'appel a estimé que :

> « *Si les caméras implantées dans certains sites particuliers, tels la gare ou le bâtiment "Les Carmes", aux abords de la "chapelle bleue" et de l'entrée de la médiathèque, peuvent être regardées comme obéissant aux finalités de protection des bâtiments publics et de leurs abords ou de régulation des flux de circulation, d'autres caméras, notamment installées aux abords des écoles ou à proximité des commerces, bars ou*

autres établissements recevant du public, sans qu'il soit établi, par les statistiques relatives à la délinquance dans la commune, que ces lieux seraient particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants, n'apparaissent pas justifiées par les finalités auxquelles elles doivent correspondre [...]. *Le dispositif autorisé, qui s'étend sans justification légale à presque tous les principaux lieux de vie de la commune, apparaît disproportionné au regard des nécessités de l'ordre public* ».

86. La proportionnalité d'un dispositif est également exigée dans le cas d'une analyse algorithmique des images, indépendamment des conditions propres à la présence d'un traitement de données biométriques. C'est ainsi que, dans le cadre d'un avertissement de la CNIL adressé à la ville de Valenciennes à propos d'un système de vidéosurveillance algorithmique (*cf.* pièce n° 19, p. 3), l'autorité affirmait que :

« *Il incombe à la commune de Valenciennes de faire la démonstration de l'adéquation et de la pertinence des données traitées dans le cadre de analyse d'impact quelle doit effectuer en application de l'article 90 de la loi « Informatique et Libertés». Cette démonstration doit notamment porter sur chaque catégorie de données traitées dans ce cadre, sur chacune des fonctionnalités des logiciels utilisés et sur leur utilité attendue. Elle doit tenir compte du nombre de caméras actuellement déployées, des considérations ayant détermine leur implantation, ou encore de leur niveau d'efficacité connu à ce jour. L'absence d'alternative moins intrusive doit également être documentée. Ainsi, en l'état, la nécessité des traitements d'analyse assistée des images n'apparaît pas établie au regard des finalités poursuivies.* »

87. Par ailleurs, la Cour de Justice de l'UE a récemment précisé que la proportionnalité d'un traitement de données personnelles s'apprécie indépendamment des moyens accordés à l'administration qui en est le responsable de traitement, jugeant que « *le manque de ressources allouées aux autorités publiques ne saurait en aucun cas constituer un motif légitime permettant de justifier une atteinte aux droits fondamentaux garantis par la Charte.* » (*cf.* CJUE, gr. ch., 1er août 2022, *Vyriausioji tarnybinės etikos komisija*, aff. C-184/20, pt. 89)

88. **En l'espèce**, la ville de Marseille échoue en tout point de vue à démontrer la proportionnalité du dispositif. Elle se contente d'énumérer les finalités du logiciel d'analyse algorithmique (« *améliorer le dispositif de vidéoprotection déjà existant* » au point 117 de la défense) sans jamais les mettre en balance au regard des moyens mis en œuvre, comme l'exige un contrôle de proportionnalité classique. Pire, elle se borne à constater que les « *fonctionnalités correspondent aux finalités* », sans chercher la proportionnalité des moyens pour atteindre lesdites finalités (*cf.* mémoire en défense, § 120).

89. Non seulement la commune de Marseille n'a jamais effectué de contrôle de proportionnalité en amont dans le cadre d'une AIPD, mais elle ne justifie à aucun moment dans son mémoire en défense de la nécessité du traitement, ni en démontrant de façon détaillée et chiffrée les risques que le système est censé réduire, ni dans quelle mesure d'autres moyens moins intrusifs ne permettaient pas d'atteindre les objectifs poursuivis.

90. Le contrat attaqué prévoit pourtant que l'ensemble des lieux de vie feront l'objet d'une surveillance algorithmique. C'est d'ailleurs une finalité du dispositif, qui consiste à remplacer (au moins en partie, si ce n'est, en pratique, en totalité), l'analyse humaine. À terme, le contrat attaqué prévoit que le dispositif litigieux couvrira l'ensemble des caméras installées dans l'espace public.

