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 D'ORLÉANS

REQUÊTE INTRODUCTIVE D'INSTANCE

POUR : **L'association « La Quadrature du Net » (LQDN), association régie par la loi du 1er juillet 1901 dont le siège social est situé au 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 : **La convention conclue le 12 octobre 2021 entre la ville d'Orléans et la société Sensivic visant à l'expérimentation d'un dispositif de détection automatisée de sons, en particulier de bruits anormaux.**

L'exposante défère le contrat attaqué à la censure du tribunal administratif d'Orléans. Elle en conteste la validité et requiert qu'il soit annulé, par les motifs suivants.

Table des matières

FAITS

1. La société Sensivic propose une solution de surveillance algorithmique des sons afin de détecter des troubles anormaux. Sur son site Internet (sensivic.com), elle affirme que « *Vos caméras peuvent maintenant avoir des oreilles affutées* [sic] ».

2. Ses produits sont notamment conçus pour détecter les « *anormalités sonores* » afin d'orienter une caméra de vidéosurveillance. La fiche de son produit « Sound-Scanner« indique que la surveillance est « *permanente* » et « *dans un rayon de 40 m* ». Les événements qui peuvent être détectés sont, par exemple, les « *détonations : les coups de feu, les explosions* », les « *bris de vitre* », les « *chocs liés aux véhicules : voitures bélier, accidents* » (*cf.* pièce n° 3).

3. D'autres produits de la société Sensivic permettent de détecter d'autres types d'événements, notamment « *les brusques montées sonores de la voix humaine associées à un rythme de parole anormal* » ou encore les « *effractions* » (même pièce).

4. La société Sensivic met en avant le fait que ses produits sont conçus pour fonctionner avec un système de vidéosurveillance afin d'orienter les caméras vers les événements détectés, pour donner une image sur les possibles troubles détecter algorithmiquement (même pièce).

5. Le 30 septembre 2021, le conseil municipal de la ville d'Orléans a adopté une délibération visant à approuver une convention d'expérimentation entre la ville d'Orléans et la société Sensivic et à déléguer au maire ou à son représentant le pouvoir de signer ladite convention (*cf.* pièce n° 4).

6. Cette délibération a été envoyée et reçue en préfecture le 7 octobre 2021 (*cf.* pièce n° 4).

7. Le 12 octobre 2021, le représentant de la mairie de la ville d'Orléans et la présidente de la société Sensivic ont signé la convention d'expérimentation. Celle-ci a été adressée et réceptionnée à la préfecture le 18 octobre 2021 (*cf.* pièce n° 5).

8. La convention a pour objet de « *déterminer les conditions dans lesquelles la*

société Sensivic pourra réaliser, sur autorisation du Maire de la ville d'Orléans, une expérimentation visant à installer des dispositifs, en certains points du territoire de la Ville, pour la détection de sons, en particulier la détection automatisée de bruits anormaux » (*cf.* pièce n° 5).

9. Il y est précisé en son article 3 que les dispositifs développés par la société Sensivic et faisant l'objet de l'expérimentation « *demandent à être couplés à un système de sécurité et plus particulièrement ceux s'appuyant sur un système de vidéo-protection pour garantir une surveillance optimale* » (*cf.* pièce n° 5).

10. C'est la convention attaquée.

DISCUSSION

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

11. L'association La Quadrature du Net est recevable à demander l'annulation du contrat attaqué.

12. **En droit**, le Conseil d'État juge que « *tout tiers à un contrat administratif susceptible d'être lésé dans ses intérêts de façon suffisamment directe et certaine par sa passation ou ses clauses est recevable à former devant le juge du contrat un recours de pleine juridiction contestant la validité du contrat ou de certaines de ses clauses non réglementaires qui en sont divisibles* » (*cf*. CE, Ass., 4 avril 2014, *Département de Tarn-et-Garonne*, n° 358994, Rec. p. 70).

13. Ce recours de pleine juridiction « *doit être exercé* [...] *dans un délai de deux mois à compter de l'accomplissement des mesures de publicité appropriées, notamment au moyen d'un avis mentionnant à la fois la conclusion du contrat et les modalités de sa consultation dans le respect des secrets protégés par la loi* » (même arrêt).

14. En ce qui concerne les tiers lésés, le Conseil d'État a circonscrit le champ des moyens invocables aux « *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* » (même arrêt).

15. 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).

16. **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, des collectivités territoriales ou des acteurs privés, et contre le fichage généralisé.

