ALEXIS FITZJEAN Ó COBHTHAIGH
Avocat au Barreau de Paris
Médiateur auprès de la cour d'appel de Paris
85, rue de la Victoire – 75009 PARIS
Tél. 01.53.63.33.10 – Fax 01.45.48.90.09
afoc@afocavocat.eu

TRIBUNAL ADMINISTRATIF

DE

GRENOBLE

OBSERVATIONS À LA SUITE DU MÉMOIRE DE LA CNIL

N° 2105328

POUR : **1°) M. Bastien Le Querrec**
2°) L'association La Quadrature du Net

CONTRE : **La commune de Moirans**

EN PRÉSENCE DE : **1°) La Ligue des droits de l'Homme**
2°) Le Syndicat de la magistrature
3°) Le Syndicat des avocats de France
4°) La CNIL

Présentation :

Vidéosurveillance algorithmique *a posteriori* – Traitement de données personnelles à des fins de police judiciaire – Absence de compétence de police judiciaire d'une commune

Table des matières

FAITS

1. Dans l'affaire numéro 2105328, alors que l'audience publique était prévue le vendredi 5 décembre 2024, la Commission nationale de l'informatique et des libertés (ci-après « la CNIL ») a produit, quatre jours avant cette audience, des observations revenant sur des éléments nouveaux, conduisant le tribunal administratif de Grenoble à reporter l'audience dans la présente affaire au 20 décembre 2024.

2. Dans ses observations, la CNIL revient sur l'utilisation *a posteriori* du dispositif litigieux « Briefcam », qu'elle considère, au prix de multiples erreurs de droit, fondé sous certaines conditions. Par ailleurs, la CNIL ne produit pas la mise en demeure adressée à la commune de Moirans qu'elle mentionne dans ses observations, ne permettant pas, ni aux exposants, ni au tribunal, d'apprécier la réalité et le bien-fondé des allégations contenues dans son mémoire.

3. Le présent mémoire entend toutefois répondre aux affirmations erronées en droit de la CNIL. Il ne remet aucunement en cause les moyens et conclusions précédemment articulés, que les exposants réitèrent expressément.

DISCUSSION

I. Sur la nature biométrique des données traitées

4. **En premier lieu**, c'est au prix d'une erreur de droit que la CNIL affirme que les données traitées par le dispositif « Briefcam » ne seraient pas des données biométriques dans le cadre d'une analyse *a posteriori* des images, c'est-à-dire lorsqu'un agent d'une commune recherche une personne sur la base de son apparence physique.

5. **En droit**, comme longuement rappelé dans les précédentes écrites des ex-

posants (*cf.* mémoire introductif d'instance du 5 août 2021, §§ 59 et s. ; mémoire du 13 décembre 2023, §§ 39 et s.), il ressort à la fois des articles 3 et 10 de la directive UE n° 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données (ci-après directive « police-justice »), de l'article 6 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après « loi Informatique et Libertés ») qui transpose cette directive, et des articles 4 et 9 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 ») qu'une donnée biométrique, loin d'être limitée au seul visage, est une donnée personnelle qui répond à trois conditions cumulatives :

— elle résulte d'un traitement technique spécifique ;
— elle est relative aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique ;
— elle permet ou confirme son identification unique.

6. Pour qu'il soit rempli, le critère relatif à l'identification unique n'implique notamment pas qu'il faille attribuer une identité civile à une personne. Il suffit de distinguer une personne physique d'une masse d'autres personnes pour que ce critère soit rempli.

7. Ainsi, dès lors qu'il est acquis qu'un dispositif de reconnaissance faciale traitera des données biométriques – même lorsqu'il n'est pas relié à une base de données permettant d'indiquer les nom et prénoms de la personne –, il en va à l'évidence de même d'autres dispositifs, notamment les dispositifs de vidéosurveillance algorithmique tel que le logiciel « Briefcam », sous les seules trois conditions rappelées précédemment.

