COMMISSION NATIONALE

DE L'INFORMATIQUE ET DES LIBERTÉS

RÉCLAMATION AU TITRE DE LA

LOI N° 78-17 DU 6 JANVIER 1978

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

CONTRE : **Le dispositif intitulé « Prevent PCP », expérimenté par la SNCF dans différentes gares françaises.**

Table des matières

FAITS

1. La Quadrature du Net, exposante, est une association de défense des droits et libertés à l'ère du numérique.

2. La société nationale des chemins de fer français (SNCF) expérimente actuellement dans certaines gares un dispositif de vidéosurveillance algorithmique (VSA) qui consiste à analyser automatiquement les images de vidéosurveillance. Plusieurs affiches en gares de Lyon et Nord à Paris, et de Saint-Charles à Marseille révèlent l'existence d'un tel dispositif de surveillance [1].

3. À l'aide de différents panneaux d'affichage obtenus par l'exposante auprès de la Commission nationale de l'informatique et des libertés (ci-après « la CNIL ») (*cf.* pièce n° 1), ainsi que par ceux constatés par l'exposante (*cf.* pièces n°s 2 et 3), la SNCF a informé les voyageurs de l'existence de ce dispositif.

4. Ces affiches indiquent que la direction de la sûreté de la SNCF met en œuvre, au moins depuis septembre 2023 et jusqu'à au moins août 2024, un dispositif d'analyse automatisée des images à des fins de détection des bagages et de suivi de leurs propriétaires.

5. Sur la page du site internet de la SNCF figurant sur les affiches (`https://www.sncf.com/fr/video-appels-surete`), il est indiqué dans l'encart « *Expérimentation de solutions de détections d'objets délaissés et suivi de leurs propriétaires* » (*cf.* pièce n° 4), dans la catégorie « À propos » :

> « *Le projet PREVENT PCP dans lequel SNCF est partenaire, a pour objectif sur 3 ans de développer des solutions de détection d'objets délaissés et de recherche des propriétaires dans le cadre d'un projet financé par la Commission Européenne (Horizon 2020, Grant Agreement N°101020374, https ://prevent-pcp.eu/).*

1. Il est possible que la RATP expérimente également ce dispositif comme annoncé sur le site du projet (`https://prevent-pcp.eu/news/phase-2-prototype-development-for-unattended-items-detection-successfully-completed/`), mais l'exposante ne dispose pas d'éléments permettant de le confirmer et invite donc la CNIL à user de ses pouvoirs pour contrôler la RATP.

Dans ce cadre et à des fins d'amélioration de la sûreté des biens et des personnes, la Direction de la Sûreté SNCF expérimente des solutions d'aide à l'identification de bagages abandonnés et au suivi de leur propriétaire en utilisant des données non-biométriques (données qui ne relèvent pas des caractéristiques physiques, biologiques, voire comportementales, strictement propres à une personne). L'objectif est ici d'évaluer techniquement, sans usage opérationnel, des solutions permettant d'associer rapidement un bagage abandonné à son propriétaire et comprendre son intention, sans impact pour les personnes concernées par le traitement car les alertes de détection ne seront pas traitées opérationnellement en temps réel et ne serviront qu'a posteriori pour le calcul des indicateurs de performances. Seules les images issues du système de vidéoprotection existant seront analysées et conservées pour une durée maximale de 14 jours et automatiquement supprimées au-delà conformément à l'autorisation préfectorale en vigueur.

Aucune donnée biométrique ne sera traitée durant cette expérimentation. »

6. Ce même site indique que le responsable de traitement est la « *Direction de la Sûreté SNCF* ».

7. Par ailleurs, il indique que ce traitement est mis en œuvre dans trois lieux :

« L'expérimentation a lieu à :

- *Gare du Nord à Paris, du 12 février au 30 août 2024 et concerne 100 caméras*
- *Gare de Lyon à Paris, du 27 mars au 30 août 2024 et concerne 70 caméras*
- *Gare Saint-Charles à Marseille, du 15 avril au 30 août 2024 et concerne 87 caméras* »

8. Les finalités annoncées par la SNCF sont :

« *Traitement de détection d'objets délaissés : à des fins statistiques, le responsable de traitement évalue la fiabilité d'algorithmes de détec-*

tion d'objets délaissés sur la base de données agrégées et anonymes produites en sortie du traitement.

Traitement de suivi des propriétaires d'objets délaissés : à des fins statistiques, le responsable de traitement évalue la fiabilité d'algorithmes de suivi des propriétaires d'objets délaissés sur la base de données agrégées et anonymes produites en sortie du traitement. »

9. Le site de la SNCF indique que la base légale du traitement est « *l'intérêt légitime du responsable de traitement* ».