17. Elle a notamment pour objet, aux termes de l'article 3 de ses statuts constitutifs, la promotion et la défense « *des réseaux – notamment Internet – libres, ouverts, distribués, neutres et éthiques* », « *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* », ou encore « *de la liberté d'expression, la liberté d'accès à l'information et la lutte contre la censure* ». La poursuite de cet objet statutaire peut notamment se faire par « *la mise en œuvre d'actions juridiques et de contentieux* ».

18. L'exposante est régulièrement amenée à défendre les droits et libertés fondamentaux devant le Conseil d'État [1] et les autres juridictions administratives [2], de même que devant le Conseil constitutionnel français [3] ou le juge de l'Union européenne [4].

19. La convention conclue par la ville d'Orléans, en ce qu'elle prévoit un dispositif de surveillance sonore de l'espace urbain, entraîne un traitement de données personnelles manifestement excessif et disproportionné qui n'est fondé sur aucune base légale. En prévoyant la mise en place sur la voie publique d'un tel système de surveillance algorithmique des sons – pouvant notamment inclure la captation de conversations –, le marché conclu par la ville d'Orléans avec la société Sensi-

1. CE, 21 avril 2021, n^{os} 393099, 394922, 397844, 397851, 424717, 424718 ; CE, 13 avril 2021, n^{o} 439360, 440978, 441151, 442307, 442317, 442363, 443239 ; CE, 22 décembre 2020, n^{o} 446155 ; CE, ord., 4 janvier 2021, n^{os} 447970, 447972 et 447974 (trois affaires) ; CE, ord., 18 mai 2020, n^{os} 440442, 440445 ; CE, 16 octobre 2019, n^{o} 433069 ; CE, 18 octobre 2018, n^{o} 404996 ; CE, 26 juillet 2018, n^{os} 394924, 394922, et 393099 (trois affaires) ; CE, 21 juin 2018, n^{o} 411005 ; CE, 18 juin 2018, n^{o} 406083 ; CE, 25 octobre 2017, n^{o} 411005 ; CE, 17 mai 2017, n^{o} 405792 ; CE, 18 novembre 2016, n^{o} 393080 ; CE, 22 juillet 2016, n^{o} 394922 ; CE, 15 février 2016, n^{o} 389140 ; CE, 12 février 2016, n^{o} 388134 ; CE, ord., 27 janvier 2016, n^{o} 396220 ; CE, 9 septembre 2015, n^{o} 393079 ; CE, 5 juin 2015, n^{o} 388134.

2. TA Marseille, 27 février 2020, n^{o} 1901249.

3. Cons. const., 20 mai 2020, n^{o} 2020-841 QPC ; Cons. const., 3 avril 2020, n^{o} 2020-834 QPC ; Cons. const., 30 mars 2018, n^{o} 2018-696 QPC ; Cons. const., 2 février 2018, n^{o} 2017-687 QPC ; Cons. const., 15 décembre 2017, n^{o} 2017-692 QPC ; Cons. const., 4 août 2017, n^{o} 2017-648 QPC ; Cons. const., 21 juillet 2017, n^{o} 2017-646/647 QPC ; Cons. const., 2 décembre 2016, n^{o} 2016-600 QPC ; Cons. const., 21 octobre 2016, n^{o} 2016-590 QPC ; Cons. const., 24 juillet 2015, n^{o} 2015-478 QPC.

4. TUE, ord., 14 décembre 2020, aff. T-738/16 ; CJUE, 6 octobre 2020, aff. C-511/18, C-512/18 et C-520/18.

vic 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.

20. **Il en résulte que** La Quadrature du Net a sans conteste intérêt à agir contre la convention passée entre la ville d'Orléans et la société Sensivic, dès lors que celle-ci lèse ses intérêts de façon suffisamment directe et certaine.

II. Sur la qualification juridique des faits

21. La convention conclue entre la ville d'Orléans et la société Sensivic autorise la mise en œuvre d'un traitement de données personnelles, et notamment de données sensibles.

A. En ce qui concerne la qualification de données personnelles, et notamment de données sensibles

22. Les données concernées par le dispositif autorisé par la convention attaquée consistent bien en des données personnelles.

23. **En droit**, aux termes du 1. 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 »), une donnée personnelle est définie comme :

> « *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification,*

des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ; »

24. Ainsi, une donnée personnelle doit pouvoir être rattachée à une personne physique identifiée ou identifiable. Le considérant 21 de la directive « police-justice » précise que « *Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement* [...] ».