8. La doctrine juridique rappelle à cet égard, à juste titre, qu'un dispositif de vidéosurveillance algorithmique comportant une fonctionnalité de recherche de personnes consiste en un traitement de données biométriques. Ainsi, pour M. Robin Médard Inghilterra, maître de conférence à l'Université Paris I, une version « *douce*

des usages de la biométrie dans l'espace public s'est déjà frayé[e] *un chemin en France sous les traits de la VSA.* » :

> « [Peuvent être] *qualifiés de biométriques des usages de la VSA accomplis grâce aux logiciels acquis par les collectivités territoriales et leurs groupements, qui les mobilisent en dehors de l'expérimentation de la loi JOP, sur réquisitions ou non, à des fins de police administrative ou de police judiciaire. Or, les fonctionnalités biométriques de ces logiciels sont patentes. À titre d'illustration, le logiciel de VSA commercialisé par BriefCam, qui équipe déjà des dizaines de collectivités, comprend un module Review qui permet un traitement différé de l'image pour afficher simultanément des évènements survenus à différents moments. Il autorise la recherche multicaméras d'"objets" (personnes ou véhicules) ayant une "similarité d'aspect". Plusieurs filtres permettent de singulariser des personnes au sein d'une "classe" (homme, femme, enfant), comme les attributs, qu'il s'agisse d'un sac (sac à dos, sac à main), d'un chapeau, d'un vêtement (sans manches, à manches courtes, à manches longues, short/jupe, pantalon), le cas échéant d'une couleur et d'une taille déterminés. Dans ce cas, la qualification de biométrie ne saurait être écartée. Il y a bien, par l'apposition de ces différents filtres, singularisation d'une personne au sein d'un environnement, et donc identification unique, après traitement technique spécifique de données physiques, physiologiques ou comportementales.* » (*cf.* pièce n° 24, § 31)

9. **En l'espèce**, la fonctionnalité de recherche de personnes par filtres du dispositif litigieux « Briefcam », dénommée « similitude d'apparence » et qui propose d'analyser les personnes en fonction de leur apparence, constitue bien un traitement de données biométriques, que cette recherche soit effectuée en temps réelle ou *a posteriori*.

10. Premièrement, cette fonctionnalité propose d'analyser les personnes en fonction de leur apparence, et donc de traiter spécifiquement leurs données dans le but de caractériser et singulariser leur apparence. Il s'agit donc d'un traitement technique spécifique.

11. Deuxièmement, il ressort du manuel d'utilisation du logiciel « Briefcam » (*cf.* pièce n° 19, pp. 19–20 et 46–48) que le dispositif litigieux permet de faire des recherches en fonction de :

— L'apparence physique des personnes (filtres en fonction des types de vêtements ou de leur couleur). Il s'agit d'une recherche en fonction de leurs caractéristiques physiques.
— Leur âge et sexe (filtres « *Garçon* », « *Fille* », « *Homme* » ou « *Femme* »). Il s'agit d'une recherche en fonction de leurs caractéristiques physionomiques.
— Leur comportement sur l'image (filtre en fonction de la trajectoire, de la vitesse ou de la présence d'un maraudage). Il s'agit d'une recherche en fonction de leurs caractéristiques comportementales.

12. Le dispositif litigieux traite donc bien de données relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique.

13. Troisièmement, la fonction de recherche par filtres vise à isoler une personne, à la distinguer d'un groupe. Ainsi, lorsqu'une personne correspondant à ces filtres est repérée par le dispositif, il est possible de lui appliquer un certain nombre d'actions : afficher son image isolée du reste de l'image (fonctionnalité « Visualiseur » du dispositif, *cf.* pièce n° 19, p. 9), ou encore afficher son image dans une version condensée de la vidéo lorsque plusieurs personnes ont été rechercher (fonctionnalité « Synopsis » du dispositif, *cf.* pièce n° 19, pp. 15–17). Il y a donc une identification unique des personnes ainsi recherchées.

14. **Il en résulte que** le dispositif litigieux constitue bien un traitement de données biométriques en raison de sa fonctionnalité de recherche de personnes en fonction de filtres fondés sur l'apparence physique. Partant, son illégalité est patente (*cf.* requête introductive d'instance du 5 août 2021, §§ 99–108).

15. À tout le moins, ainsi que rappelé dans les précédentes écritures des exposants, le dispositif constitue un traitement de données sensibles et son illégalité est également acquise de ce fait (*cf.* mémoire du 13 décembre 2023, §§ 59 et s.).

II. Sur l'absence de compétence de police judiciaire d'une commune

16. **En second lieu**, les dispositions du code de procédure pénale relatives aux réquisitions judiciaires d'images de vidéosurveillance n'ont pas pour effet de conférer un pouvoir de police judiciaire aux communes ou à leurs agents. C'est à tort que la CNIL estime qu'un dispositif de vidéosurveillance algorithmique tel que celui en cause pourrait être fondé par les dispositions du code de procédure pénale lors d'une recherche *a posteriori* de personnes sur les images de vidéosurveillance.