10. Ce même site indique que les images de vidéosurveillance sont utilisées pour le traitement et sont conservées au maximum 14 jours. Enfin, il est indiqué les coordonnées du responsable de traitement et la possibilité d'introduire une réclamation auprès de la CNIL.

11. Par ailleurs, selon un document de présentation rédigé par SNCF et obtenu par l'exposante, les objectifs du dispositif « Prevent PCP » sont de « *Détecter et envoyer des alertes en temps réel aux patrouilleurs vidéo lorsqu'un bagage est abandonné* », de « *Retrouver et suivre le(s) propriétaire(s) du bagage abandonné* » et de « *Coordonner les équipes opérationnelles pour retrouver le propriétaire s'il est toujours en gare* » (*cf.* pièce n° 5, p. 6).

12. C'est le traitement visé par la présente réclamation.

DISCUSSION

I. Sur la procédure

13. À titre liminaire, il convient de rappeler que la présente réclamation est recevable.

14. Aux termes du 2° de l'article 8 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 ») :

> « [La CNIL] *veille à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente loi et aux autres dispositions relatives à la protection des données personnelles prévues par les textes législatifs et réglementaires, le droit de l'Union européenne et les engagements internationaux de la France.*
>
> *A ce titre :*
>
> [. . .]
>
> *d) Elle traite les réclamations, pétitions et plaintes introduites par une personne concernée ou par un organisme, une organisation ou une association, examine ou enquête sur l'objet de la réclamation, dans la mesure nécessaire, et informe l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable, notamment si un complément d'enquête ou une coordination avec une autre autorité de contrôle est nécessaire ;*
>
> [. . .] »

15. Ces dispositions doivent être lues à la lumière de l'article 14 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 cir-

culation de ces données (ci-après directive « police-justice ») et 77 du 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 »), qui donnent à toute personne concernée le droit d'introduire une réclamation contre un responsable de traitement.

16. La Quadrature du Net défend les droits et libertés à l'ère du numérique. Aux termes de l'article 3 de ses statuts [2], elle oeuvre à « *la promotion et la défense du droit à l'intimité, à la vie privée, à la protection de la confidentialité des communications et du secret des correspondances et à la protection des données à caractère personnel* », ainsi qu'à « *la lutte contre la surveillance généralisée ou politique, d'origine privée ou publique* » et à « *la lutte contre l'utilisation d'outils numériques à des fins de surveillance illégitime* ». La poursuite de cet objet statutaire peut notamment se faire par « *la mise en œuvre d'actions juridiques et de contentieux* ».

17. Or, le dispositif litigieux instaure précisément une surveillance des lieux couverts par ce dispositif de VSA. Les personnes filmées verront leurs données personnelles traitées de manière illicite et en dehors de toute proportion – tel qu'il sera développé ci-après –, impliquant une atteinte manifestement disproportionnée au droit à la protection des données personnelles que protègent le RGPD, la directive « police-justice » et la loi Informatique et Libertés, textes que La Quadrature du Net s'est donné pour mission de protéger et que la CNIL est chargée de faire respecter.

18. Au demeurant, La Quadrature du Net a déjà adressé à la Commission plusieurs réclamations, soit en application de l'article 38 de la loi Informatique et Libertés, soit directement comme plaignante, et celles clôturées ont été considérées recevables par la Commission (saisines n° 21022264 et n° 18010725).

19. Partant, la présente réclamation au titre de la loi Informatique et Libertés est recevable.

2. Disponibles à l'adresse suivante : `https://www.laquadrature.net/wp-content/uploads/sites/8/2024/04/Statuts_LQDN_6_avril_2024.pdf`

II. Sur la qualification juridique des faits

20. À titre liminaire toujours, il convient de préciser le cadre juridique applicable, les finalités poursuivies, et la nature du dispositif litigieux.

A. En ce qui concerne le cadre juridique applicable et les finalités poursuivies

21. Le dispositif litigieux consiste en un traitement de données personnelles relevant du titre III de la loi Informatique et Libertés, lue à la lumière de la directive « police-justice ».

22. **En droit**, aux termes du premier alinéa de l'article 87 de la loi Informatique et Libertés :

> « *Le présent titre s'applique, sans préjudice du titre Ier, aux traitements de données à caractère personnel mis en œuvre, 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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, par toute autorité publique compétente ou tout autre organisme ou entité à qui a été confié, à ces mêmes fins, l'exercice de l'autorité publique et des prérogatives de puissance publique, ci-après dénommés autorité compétente.* »

23. Cet article 87 de la loi Informatique et Libertés reprend les critères de la directive « police-justice » pour transposer au titre III de cette loi les exigences de la directive « police-justice ». En particulier, le champ d'application de la directive « police-justice » concerne, selon le 1 de l'article 1er de la directive, le « *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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.* »

24. Il ressort de ces dispositions que, pour relever du champ d'application de la directive « police-justice » et être, dès lors, régi par le titre III de la loi Informatique et Libertés, un traitement de données doit respecter deux conditions cumulatives : être mis en œuvre par une « *autorité compétente* » ; poursuivre une finalité « *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* ».