25. 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 ») reprend la même définition que la directive « police-justice » au 1. de son article 4. De même, le troisième alinéa de l'article 2 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 ») renvoie directement aux définitions du RGPD (et indirectement à celles de la directive « police-justice »).

26. Par ailleurs, l'article 10 de la directive « police-justice » précise qu'il existe certaines catégories particulières de données personnelles, dites « données sensibles », 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* ». Cette définition est reprise à l'identique par l'article 6 de la loi Informatique et Libertés et l'article 9 du RGPD.

27. Dans son courrier adressé à la mairie de Saint-Étienne le 25 octobre 2019, la présidente de la Commission nationale de l'informatique et des libertés (ci-après « la CNIL »), Mme Marie-Laure Denis, a analysé la légalité d'un dispositif de captation et d'analyse de sons dans l'espace public. Ce dispositif permettait, selon elle, de capter de manière indifférenciée « *les sons émis sur la voie publique, y compris des sons de bombes aérosols bris de verre ou de crépitements* » (*cf.* pièce n° 6).

28. Elle a considéré que « *Si les dispositifs de captation et d'analyse des sons ne permettent pas d'identifier directement les personnes, leur association avec le système de vidéo protection existant peut permettre in fine cette identification. En effet, ainsi que la délégation en a été informée, la détection d'un son relevant d'une des catégories de sons visées déclenche l'envoi d'une alerte aux opérateurs de vidéo-protection du centre de supervision urbaine qui pourront orienter les caméras de vidéo-protection vers la zone concernée et être ainsi en mesure d'identifier ainsi la source et l'auteur du son détecté* » (même pièce).

29. La présidente de la CNIL a également précisé que « *Les voix et conversations des personnes se situant dans la zone couverte sont ainsi susceptibles d'être captées par le dispositif envisagé* ». Elle a ainsi considéré que « *le traitement de captation et d'analyse des sons dont la mise en œuvre est envisagée est susceptible de porter sur des catégories de données personnelles relevant de l'article 9 du RGPD et de l'article 6 de la loi du 6 janvier 1978 modifiée (données dites « sensibles »), telles que les opinions politiques, les convictions religieuses et les données concernant la santé, la vie sexuelle ou l'orientation sexuelle de personnes physiques* » (même pièce).

30. **En l'espèce**, la convention attaquée autorise une expérimentation visant à installer dans la ville d'Orléans des dispositifs pour la détection de sons, en particulier la détection automatisée de bruits anormaux.

31. Lors de la description à la presse de l'expérimentation, il a été précisé que l'expérimentation aurait lieu « *au CSO, le centre de sécurité orléanais* » et que les dispositifs seraient couplés à « *3 ou 4 caméras de la ville* ». M. Florent Montillot, l'adjoint au maire d'Orléans a précisé que « *l'idée, c'est que si un son anormal est détecté, comme un coup de feu, un bris de glace, un cri de détresse, immédiatement une alerte avertirait l'agent qui surveille les écrans au CSO ; celui-ci pourrait aussitôt regarder et identifier le lieu où cela s'est passé, et donc envoyer une équipe* » (*cf.* pièce n° 7).

32. La délibération autorisant la signature de la convention précise que l'entreprise Sensivic « *propose un dispositif qui, couplé avec un système de vidéo-protection, détecte les sons et en particulier les sons anormaux, dans l'objectif d'améliorer les performances des installations de sécurité* » (*cf.* pièce n° 4).

33. L'article 3 de la convention attaquée prévoit que les dispositifs « *demandent à être couplés à un système de sécurité et plus particulièrement ceux s'appuyant sur un système de vidéo-protection pour garantir une surveillance optimale* », et qu'ils ont pour objectif « *la détection en temps réel d'événements anormaux comme des coups de feu, des intrusions, des détonations, des cris de peur, des bris de verre, etc.* » (*cf*. pièce n° 5).

34. Il est précisé au même article de la convention attaquée que « *tous les produits d'analyse sonore SENSIVIC sont dotés d'un système d'intelligence artificielle permettant d'analyser en permanence le son ambiant pour pouvoir détecter des anomalies* » (même pièce).

35. La partie 1.3 de l'article 4 de la convention attaquée illustre par ailleurs l'installation d'un dispositif de captation sonore installé juste en-dessous d'un dispositif de caméra de vidéosurveillance de la voie publique (même pièce).

