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 enregistrée le 3 décembre 2020, 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. Par un mémoire en défense daté du 2 août 2021, la commune de Marseille a conclu au rejet de la requête. L'exposante a apporté des observations en réplique aux écritures de la commune de Marseille par un mémoire déposé le 5 août 2022.

3. Par le présent mémoire, l'exposante entend apporter des précisions sur la qualification juridique du traitement litigieux. Ce mémoire ne remet nullement en cause les moyens et conclusions précédemment articulés, que l'exposante réitère expressément.

DISCUSSION

I. Sur le traitement de données biométriques par le traitement litigieux

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

5. **En droit**, le 13 de 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 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* ».

6. **En l'espèce**, il a été démontré dans les précédentes écritures de l'exposante (*cf.* requête introductive d'instance du 3 décembre 2020, §§ 29–34 ; mémoire en réplique du 5 août 2022, §§ 34–61) que cette définition s'applique en tout point au traitement litigieux, en ce qu'il analyse et classifie les données physiques, physiologiques et comportementales des personnes.

7. À cet égard, une telle interprétation de la définition de « *traitement biométrique* » est partagée par le Défenseur des droits dans sa récente enquête sur la « *Perception du développement des technologies biométriques en France* » publiée en octobre 2022 (*cf.* pièce n° 22).

8. Ainsi, en introduction, le Défenseur des droits rappelle que les technologies biométriques sont définies comme « *des technologies dont le fonctionnement 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° 22, p. 2).

9. Ainsi, le Défenseur des droits estime que les données biométriques doivent, au sens du droit européen des données personnelles – 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 ») 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° 22, p. 3).

10. 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.* »

11. 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).

12. **En l'espèce**, **premièrement**, le traitement litigieux analyse les données

comportementales, physiques et physiologiques des personnes filmées afin de catégoriser ces comportements (« *anomalies / incidents / faits remarquables* ») tel que par exemple un « *individu au sol* » ou le « *franchissement d'une zone* » par une personne.

13. Il s'agit donc bien d'une catégorisation biométrique : les images des corps sont évaluées par le traitement litigieux qui va les catégoriser pour ensuite déterminer quelle action entreprendre.

Deuxièmement, le dispositif vise également à détecter les comportements anormaux, au-delà d'une seule catégorisation des images.

14. Ainsi, la recherche de « *bagarres* », « *maraudage* » ou « *rixes* » (*cf.* pièce n° 5, p. 19) vise à donner une qualification automatique à des comportements (ces qualificatifs sont classés dans la catégorie « *Comportements anormaux* » par le Programme fonctionnel technique). Ce faisant, il s'agit bien de déduire les « *intentions* », pour reprendre le terme du Défenseur des droits.

15. **Il en résulte que** le dispositif litigieux traite bien des données personnelles biométriques.

II. Sur le traitement, à tout le moins, de données sensibles

16. **En second lieu**, le dispositif litigieux constitue également, à tout le moins, un traitement de données sensibles de manière générale.

17. **En droit**, comme indiqué précédemment (*cf.* requête introductive du 3 décembre 2020, § 29), l'article 10 de la directive « police-justice » et 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 ») 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 ».

18. 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.

19. La Cour de justice de l'Union européenne a récemment donné des précisions sur 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.

20. 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, Rec.), 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).

21. Dans cet arrêt, la Cour 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 retient alors 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).

22. 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.

23. 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.

24. **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° 5, 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*.).

25. 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.

26. **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° 5, p. 19), impliquent notamment d'isoler une personne du reste de la foule puis de catégoriser comportement.

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

28. **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.

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

Fait à Paris, le 8 décembre 2022

Alexis FITZJEAN Ó COBHTHAIGH
Avocat au Barreau de Paris

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`.

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* ;

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.

<u>Nouvelles pièces :</u>

Pièce n° 22 : Enquête du Défenseur des droits « Perception du développement des technologies biométriques en France – Entre manque d'information et demande d'encadrement », octobre 2022.