25. La notion d'« autorité compétente » au sens de la directive « police-justice » est définie au 7 de l'article 3 :

> « *"autorité compétente" :*
>
> *a) toute autorité publique compétente pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ; ou*
>
> *b) tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique 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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ;* »

26. Par ailleurs, il ressort du I de l'article L. 2241-1 du code des transports que « *Sont chargés de constater par procès-verbaux les infractions aux dispositions du présent titre* […] *4° Les agents assermentés de l'exploitant du service de transport ou les agents assermentés d'une entreprise de transport agissant pour le compte de l'exploitant ; 5° Les agents assermentés missionnés des services internes de sécurité de la SNCF et de la Régie autonome des transports parisiens* ».

27. **En droit**, toujours, le Conseil d'État a rappelé que le traitement de données personnelles mis en œuvre pendant une phase de développement d'un dispositif poursuivant des finalités relevant de la directive « police-justice » relève lui-aussi de la directive (*cf.* CE, 22 juillet 2022, *La Quadrature du Net*, n° 451653, pt. 7).

28. Autrement dit, le développement d'un traitement n'est pas en soi une finalité autonome, et il faut déterminer la finalité que le traitement en cours de développement vise afin d'identifier celle du traitement mis en œuvre pendant la phase de développement. Cette finalité permettra alors de déterminer le cadre juridique applicable.

29. La CNIL avait, par ailleurs, adopté un raisonnement similaire en 2020 pendant la pandémie de covid-19 concernant un dispositif de comptage de masques par analyse algorithmique des images (*cf.* pièce n° 6). Elle avait considéré qu'un traitement de données analysant les images afin de déterminer le nombre de personnes portant ou non un masque, dont le résultat était l'établissement de statistiques, ne poursuivait pas une finalité statistique au sens du RGPD dans la mesure où ces statistiques visaient à poursuivre d'autres finalités futures (en l'espèce une adaptation des mesures de prévention).

30. **En l'espèce**, le traitement litigieux est mis en œuvre par la direction de la sûreté de la SNCF et vise à détecter et prévenir le dépôt de bagages abandonnés.

31. Ainsi, premièrement, conformément au code des transports, et en particulier son article L. 2241-1, la SNCF est chargée d'une mission de police des transports et ses agents disposent à cette fin de compétences particulières.

32. Ce faisant, la SNCF est bien une « *entité* » qui s'est vue confier « *des prérogatives de puissance publique à des fins de* [...] *protection contre les menaces pour la sécurité publique et la prévention de telles menaces* ». Il s'agit donc d'une autorité compétente au sens de la directive « police-justice ».

33. Deuxièmement, le dispositif mis en œuvre poursuit une finalité de prévention de troubles à l'ordre public que constitue le dépôt d'un bagage abandonné dans une gare.

34. En effet, l'abandon d'un bagage peut constituer dans certains cas une infraction au sens du 4° de l'article L. 2242-4 du code des transports. Il peut également s'agir, en absence d'élément intentionnel, d'une négligence dans la mesure où les bagages d'un passager doivent mentionner les nom et prénom de ce dernier, conformément à l'article L. 3116-1-1 du code des transports. De manière plus générale,

un bagage abandonné constitue un trouble à l'ordre public.

35. Ce faisant, en poursuivant une finalité de détection et de prévention de dépôt de bagages abandonnés, le dispositif litigieux vise directement une finalité de « *protection contre les menaces pour la sécurité publique et la prévention de telles menaces* », ainsi que de « *prévention et de détection des infractions pénales* ».

36. Par ailleurs, la circonstance que le traitement litigieux vise à déterminer l'efficacité d'un algorithme de détection de bagages abandonnés est sans incidence sur la finalité poursuivie et ne permet pas au dispositif litigieux de poursuivre une finalité statistique. En effet, le traitement litigieux ne sert qu'à évaluer, pendant une phase préalable à son exploitation, l'efficacité d'un traitement poursuivant des finalités de détection de bagage abandonné. C'est donc bien cette dernière finalité de détection des bagages – conformément à la jurisprudence du Conseil d'État – et non une finalité statistique que poursuit le traitement litigieux.

37. Au demeurant, la SNCF elle-même est bien consciente que ce traitement de données est susceptible d'entrer dans le champ d'application de la directive « police-justice » car poursuivant une finalité de la directive, puisqu'elle écrivait, dans un encadré « Points d'attention » d'un document de présentation de ce dispositif, que ce « *Projet s'inscri*[t] *dans le cadre du RGPD et de la Directive Police Justice mais soumis à des réglementations nationales potentielles différentes* », en précisant immédiatement : « *Analyse de l'ensemble de la chaîne de traitement (collecte, détection de bagage, réidentification du propriétaire et recherche du propriétaire, …)* » (*cf.* pièce n° 5, p. 7).