36. Ainsi, la convention prévoit l'installation d'un dispositif permettant la captation indifférenciée et permanente de sons afin de détecter automatiquement non seulement des bruits tels que des intrusions ou des détonations, mais également des cris. Ce dispositif est, dès le stade de l'expérimentation, couplé à des caméras de vidéosurveillance permettant notamment à la police municipale d'envoyer une équipe sur place ou d'orienter les caméras vers la zone concernée pour être en mesure d'identifier la source et l'auteur du son détecté.

37. À ce titre, la longueur ou la qualité du son capté importe peu : à partir du moment où le dispositif capte un son permettant d'identifier, même indirectement, une personne (par exemple *via* un agent de police municipale ou une caméra de surveillance), il s'agit, comme l'a rappelé la CNIL dans son courrier à Saint-Étienne, d'une donnée personnelle. Le couplage du dispositif à des caméras de vidéosurveillance dans le but d'identifier la source d'un bruit et d'envoyer une équipe sur place pour, notamment, identifier une personne responsable du bruit, a d'ailleurs été directement admis par la mairie d'Orléans.

38. Aussi bien, c'est au prix d'une erreur de droit manifeste que la société Sensivic affirme sur son site Internet, s'appuyant sur un audit d'un laboratoire, que son dispositif serait conforme au RGPD (qui, au demeurant, n'est pas applicable

en l'espèce, *cf.* §§ 56 et s.) au motif que seules quelques dizaines de millisecondes seraient analysées. En effet, à supposer même que ces données ne seraient pas *per se* identifiantes – ce qui, au demeurant, n'est pas démontré –, elles permettent en toute hypothèse, notamment à l'aide du dispositif de vidéosurveillance, d'alerter les opérateurs du centre de sécurité urbaine qui pourront alors être en mesure, grâce aux caméras ou à des agents sur place, d'identifier l'auteur du son de manière indirecte, au sens du 1. de l'article 3 la directive « police-justice ».

39. Enfin, et de la même manière qu'à Saint-Étienne (*cf.* pièce n° 6), les sons captés par le dispositif qui, comme cela a été indiqué, analyse en permanence le son ambiant dans l'espace public, sont susceptibles d'être relatifs aux opinions politiques, aux convictions religieuses, ou concernant la vie sexuelle, la santé ou l'orientation sexuelle de personnes physiques. Des données sensibles sont donc susceptibles d'être captées et traitées par le dispositif litigieux.

40. **Il en résulte que** la convention litigieuse permet et met en place une expérimentation d'un dispositif susceptible de traiter des données personnelles, dont des données sensibles, que celles-ci soient directement identifiantes ou indirectement identifiantes *via* notamment le couplage du dispositif de captation sonore avec une caméra de vidéo-surveillance.

B. En ce qui concerne l'existence d'un traitement

41. Le dispositif autorisé par la convention attaquée consiste bien en un traitement de données personnelles.

42. **En droit**, aux termes du 2. de l'article 3 de la directive « police-justice », un traitement est ainsi défini :

> « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou*

toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ; »

43. Le RGPD reprend une définition identique au 2. de son article 4. L'article 2 de la loi Informatique et Libertés renvoie explicitement à la définition du RGPD.

44. Il ressort de cette définition que la simple collecte d'une donnée personnelle constitue un traitement.

45. Il en ressort également que si, à la suite d'une chaîne d'opérations, une donnée perd son caractère *identifiant*, par le biais d'une opération d'anonymisation ou de suppression, cela est dépourvu d'incidence sur la qualification de traitement de données *personnelles* du dispositif. Autrement dit, un dispositif complexe devra être qualifié de traitement de données personnelle si, à un moment où à un autre, des données personnelles sont traitées.

46. Sur ce point, le Conseil d'État a notamment précisé qu'un dispositif de floutage postérieur à la captation d'images, et ne renvoyant que des images floutées au responsable de traitement, doit s'analyser en un traitement de données personnelles soumis à la directive « police-justice » et la loi Informatique et Libertés (*cf.* CE, 22 décembre 2020, *La Quadrature du Net*, n° 446155, Rec. T., pts. 6 et 7). M. le rapporteur public Laurent Domingo précisait dans cette affaire que « *Peu importe qu'une partie du flux d'informations, à l'une des étapes de la transmission de ce flux, subissent une altération technique. En réalité, en floutant les images captées par le drone lors de leur transmission au centre de commandement, la préfecture de police n'a fait qu'ajouter un traitement aux données captées.* »

47. De même, si la conservation sur un support d'une donnée personnelle est un élément suffisant pour qu'un dispositif puisse être qualifié de traitement, une telle conservation n'est pas un élément nécessaire à la qualification de *traitement de données* d'un dispositif. Autrement dit, un dispositif peut être qualifié de traitement même si les données personnelles ne sont pas conservées, à partir du moment où d'autres opération comme, notamment, « *l'organisation* », « *la structuration* », « *l'adaptation* », « *la limitation* », « *l'effacement* » ou encore « *la destruction* » sont effectuées.