91. Par ailleurs, la commune de Marseille admet 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, § 4), ce que précisait déjà le PFT (*cf.* pièce n° 5, p. 12 : « *Les opérateurs ne peuvent pas visualiser l'ensemble des flux.* »). C'est parce que la commune ne souhaite pas disposer de suffisamment d'agents pour pouvoir analyser l'ensemble des images qu'elle souhaite s'équiper du dispositif litigieux. Or, le peu de moyens humains à disposition de la police municipale de la commune de Marseille n'a pas de conséquence sur la proportionnalité du dispositif (*cf.* CJUE, gr. ch., 1er août 2022, *Vyriausioji tarnybinės etikos komisija*, préc., pt. 89).

92. **Il en résulte que** le contrat attaqué met en place un traitement de données personnelles disproportionné.

VI. Sur le caractère disproportionné du traitement de données biométriques

93. **En sixième lieu**, le contrat attaqué est contraire à l'article 10 de la directive « police-justice » et aux articles 6 et 88 de la loi Informatique et Libertés en tant qu'il met en place un traitement de données biométriques disproportionné.

94. **En droit**, le traitement mis en œuvre par le dispositif litigieux étant un traitement de données biométriques, il doit répondre à des exigences de proportionnalité supplémentaires. L'article 10 de la directive « police-justice » et les articles 6 et 88 de la loi Informatique et Libertés posent un principe d'interdiction de traiter des données sensibles et n'autorisent de les traiter que par exception, en cas de « *nécessité absolue* » et « *sous réserve de garanties appropriées pour les droits et libertés de la personne concernée* ».

95. Ainsi, 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° 20). L'autorité précisait qu'en l'espèce la finalité de sécurisation et de fluidification des entrées au sein de 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* ». Ce raisonnement de la CNIL a été repris par le tribunal administratif de Marseille (*cf.* TA Marseille, 27 février 2020, *La Quadrature du Net et autres*, n° 1901249, pt. 13) et est, *mutatis mutandis*, applicable aux situations régies par les articles 88 de la loi Informatique et Libertés et 10 de la directive « police-justice ».

96. **En l'espèce**, comme rappelé ci-avant à propos de la proportionnalité, le dispositif litigieux échoue à démontrer la moindre proportionnalité.

97. La commune de Marseille échoue ainsi non seulement à démontrer la « *nécessité absolue* » de son dispositif, mais ne démontre aucunement non plus en quoi des « *garanties appropriées* » ont été prises.

98. **Il en résulte que** le contrat attaqué met en place un traitement de données biométriques en absence de toute nécessité absolue et de garanties appropriées à la sauvegarde des droits des personnes concernées.

VII. Sur l'absence d'AIPD

99. **En septième lieu**, le contrat attaqué est contraire à l'article 90 de la loi Informatique et Libertés en ce qu'aucune AIPD n'a été produite, et c'est à tort que la commune de Marseille prétend en défense qu'il conviendrait d'écarter « tout débat » sur l'AIPD.

100. **En droit**, comme la commune l'affirme elle-même dans ses écritures (*cf.* mémoire en défense, §§ 99 et 100), il résulte de l'article 90 de la loi Informatique et Libertés qu'une AIPD est nécessaire avant toute mise en œuvre de traitement de données personnelles.

101. **En l'espèce**, il a été exposé ci-avant que la commune de Marseille a bien commencé à mettre en œuvre le contrat qui a pour objet le traitement de données personnelles litigieux.

102. En outre, si celle-ci a éventuellement rédigé une première version incomplète d'AIPD, aucune version finalisée du document n'a été produite dans le cadre du présent litige permettant de l'attester. De plus, la CNIL elle-même affirmait 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* », celle ci ne disposant pas « *d'une version définitive et complète de l'AIPD* » (*cf.* pièce n° 21).

103. Quand bien même la commune aurait entrepris la réalisation d'une AIPD, celle-ci n'existait pas au moment de la mise en œuvre du traitement et était de surcroît incomplète.

104. **Il en résulte que** le contrat attaqué est exécuté en l'absence d'AIPD.

VIII. Sur la délégation de compétence d'une autorité publique à une personne de droit privé

105. **En huitième lieu**, le contrat litigieux est contraire à l'article 10 de la Déclaration de 1789 en ce qu'il organise une délégation de compétence d'une autorité publique à une personne de droit privé.

106. **En droit**, comme rappelé dans la requête introductive (*cf.* requête introductive, §§ 84 et s.), l'article 12 de la Déclaration de 1789 telle qu'interprétée par le Conseil constitutionnel prohibe le fait que la « force publique », dont la police administrative, soit déléguée à une personne de droit privé.