38. **Il en résulte que** le dispositif litigieux est mis en œuvre par une autorité compétente au sens de la directive « police-justice » et poursuit une finalité relevant de la directive « police-justice ».

39. Par conséquent, sa légalité doit être déterminée au regard du titre III de la loi Informatique et Libertés, lu à la lumière de la directive « police-justice ».

B. En ce qui concerne la nature biométriques des données traitées

40. Le traitement litigieux est un traitement de données biométriques.

41. **En droit**, il existe au sein de la notion de donnée personnelle une sous-catégorie de données dites « sensibles », qui comprend notamment, selon l'article 6 de la loi Informatique et Libertés, les données qui « *révèlent* [...] *les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique* », ainsi que « [l]*es données génétiques,* [l]*es données biométriques aux fins d'identifier une personne physique de manière unique,* [l]*es données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique* ».

42. La notion de données biométriques est détaillée par le 14 de l'article 4 de la directive « police-justice » comme désignant des données « *résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales* ». Le Comité européen de la protection des données (ci-après le « CEPD »), autorité européenne chargée de garantir l'application effective des règles européennes en matière de données personnelles, détaille, dans ses lignes directrices, le traitement de données biométriques comme étant un « *traitement technique spécifique* » des données se rapportant « *aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique* » dans le but précis « *d'identifier une personne physique de manière unique* » (*cf.* pièce n° 7, pt. 74). Si l'approche du CEPD concerne le RGPD, elle est bien entendu applicable *mutatis mutandis* à la directive « police-justice », cette dernière reprenant exactement les mêmes définitions que le RGPD.

43. Trois conditions sont donc nécessaires, au sens de l'article 4 de la directive « police-justice » et 6 de la loi Informatique et Libertés, pour qu'un dispositif puisse être qualifié de traitement de données biométriques : il faut qu'il y ait un traitement spécifique, qui analyse des caractéristiques physiques, physiologiques ou comportementales des personnes, et qui vise à identifier ces dernières de manière unique.

44. 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.

45. En ce qui concerne l'analyse des caractéristiques physiques ou physiologiques, celles-ci peuvent se rapporter au corps d'une personne filmée au sens large, tels que des visages, des silhouettes ou toute caractéristique isolée du corps, telle la couleur des cheveux, la couleur des yeux, la forme du visage, la taille, le poids, l'âge. Les données comportementales, quant à elles, visent toute information relative à l'action du corps dans l'environnement et l'espace. Pourront être qualifiés de biométriques un vêtement ou accessoire porté par la personne à un instant *t*, un geste, une expression d'émotion, une direction de déplacement, une position dans l'espace et le temps (assis, debout, statique, allure de la marche, etc.).

46. En ce qui concerne l'identification unique, celle-ci n'implique pas nécessairement de révéler l'état civil d'une personne mais, plus largement, de pouvoir individualiser une personne au sein d'un groupe, généralement afin de lui appliquer des mesures spécifiques. Au point 82 de ses lignes directrices, le CEPD donne l'exemple concret d'un traitement permettant de suivre le trajet d'une personne entre plusieurs zones à partir de ses caractéristiques physiques, et sans que cela n'implique de pouvoir en connaître l'état civil. Il s'agit bien ici pour l'autorité d'un traitement de données biométriques :

> « *Toutefois, l'article 9* [du RGPD et, *mutatis mutandis*, l'article 10 de la directive « police-justice »] *s'applique si le responsable du traitement conserve des données biométriques* [...] *afin d'identifier une personne de manière unique. Si un responsable du traitement souhaite détecter une personne concernée qui pénètre à nouveau dans l'espace surveillé ou dans une autre zone* [...] *la finalité serait alors d'identifier de manière unique une personne physique, ce qui signifie que l'opération relèverait d'emblée de l'article 9* [...] . *Dès lors que le système se fonde sur l'analyse de caractéristiques physiques pour détecter des personnes spécifiques qui entrent dans le champ de la caméra (comme les visiteurs d'un centre commercial) et les suivre, il constitue une méthode d'identification biométrique, car il vise la reconnaissance par l'utilisation d'un traitement technique spécifique.* » (*cf.* pièce n° 7, pt. 82)

47. En effet, même sans recourir aux empreintes faciales des individus (reconnaissance faciale), plusieurs méthodes de VSA permettent de suivre une personne – par exemple à travers la couleur de ses vêtements ou sa démarche – à mesure qu'elle évolue dans un espace urbain et passe dans le champ de vision de différentes caméras. Cette capacité de suivi des personnes repose sur des algorithmes dits de « réidentification ».