48. Enfin, dans son courrier à la ville de Saint-Étienne, la présidente de la CNIL a précisé que les données captées par un dispositif de captation sonore font bien l'objet d'un traitement car « *la simple collecte d'une donnée à caractère personnel constitue un traitement au sens des textes précités, y compris en l'absence d'enregistrement. Le fait que ces données soient effacées ou anonymisées, même à très bref délai, ne remet pas en cause cette qualification* » (*cf.* pièce n° 6).

49. **En l'espèce**, comme présenté ci-avant, le dispositif litigieux consiste en la captation (c'est-à-dire la collecte) de sons, puis en leur analyse postérieurement à la captation. En cela, il s'agit donc d'un traitement au sens du droit des données personnelles.

50. Premièrement, le dispositif litigieux analyse des sons pour détecter automatiquement des menaces potentielles. La convention passée entre la ville d'Orléans et la société Sensivic précise que « *Tous les produits* [du dispositif litigieux] *sont dotés d'un système d'intelligence artificielle permettant d'analyser en permanence le son ambiant pour pouvoir détecter des anomalies* » (*cf.* pièce n° 5).

51. Il s'en déduit que l'objectif du dispositif litigieux est d'effectuer une analyse automatisée et systématique, à l'aide d'outils informatiques, des sons captés afin de détecter ceux susceptibles de constituer un possible trouble à l'ordre public. Le dispositif litigieux détermine si un son donné à un instant *t* correspond à l'une des caractéristiques pré-établies par la société Sensivic (« *coups de feu* », « *intrusions* », « *détonations* », « *cris de peur* », « *bris de verre*, « *bris de vitrine* », « *chocs sur du mobilier urbain* », etc., *cf.* pièce n° 5). Ainsi, à partir d'un son, le dispositif pourra le classifier automatiquement dans une catégorie de troubles à l'ordre public pour permettre ensuite au responsable de traitement, et notamment à l'aide de la vidéosurveillance ou l'envoi sur place d'agents de la police municipale, de prendre des mesures individuelles.

52. Le traitement consiste donc bien dans un premier temps en la « *captation* » de données personnelles (les sons), captation qui est faite de manière permanente selon la convention, puis en leur « *organisation* » et en leur « *structuration* ».

53. Deuxièmement, si les données personnelles captées (*i.e.* les sons) étaient considérées comme perdant leur rattachement à une personne par les opérations

postérieures à la collecte – *quod non*, *cf.* §. 37 –, cette seule captation de sons initiale suffit à considérer le dispositif litigieux comme étant un traitement au sens de la directive « police-justice » et de la loi Informatique et Libertés. En effet, les opérations effectuées sur les sons postérieurement à leur captation (c'est-à-dire effacer ce qui a déjà été collecté) aux fins de leur faire perdre tout caractère identifiant constituent, en elles-mêmes, des traitements, la directive « police-justice » qualifiant « *la limitation, l'effacement ou la destruction* » de données personnelles comme étant des traitements.

54. Comme l'a rappelé la CNIL dans son courrier à Saint-Étienne (*cf.* pièce n° 6), la simple collecte du son suffit pour constituer un traitement, nonobstant les circonstances qu'il n'y ait pas d'enregistrement effectué, ou que le son soit ultérieurement anonymisé ou effacé à bref délai.

55. **Il en résulte que** le dispositif litigieux consiste bien en un traitement au sens de la directive « police-justice » et de la loi Informatique et Libertés. En conséquence, le dispositif litigieux est bien un traitement de données personnelles.

C. En ce qui concerne l'applicabilité de la directive « police-justice » et du titre III de la loi Informatique et Libertés

56. Le titre III de la loi Informatique et Libertés, pris en application de la directive « police-justice » trouve à s'appliquer en l'occurrence.

57. **En droit**, les articles 1 et 2 de la directive « police-justice » prévoient que cette dernière s'applique aux traitement de données personnelles effectué par les autorités compétentes aux fins « *de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces* ». L'article 87 de la loi Informatique et Libertés reprend ce champ d'application.