107. **En l'espèce**, si la commune de Marseille affirme que son dispositif ne consisterait qu'en une aide à la prise de décision, cet élément échoue pourtant à écarter le moyen tiré de la délégation à une personne de droit privé.

108. En effet, premièrement, comme indiqué *supra* (*cf.* §§ 56 et s.), le dispositif vise bien *in fine* à produire des effets sur les personnes surveillées. C'est à partir du résultat d'analyse algorithmique des images par le dispositif litigieux que l'opérateur prendra sa décision : la décision finale est donc influencée par le dispositif attaqué.

109. 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° 5, p. 5). La commune de Marseille admet 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, § 4).

110. Ainsi, l'objectif même du contrat litigieux est de fournir à la commune de Marseille un outil lui permettant d'analyser automatiquement, et non plus humainement, les images. C'est parce que la commune ne souhaite pas disposer de suf-

fisamment d'agents pour pouvoir analyser l'ensemble des images qu'elle souhaite s'équiper du dispositif litigieux. Autrement dit, l'analyse algorithmique remplace l'analyse humaine.

111. Le dispositif litigieux vise donc à « *rationaliser* » la mission de police administrative de la commune, dans le sens où elle souhaite utiliser moins d'humains et plus d'automatisation dans la prise de décisions de police administrative. Même si une confirmation humaine de l'algorithme doit être donnée par l'agent recevant une alerte, celui-ci sera toujours dans une situation de devoir analyser toujours plus d'images et, *in fine*, devra faire confiance au dispositif litigieux.

112. De plus, deuxièmement, si le dispositif litigieux est présenté comme une aide à la prise de décision, il ne s'agit que d'une aide en cas de menace détectée. En effet, lorsque le dispositif litigieux conclut à l'absence de trouble à l'ordre public, aucune alerte ne sera envoyée pour confirmation à un agent humain, en raison de la nature même du dispositif litigieux qui consiste à limiter l'analyse humaine dans le processus de prise de décision.

113. Ainsi, la supposée confirmation humaine d'une situation présentée par la commune de Marseille n'est pas prévue si le dispositif litigieux a estimé que les images ne présentent aucun trouble à l'ordre public. C'est donc bien le dispositif litigieux qui décidera ce qui relève ou non un tel trouble.

114. **Il en résulte que** le contrat attaqué, par sa nature même et en raison de la finalité de remplacer l'analyse humaine par une analyse algorithmique, consiste en une délégation de compétence de la police municipale de Marseille à la SNEF et ses sous-traitants concevant le dispositif litigieux.

115. À tous égards, la résiliation immédiate du contrat, qui ne peut être régularisé en raison de son objet même, s'impose.

PAR CES MOTIFS, l'association La Quadrature du Net, exposante, persiste dans ses conclusions.

Fait à Paris, le 5 août 2022

Alexis FITZJEAN Ó COBHTHAIGH
Avocat au Barreau de Paris

BORDEREAU DES PRODUCTIONS

Pièces déjà communiquées :

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

Pièce n° 2 : Pouvoir spécial ;

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

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

Pièce n° 5 : Programme technique fonctionnel final ;

Pièce n° 6 : Cahier des Clauses Administratives Particulières ;

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

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

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

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

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

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

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

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

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

Pièce n° 16 : Groupe de travail « Article 29 » sur la protection des données, 4 avril 2017, *Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679* ;

Nouvelles pièces :

Pièce n° 17 : Demande de communication du nom et manuels d'utilisation des logiciels utilisés par la ville de Marseille dans le cadre du contrat litigieux ;

Pièce n° 18 : CNIL, Caméras dites « intelligentes » ou « augmentées » dans les espaces publics : position sur les conditions de déploiement ;

Pièce n° 19 : Avertissement de la CNIL à la ville de Valenciennes pour son dispositif d'analyse automatisée des images de vidéosurveillance ;

Pièce n° 20 : Courrier adressé le 25 octobre 2019 au président de la région Provence-Alpes-Côte d'Azur par la CNIL ;

Pièce n° 21 : Courrier de la CNIL adressé le 30 octobre 2020 à l'exposante concernant l'AIPD du dispositif de vidéosurveillance algorithmique de Marseille.