48. Une telle interprétation de la définition de « *traitement biométrique* » est partagée par le Défenseur des droits dans son enquête sur la « *Perception du développement des technologies biométriques en France* » publiée en octobre 2022 (*cf.* pièce n° 8).

49. 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° 8, p. 2).

50. L'autorité estime que les données biométriques doivent, au sens du droit européen des données personnelles – RGPD ou directive « police-justice » qui partagent les mêmes définitions –, également s'entendre comme l'évaluation des personnes à partir du moment où les données traitées pour cette évaluation sont « *des données corporelles et/ou issues de systèmes biométriques* », et que le traitement vise à « *Identifier ou déduire des émotions, des traits de personnalité ou des intentions (on parle alors de systèmes de "reconnaissance des émotions")* », ou bien à « *Inscrire la ou les personnes visées dans des catégories spécifiques, par exemple de sexe, d'âge, de couleur de cheveux, de couleur des yeux, d'origine ethnique ou d'orientation sexuelle ou politique en vue de prendre des mesures spécifiques (on parle alors de systèmes de "catégorisation")* » (*cf.* pièce n° 8, p. 3).

51. De manière plus générale, il explique que « *les technologies d'évaluation dites également d'analyse (on parle également de vidéo "intelligente" ou "aug-*

mentée") » sont des dispositifs d'évaluation et sont donc, à ce titre, des traitements de données biométriques (même pièce).

52. **En l'espèce**, le dispositif litigieux consiste non seulement à analyser algorithmiquement les images afin de repérer les situations où un bagage serait abandonné, mais également de suivre la personne qui a déposé le bagage à travers les différentes caméras connectées au dispositif.

53. Or, d'une part, en ce qui concerne la détection de comportement, celle-ci consiste à analyser l'ensemble des images afin de repérer les personnes déposant un objet. Est ainsi recherché par le dispositif litigieux non pas un objet qui serait statique, mais bien une personne qui se séparerait d'un bagage.

54. C'est donc bien le comportement de chaque personne qui sera analysé, pour savoir s'il correspond à celui d'un abandon de bagage. Concrètement, le dispositif litigieux va premièrement chercher à détecter l'ensemble des personnes filmées, en les individualisant afin de les distinguer. Deuxièmement, pour chaque personne individualisée, il va déterminer s'il s'agit d'une situation pré-déterminée d'abandon de bagage. Il y a donc bien une identification unique par l'individualisation de chaque individu, sur la base de ses caractéristiques physiques et comportementales (une personne humaine ne ressemble ni se comporte comme un objet), par un traitement spécifique de détection de bagages abandonnés distinct de celui de la collecte des images par la vidéosurveillance.

55. D'autre part, en ce qui concerne le suivi des personnes soupçonnées d'avoir déposé un bagage, il s'agit de retrouver, sur différentes caméras, une même personne – celle qui aurait déposé un bagage. Le dispositif va donc, après avoir repéré qu'une personne, distincte des autres filmées, a déposé un bagage, enregistrer temporairement ses caractéristiques physiques et physiologiques afin de rechercher sur les images des autres caméras ces mêmes caractéristiques pour pouvoir retracer le parcours de la personne. Ces caractéristiques sont donc nécessairement uniques puisque, parmi les personnes entrant dans le champ d'une caméra, le dispositif est capable de faire la différence entre celles qui n'ont pas déposé un bagage, et celle (au singulier) qui a déposé le bagage détecté préalablement.

56. Le traitement effectué par ce dispositif à l'étape de suivi du parcours des

personnes se singularise donc d'autres dispositifs de VSA de détection de comportement. Cette étape de suivi du parcours des personnes implique nécessairement de traiter des données biométriques d'une personne soupçonnée d'avoir abandonné un bagage, afin non seulement de pouvoir la distinguer des autres personnes filmées, mais aussi afin de pouvoir dire à un agent de la SNCF que cette personne se trouve précisément sur telle image et non sur telle autre. Ce suivi des personnes est donc bien un traitement spécifique qui, sur la base des caractéristiques physiques des personnes, permet de les identifier sur une caméra autre que celle ayant filmé l'abandon de bagage.

57. Au demeurant, ce fonctionnement est confirmé par la SNCF elle-même. Dans un document de présentation du dispositif, elle écrit que ce traitement opère une « *réidentification du propriétaire* » et une « *recherche du propriétaire* » (*cf.* pièce n° 5, p. 7). Or, cette réidentitification et cette recherche ne sont possibles que par l'analyse par un traitement spécifique des données physiques ou physiologiques des personnes à des fins d'identification unique.

58. **Il en résulte que** le dispositif litigieux est bien un traitement de données biométriques, donc de données sensibles.

III. Sur l'illégalité du dispositif litigieux

A. En ce qui concerne l'absence de base légale

59. **En premier lieu**, le dispositif litigieux est contraire aux articles 4, 5 et 88 de la loi Informatique et Libertés, lus à la lumière des articles 4, 8 et 10 de la directive « police-justice », en ce qu'il souffre d'une absence de base légale.