58. Dans le courrier adressé à la ville de Saint-Étienne, la présidente de la CNIL a considéré que le dispositif envisagé par la ville de Saint-Étienne relevait de la directive « police-justice » en raison de ses conséquences opérationnelles concrètes,

et cela malgré son caractère expérimental. Elle soulignait qu'un dispositif qui « *ne se borne pas uniquement à tester la technologie de captation et d'analyse des sons de l'espace public* » et « *peut, en outre, avoir des conséquences opérationnelles concrètes (déclenchement d'interventions) dès cette phase expérimentale* » relève de la « *directive "police justice" du 27 avril 2016 et des textes pris pour sa transposition (articles 87 et suivants de la loi du 6 janvier 1978)* » (*cf.* pièce n° 6, pp. 2–3).

59. **En l'espèce**, la convention a pour objectif de déterminer les conditions permettant d'installer des dispositifs pour détecter automatiquement des bruits anormaux. Il est précisé à l'article 3 de la convention litigieuse que le dispositif de la société Sensivic a pour objectif d'améliorer les performances des installations de sécurité, en étant couplé à des caméras de vidéosurveillance (*cf.* pièce n° 5).

60. L'article 4 précise que l'objectif n° 2 de l'expérimentation est d'« *améliorer les connaissances concernant les types d'anormalités sonores intéressant le domaine de la sécurité publique* » (*cf.* pièce n° 5).

61. Par ailleurs, l'article 5 de la convention « *Déroulé du processus d'expérimentation* » précise que l'installation du dispositif se fait « *après validation des emplacements par la Direction de la Sécurité et de la Tranquillité Publiques* ».

62. Enfin, comme souligné précédemment, il a été expliqué dans la presse que l'expérimentation objet de la convention aurait lieu « *au CSO, le centre de sécurité orléanais* » et que les dispositifs seraient couplés à « *3 ou 4 caméras de la ville* » (*cf.* pièce n° 7).

63. Le dispositif envisagé par la convention a donc bien une finalité de sécurité publique : il est installé à des fins de détections de sons susceptibles d'être liés notamment à des infractions ou troubles à l'ordre public, couplé à des caméras de vidéosurveillance et sous la direction de la Direction de la sécurité et de la tranquillité publique.

64. **Il en résulte que** le traitement de données personnelles autorisé par la convention est soumis au titre III de la loi Informatique et Libertés, pris en application de la directive « police-justice ».

65. **En tout état de cause**, s'agissant d'un traitement de données personnelles, le traitement est soumis au RGPD et à la loi Informatique et Libertés.

III. Sur l'illégalité de la convention

A. En ce qui concerne le caractère excessif et l'absence de caractère adéquat et pertinent du traitement

66. **En premier lieu**, la convention attaquée est illégale, en ce qu'elle autorise la mise en œuvre un traitement méconnaissant l'article 8 de la Convention européenne des droits de l'homme et des libertés fondamentales (ci-après « CESDH »), l'article 4 de la directive « police-justice » et l'article 4 de la loi Informatique et Libertés, dès lors que les données collectées et traitées 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.

67. **En droit**, le 2. de l'article 8 de la CESDH prévoit qu'« *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.* »

68. De même, le 1. de l'article 4 de la directive « police-justice » dispose que « *les États membres prévoient que les données à caractère personnel sont :* [...] *c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées ;* [...] ».

69. À ce titre, le considérant 26 de la directive « police-justice » énonce qu'« [i]*l convient notamment de veiller à ce que les données à caractère personnel collectées ne soient pas excessives, ni conservées pendant une durée excédant celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Les données à caractère personnel ne devraient être traitées que si la finalité du traitement*

ne peut être raisonnablement atteinte par d'autres moyens ».

70. L'article 4 de la loi Informatique et Libertés reprend ces dispositions en exigeant 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 ou, pour les traitements relevant des titres III et IV, non excessives ;* [...] ».

71. Il en résulte que pour déterminer le caractère adéquat, pertinent et non excessif d'un traitement de données, il convient notamment de vérifier si la finalité poursuivie pouvait être atteinte par d'autres moyens moins intrusifs et de prendre en compte le contexte de sa mise en œuvre, les 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.

72. Par ailleurs, il incombe au responsable du traitement de démontrer, par exemple dans le cadre d'une analyse d'impact sur la protection des données (AIPD), en quoi le traitement est proportionné et que la finalité poursuivie ne peut pas être atteinte autrement.

73. C'est notamment en application de ce principe que le Conseil d'État a pu reprocher au ministre de l'intérieur de ne pas avoir démontré la nécessité du recours à des drones aux fins de garantie de la sécurité publique : « *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* » (*cf.* CE, 22 décembre 2020, *La Quadrature du Net*, préc., pt. 11).

74. **En l'espèce**, la convention attaquée autorise, à des fins de sécurité publique, le déploiement d'un dispositif permettant le traitement de données personnelles, dont des données sensibles.

75. Comme souligné précédemment, il ne fait aucun doute que le dispositif poursuit notamment un objectif de sécurité publique : l'expérimentation a lieu dans le centre de sécurité de la ville, sous le contrôle de la Direction de la tranquillité et de la sécurité, et le dispositif est couplé à plusieurs caméras de vidéosurveillance de

la ville afin de permettre aux agents de la police municipale d'identifier la source des bruits détectés.

76. De la même manière, l'article 3 de la convention précise que les dispositifs faisant l'objet de l'expérimentation ont pour objectif « *d'améliorer les performances des installations de sécurité existantes ou à venir* » (*cf.* pièce n° 5).

77. Or, la ville échoue manifestement à apporter le moindre élément concernant la nécessité à traiter de telles données personnelles. Il n'est à aucun moment défini dans la convention ou la délibération prise par le conseil municipal de la ville, en quoi ce traitement serait nécessaire à des fins de sécurité publique. Ni la ville, ni la société Sensivic n'apportent le moindre commencement de preuve de la nécessité de recourir au dispositif litigieux pour les missions de tranquillité publique dévolues à la ville. En particulier, aucun élément ne permet d'affirmer que cet objectif de tranquillité publique ne pourrait pas être atteint autrement que par l'usage d'une surveillance sonore constante de l'espace urbain.

78. **Il en résulte que** le dispositif n'est pas nécessaire aux finalités envisagées.

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

79. **En deuxième lieu**, la convention attaquée est illégale, en ce qu'elle autorise la mise en œuvre un traitement de données contraire à l'article 8 de la CESDH, à l'article 10 de la directive « police-justice » et à l'article 88 de la loi Informatique et Libertés, dès lors qu'elle entraîne notamment le traitement de données sensibles sans respecter les conditions de légalité d'un tel traitement.

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

81. De même, l'article 10 de la directive « police-justice », intitulé « *Traitement portant sur des catégories particulières de données à caractère personnel* », indique que :

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

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

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

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

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

83. Il en résulte qu'un traitement de données sensibles n'est légalement possible qu'en cas de *nécessité absolue*, sous réserve de garanties appropriées pour les droits et libertés des personnes concernées, et à condition d'être préalablement autorisé par une disposition législative ou réglementaire, ou de viser à protéger les intérêts vitaux d'une personne physique déterminée, ou de porter des données manifestement rendues volontairement publiques par la personne concernée.

84. **En l'espèce**, comme indiqué ci-dessus, il ne fait aucun doute que le dispositif litigieux consiste en un traitement de données personnelles, notamment de

données biométriques.

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

86. Or, comme rappelé ci-avant, la ville d'Orléans n'a, à aucun moment, démontré la nécessité de mettre en place et de recourir à un tel traitement, encore moins la *nécessité absolue* de ce dispositif par rapport à d'autres moyens, notamment humains, surtout pour une petite ville dépourvue de tout problème de sécurité.

87. Par ailleurs, aucune AIPD n'a été soumise à la CNIL alors qu'un tel document, au demeurant obligatoire avant la mise en oeuvre d'un traitement de données sensibles, aurait pu permettre à la ville de prendre conscience que cette nécessité absolue faisait manifestement défaut.

88. **Il en résulte que** la convention attaquée est illégale, en ce qu'elle autorise la mise en œuvre un traitement de données sensibles manifestement dépourvu de nécessité absolue et de garanties appropriées.

C. En ce qui concerne le défaut de base légale du traitement litigieux

89. **En troisième lieu**, la convention attaquée est illégale dès lors qu'elle est contraire à l'article 8 de la CESDH, à la lecture combinée des articles 4, 8 et 10 de la directive « police-justice », et à la lecture combinée des articles 4, 5 et 88 de la loi Informatique et Libertés, en ce qu'elle prévoit une atteinte au droit à la vie privée qui n'est pas prévue par la loi.

90. **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. »

91. 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).

92. 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)

93. 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).

94. 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.

95. 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 ;* [...] ».