60. **En droit**, aux termes de l'article 4 de la loi Informatique et Libertés, « *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 ;* [...] ». Cette exigence est tirée du 1 de l'article 4 de la directive « police-justice », qui exige que « *les États membres prévoient que les données à caractère personnel sont : a) traitées de manière licite et loyale ;* [...] ».

61. 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.* »

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

63. 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 spécifique 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° 9, pt. 4.1).

64. 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'est pas une base légale pour ce genre de dispo-

sitifs. 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° 10, p. 2). Cette interprétation est applicable, *mutatis mutandis*, à tout dispositif d'analyse algorithmique des images mis en œuvre par une autorité compétente.

65. Par ailleurs, les traitements de données sensibles doivent également répondre à une obligation renforcée de base légale. Aux termes de l'article 88 de la loi Informatique et Libertés :

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

66. Cette exigence provient de l'article 10 de la directive « police-justice » qui exige lui aussi que les traitements de données sensibles soient « *autorisés par le droit de l'Union ou le droit d'un État membre* », nécessaires pour « *protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique* » ou portant « *sur des données manifestement rendues publiques par la personne concernée* ».

67. **En l'espèce**, la SNCF indique sur son site internet que la base légale est l'intérêt légitime du responsable de traitement.

68. Comme rappelé ci-avant (*cf. supra*, §§ 27 et 36), la finalité du dispositif litigieux n'est pas une finalité statistique, contrairement à ce qu'affirme la SNCF sur son site internet, mais bien une finalité de « *protection contre les menaces pour*

la sécurité publique et la prévention de telles menaces » et de « *prévention et de détection des infractions pénales* ».

69. Pourtant, force est de constater qu'il n'est pas possible de fonder un traitement de données personnelles relevant du titre III de la loi Informatique et Libertés et de la directive « police-justice » sur les intérêts légitimes du responsable de traitement. Contrairement aux traitements relevant du RGPD, ceux relevant de la directive doivent être fondés sur le droit de l'Union ou le droit national.

70. Or, on ne peut que constater l'absence de toute base légale en droit français permettant de fonder un dispositif de détection et de prévention de bagages abandonnés sur des images de vidéosurveillance.

71. **Il en résulte que** le dispositif litigieux est dépourvu de toute base légale.

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

72. **En deuxième lieu**, le dispositif litigieux méconnaît l'article 4 de la loi Informatique et Libertés, lu à la lumière de l'article 4 de la directive « police-justice », dès lors que les données collectées et faisant l'objet d'un traitement ne sont ni adéquates, ni pertinentes et, en tout état de cause, manifestement excessives au regard des finalités pour lesquelles elles sont collectées et traitées.

73. **En droit**, le 3° de l'article 4 de la loi Informatique et Libertés exige que « *Les données à caractère personnel doivent être :* [...] *3° Adéquates, pertinentes et, au regard des finalités pour lesquelles elles sont traitées, limitées à ce qui est nécessaire et* [...] [pour les traitements relevant de la directive « police-justice »] *non excessives* ». L'article 4 de la directive « police-justice » précise que « *les États membres prévoient que les données à caractère personnel sont* [...] *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées* ».

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

personnel ne devraient être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens ».

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

76. Ainsi, pour déterminer le caractère adéquat, pertinent et non excessif d'un traitement de données, il convient notamment de prendre en compte le caractère nécessaire du dispositif (par exemple, si la finalité poursuivie ne pouvait être atteinte par d'autres moyens moins invasifs), du contexte de sa mise en œuvre et des risques qu'il représente pour les droits et libertés des personnes concernées, la possibilité de détournement ou de mauvais usage du dispositif, ou, enfin, la nature des données traitées.

77. **En l'espèce**, il ressort du site internet de la SNCF que le dispositif litigieux est mis en œuvre sur plusieurs dizaines de caméras dans trois gares majeures de France. On peut supposer, en raison du nombre très important de caméras concernées, que les images analysées par le dispositif litigieux sont celles de l'ensemble des caméras de chaque gare concernée.

78. Premièrement, le dispositif est relié à un nombre particulièrement élevé de caméras – entre 70 et 100 en fonction de la gare.

79. Or, pour qu'un traitement algorithmique puisse déterminer si une situation correspond ou non à celle recherchée, il doit analyser en continu mes images, y compris lorsqu'aucun dépôt de bagage n'est fait. Dès lors, toute personne filmée devant l'une des caméras de ces trois gares verra ses données personnelles traitées, qu'un bagage soit en train d'être abandonné sur la scène filmée ou non.

80. Par ailleurs, ce travail de détection de bagages abandonnés peut parfaitement être fait de manière humaine, et ne requiert pas pour cela de compétences ou d'habilitations particulières. Personnel de ménage, conducteurs de trains, contrôleurs, agents de sûreté de la SNCF, etc. : tous peuvent signaler un bagage qui paraîtrait abandonné.