96. 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****.* »

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

98. **En droit**, toujours, en ce qui concerne le cas particulier des traitements de données sensibles, l'article 10 de la directive « police-justice » pose un principe d'interdiction et, par exception, « *uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée* », les autorise seulement « *lorsqu'ils sont autorisés par le droit de l'Union ou le droit d'un État membre* », « *pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique* » ou « *lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée* ».

99. Ce principe d'interdiction de traiter des données sensibles sans base légale spécifique a été transposée dans la loi Informatique et Libertés à l'article 88 qui, tout en posant un même principe d'interdiction traiter des données sensibles, l'autorise par exception uniquement par « *une disposition législative ou réglementaire* », ou bien « *s'il vise à protéger les intérêts vitaux d'une personne physique, soit s'il porte sur des données manifestement rendues publiques par la personne concernée* ». Cette exception, à l'instar de tout exception, doit être interprétée strictement.

100. Enfin, dans son courrier adressé à la ville de Saint-Étienne, la CNIL a considéré qu'un dispositif de captation et d'analyses de sons ne relevait pas des dispositions prévues par le code de sécurité intérieure et souffrait, en l'état actuel du droit français, d'une absence de base légale suffisante. Elle considérait en effet que « *le recours au dispositif de captation et d'analyse des sons de l'espace public ne saurait trouver un fondement suffisant dans les dispositions législatives d'ordre général de la loi du 6 janvier 1978, ou dans le seul pouvoir réglementaire de la commune de Saint-Etienne ou de Saint-Etienne Métropole* » et en concluait à l'illicéité d'un tel dispositif (*cf.* pièce n° 6).

101. La CNIL a ainsi souligné que « *à défaut d'un cadre légal spécifique et adapté permettant d'assurer la conciliation entre, d'une part, les objectifs légitimes poursuivis par le dispositifs en termes de tranquillité et de sécurité publique, et, d'autre part, le respect des droits et libertés constitutionnellement protégés, le traitement de données à caractère personnel en question ne saurait être mis en œuvre de façon licite* » (même pièce).

102. **En l'espèce**, la convention attaquée autorise un traitement de données personnelles, dont des données sensibles, correspondant à la captation et à l'analyse de sons sur la voie publique.

103. De la même manière que le dispositif de la ville de Saint-Étienne considéré comme illicite par la CNIL, le traitement litigieux n'est fondé sur aucun texte légal ou réglementaire. Aucun acte réglementaire n'autorise en effet la ville d'Orléans à procéder à un tel traitement de données personnelles, dont des données sensibles, et cela alors qu'il constitue sans aucun doute une ingérence grave dans de droit à la vie privée et à la protection des données personnelles de ses habitants. En particulier, le code de la sécurité intérieure ne saurait servir de base légale à une telle captation ou détection de sons dans l'espace public.

104. **Il en résulte que** la convention autorise un traitement de données personnelles, notamment sensibles, qui n'est fondé sur aucun cadre légal ou réglementaire.

105. À tous égards, l'annulation de la convention s'impose.

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

106. Compte tenu des frais qu'elle a été contrainte d'engager pour assurer la défense de ses intérêts dans cette procédure, l'exposante demande qu'une somme de 4 096 euros soit mise à la charge de la ville d'Orléans sur le fondement des dispositions de l'article L. 761-1 du code de justice administrative.

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

ANNULER la convention attaquée, avec toutes conséquences de droit ;

ENJOINDRE à la ville de cesser d'utiliser le dispositif de surveillance des sons de la société Sensivic et d'effacer toutes les données collectées, sous astreinte de 1 024 euros par jour de retard à compter de la notification du jugement à intervenir ;

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

Fait à Paris, le 12 décembre 2021

Alexis FITZJEAN Ó COBHTHAIGH
Avocat au Barreau de Paris

BORDEREAU DES PRODUCTIONS

Pièce n° 1 : Statuts de LQDN ;

Pièce n° 2 : Pouvoir spécial ;

Pièce n° 3 : Fiches des produits de la société Sensivic ;

Pièce n° 4 : Délibération autorisant la signature de la convention ;

Pièce n° 5 : Convention attaquée ;

Pièce n° 6 : Courrier daté du 25 octobre 2019 adressé par la CNIL à la ville de Saint-Étienne concernant un dispositif de surveillance algorithmique des sons ;

Pièce n° 7 : François Guéroult, « Sécurité : la ville d'Orléans va tester des détecteurs de sons anormaux », France Bleu Orléans, 2 octobre 2021, URL : `https://www.francebleu.fr/infos/societe/securite-la-ville-d-orleans-va-tester-des-detecteurs-de-sons-anormaux-1633096839`.