81. Il n'est par ailleurs à aucun moment indiqué en quoi un tel traitement de données, pratiqué sur l'ensemble des gares concernées, serait adéquat, pertinent et manifestement non-excessif par rapport à l'objectif poursuivi, c'est-à-dire strictement nécessaire au regard de la finalité. Sur son site internet ou sur les affiches d'informations en gare, la SNCF n'apporte ainsi, contrairement à ce qui est requis par la directive « police-justice » et par les dispositions de la loi Informatique et Libertés, aucun élément précis ou factuel qui permettrait de déterminer qu'aucun autre moyen n'aurait permis de parvenir à l'objectif visé.

82. **Il en résulte que** le dispositif litigieux n'est ni adéquat, ni nécessaire, et manifestement excessif par rapport à la finalité envisagé.

C. En ce qui concerne l'absence de nécessité absolue

83. **En troisième lieu**, le dispositif litigieux est contraire à l'article 88 de la loi Informatique et Libertés, lu à la lumière de l'article 88 de la directive « police-justice », en ce qu'il n'existe aucune nécessité absolue à traiter les données.

84. **En droit**, en ce qui concerne les données sensibles, l'article 88 de la loi Informatique et Libertés et 10 de la directive « police-justice » posent un principe d'interdiction de ces données, et exigent par exception une « *nécessité absolue* », combinée à des « *garanties appropriées pour les droits et libertés de la personne concernée.* »

85. Il ressort de ces articles que le contrôle de proportionnalité d'un traitement de données sensibles est renforcé. N'est plus seulement exigée une simple « nécessité », mais désormais une « nécessité absolue ».

86. La Cour de Justice de l'Union européenne (CJUE) a précisé, à l'occa-

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

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

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

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

88. Ainsi, pour que l'exigence de « nécessité absolue » au sens de l'article 10 de la directive « police-justice » soit remplie, la CJUE exige, premièrement, que les finalités du traitement soient particulièrement précises (*ibid*., pts. 122–124). Elle a notamment indiqué que « *les finalités du traitement de* [données sensibles] *ne sauraient être désignées dans des termes à caractère trop général, mais requièrent d'être définies de manière suffisamment précise et concrète pour permettre d'évaluer la "nécessité absolue" dudit traitement* » (*ibid*., pt. 124).

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

90. Dans ses observations dans l'affaire *Ministerstvo na vatreshnite raboti*, la Commission européenne soulignait ainsi l'obligation d'adopter un contrôle de proportionnalité renforcé lorsqu'est exigée une « nécessité absolue » (*cf*. pièce n° 11, pt. 44) :

> « *En ce qui concerne les données* [sensibles]*, le seuil réglementaire plus élevé de l'article 10 de la directive 2016/680, à savoir la "nécessité absolue", trouve à s'appliquer. Cela suppose qu'il soit non seulement raisonnablement impossible, mais aussi totalement impossible, d'atteindre l'objectif du traitement par d'autres moyens et*

que les données sensibles en question soient directement pertinentes et contribuent à la réalisation de l'objectif poursuivi par la loi. L'exigence de "nécessité absolue" étant plus stricte que celle de "nécessité", la vérification du caractère nécessaire des données doit elle aussi être plus stricte. »

91. La CJUE reprenait ainsi cette interprétation en exigeant, pour que la condition tirée de la « nécessité absolue » soit caractérisée, bien plus qu'une impossibilité raisonnable de traiter les données autrement (*ibid*., pt. 126).

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

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

laquelle elle est mise en examen, les circonstances particulières de cette infraction, le lien éventuel de ladite infraction avec d'autres procédures en cours, les antécédents judiciaires ou le profil individuel de la personne en cause ».

94. **En l'espèce**, le traitement litigieux consiste en un traitement de l'ensemble des images de vidéosurveillance à des fins de détection et de prévention de bagages abandonnés.

95. Premièrement, cette finalité est particulièrement large. Elle implique le traitement de nombreuses images, sans être limitée à certaines zones, sans que ne soient exigés des critères permettant de limiter les conditions de sa mise en oeuvre.

96. Deuxièmement, il ne fait aucun doute qu'il est possible de poursuivre autrement cette même finalité. Comme développé ci-avant, la nécessité « classique » de ce dispositif fait défaut, dans la mesure où la détection de bagages abandonnés peut être faite avec du personnel humain – qui est déjà largement présent en gare – et sans devoir recourir à une surveillance algorithmique. La « nécessité absolue » fait donc *a fortiori* défaut, au sens où il n'est pas « *totalement impossible* », pour reprendre les termes de la Commission européenne, de traiter moins de données pour poursuivre cette même finalité.

97. **Il en résulte que** le dispositif litigieux ne respecte pas l'exigence de nécessité absolue.

D. En ce qui concerne l'absence de droit d'opposition

98. **En quatrième lieu**, le dispositif litigieux est illégal en ce qu'il est contraire à l'article 110 de la loi Informatique et Libertés.

99. **En droit**, aux termes de l'article 110 de la loi Informatique et Libertés :

> « *Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.*

Les dispositions du premier alinéa ne s'appliquent pas lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte instaurant le traitement. »

100. Cet article, inséré au titre III de la loi Informatique et Libertés, s'applique aux traitements relevant de la directive « police-justice ».

101. En 2020, saisie du cas d'un traitement d'analyse automatisée des images à des fins de comptage de masques pendant la pandémie de covid-19, la CNIL avait considéré qu'un tel dispositif ne permettait pas d'exercer son droit d'opposition et était, dès lors, contraire à l'article 21 du RGPD (*cf.* pièce n° 6). Cette interprétation du RGPD est applicable, *mutatis mutandis*, à l'article 110 de la loi Informatique et Libertés.

102. **En l'espèce**, le dispositif litigieux consiste en l'analyse de l'ensemble des images de vidéosurveillance des gares concernées afin d'analyser les comportements des personnes filmées et de repérer des bagages qu'elles auraient abandonnés, puis de retracer leur parcours.

103. Or, ce mode de fonctionnement empêche l'exercice même du droit d'opposition. En effet, il n'est techniquement pas possible pour les personnes filmées de pouvoir s'opposer au traitement de leurs données personnelles avant la mise en oeuvre de celui-ci, dans la mesure où les données personnelles de toute personne filmée par une caméra connectée au dispositif litigieux sont *de facto* traitées.

104. **Il en résulte que** le dispositif litigieux est illégal en ce qu'il ne permet pas aux personnes concernées d'exercer leur droit d'opposition.

PAR CES MOTIFS, l'association La Quadrature du Net, exposante, conclut qu'il plaise à la CNIL de :

CONTRÔLER la légalité, en particulier la licéité, la nécessité, la nécessité absolue, l'adéquation, la proportionnalité et le respect du droit d'opposition du dispositif « Prevent PCP » mis en œuvre par la SNCF, au regard de la loi Informatique et Libertés lue à la lumière de la directive « police-justice » ;

ENJOINDRE à la SNCF de cesser d'utiliser ce dispositif et de supprimer toute donnée personnelle traitée par ce dispositif ;

SANCTIONNER la SNCF pour l'utilisation de ce dispositif et les violations constatées à la loi Informatique et Libertés.

Fait à Paris, le 2 mai 2024

[redacted]

Membre du collège solidaire de La Quadrature du Net

BORDEREAU DES PRODUCTIONS

Pièce n° 1 : Exemple d'affiche d'information du dispositif litigieux ;

Pièce n° 2 : Affiche d'information dont la présence a été constatée par La Quadrature du Net en gare de Lyon à Paris le 22 avril 2024 ;

Pièce n° 3 : Affiche d'information dont la présence a été constatée par La Quadrature du Net en gare du Nord à Paris le 30 octobre 2023 ;

Pièce n° 4 : Site internet de la SNCF mentionné sur les affiches en gare (`https://www.sncf.com/fr/video-appels-surete`);

Pièce n° 5 : Présentation de « Prevent PCP » par la SNCF ;

Pièce n° 6 : Courrier de la CNIL à la RATP concernant l'usage d'un traitement de données d'analyse vidéo à des fins de comptage de masques, URL : `https://data.technopolice.fr/fr/entity/rgp85zlnz8e`;

Pièce n° 7 : EDPB, Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo, version 2.1, 26 février 2020, URL : `https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_fr.pdf`;

Pièce n° 8 : Enquête du Défenseur des droits « Perception du développement des technologies biométriques en France – Entre manque d'information et demande d'encadrement », octobre 2022, URL : `https://www.defenseurdesdroits.fr/sites/default/files/2023-07/ddd-enquete-perception-du-developpement-des-technologies-biom%C3%A9triques-en-France-20221004.pdf`;

Pièce n° 9 : CNIL, Caméras dites « intelligentes » ou « augmentées » dans les espaces publics : position sur les conditions de déploiement, URL : `https://www.cnil.fr/sites/cnil/files/atoms/files/cameras-intelligentes-augmentees_position_cnil.pdf`;

Pièce n° 10 : Avertissement de la CNIL à la commune de Valenciennes pour son dispositif d'analyse automatisée des images de vidéosurveillance ;

Pièce n° 11 : Observations écrites à la Cour de justice de l'UE présentée par la Commission européenne dans l'affaire C-205/21, *Ministerstvo na vatreshnite raboti* ; URL : `https://www.asktheeu.org/en/request/ec_written_observations_in_c_205`.