17. Elle fonde son raisonnement – à nouveau au prix d'une erreur de droit – sur l'idée erronée qu'un logiciel de vidéosurveillance algorithmique pourrait prétendument relever de la notion de « logiciel de rapprochement judiciaire ».

18. **En droit**, aux termes du premier alinéa de l'article 60-1 du code de procédure pénale, applicable aux crimes et délits flagrants :

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

19. Les articles 77-1-1 et 99-3 du même code reprennent les dispositions de l'article 60-1 pour les cas respectivement de l'enquête préliminaire et de l'instruction.

20. Il ressort de ces dispositions qu'une commune est seulement autorisée à communiquer les images de vidéosurveillance qu'elle détient, sur réquisition de l'autorité judiciaire. Cette communication n'implique aucunement une recherche

par filtres, ni humaine, ni algorithmique, qui relève de missions de police judiciaire qu'une commune ne détient pas. En pratique, lorsqu'une telle réquisition est exigée par l'autorité judiciaire, une commune doit seulement fournir les images qu'elle détient, indépendamment de son contenu. L'analyse des images – et la détermination de l'utilité ou non pour la procédure judiciaire – ne sera pas réalisée par la commune mais par l'autorité judiciaire elle-même. Il ne peut en aller autrement sans que la commune s'arroge des pouvoirs de police judiciaire qu'elle ne détient légalement pas.

21. Par ailleurs, comme les exposants l'ont expliqué dès leurs premières écritures (*cf.* requête introductive d'instance du 5 août 2021, §§ 68 et s.), tout traitement de données doit être licite, au sens où une base légale suffisamment claire et prévisible doit exister dans l'ordre juridique. Cette exigence s'applique aussi bien pour les traitements mis en œuvre dans le cadre de missions de police administrative que pour ceux mis en œuvre dans le cadre de missions de police judiciaire.

22. À titre d'illustration, par un jugement désormais définitif, le tribunal administratif d'Orléans a récemment annulé un contrat passé entre la commune d'Orléans et une société qui fournissait un dispositif d'audiosurveillance algorithmique (c'est-à-dire d'analyse des sons couplée au dispositif de vidéosurveillance de la commune) en raison de l'absence de base légale (*cf.* TA Orléans, 12 juillet 2024, *La Quadrature du Net*, n° 2104478).

23. De plus, une analyse *a posteriori* des images à la suite d'une demande de l'autorité judiciaire relève, contrairement à ce qu'affirme la CNIL dans ses observations, du titre III de la loi Informatique et Libertés transposant la directive « police-justice », et non du RGPD, dans la mesure où un tel traitement est expressément exclu du champ d'application de ce dernier par le d) du 2 de son l'article 2 (*cf.* CE, 22 juillet 2022, *La Quadrature du Net*, n° 451653).

24. Enfin, un logiciel de rapprochement judiciaires est défini à l'article 230-20 du code de procédure pénale, aux termes duquel :

> « *Afin de faciliter le rassemblement des preuves des infractions et l'identification de leurs auteurs, les services de la police nationale et de la gendarmerie nationale chargés d'une mission de police ju-*

> *diciaire ainsi que le service placé sous l'autorité du ministre chargé du budget chargé d'effectuer des enquêtes judiciaires peuvent mettre en œuvre, sous le contrôle de l'autorité judiciaire, des logiciels destinés à faciliter l'exploitation et le rapprochement d'informations sur les modes opératoires réunies par ces services* [...] »

25. En dehors du cas d'un rapprochement d'informations sur les « modes opératoires », il n'est donc pas possible pour l'autorité judiciaire d'utiliser un traitement de données relevant de l'article 230-20 du code de procédure pénale.

26. **En l'espèce**, c'est à tort que la CNIL estime qu'il serait « *acceptable* » (*cf.* mémoire de la CNIL du 2 décembre 2024, p. 6) qu'un dispositif de vidéosurveillance algorithmique tel que celui utilisé par la commune de Moirans puisse être fondé sur les dispositions du code de procédure pénale relatives aux réquisitions judiciaires.

27. En effet, ni la lettre, ni l'esprit des dispositions relatives aux réquisitions judiciaires ne permettent sérieusement d'aboutir à une telle conclusion. Le principe de clarté, exigé notamment par la Cour européenne des droits de l'homme (ci-après « CEDH »), la loi Informatique et Libertés et la directive « police-justice », fait également obstacle à ce que ces dispositions puissent être interprétées en ce sens (*cf.* mémoire du 5 août 2021, §§ 70–76). La CNIL se montre d'ailleurs très prudente dans sa formulation, usant du terme « *acceptable* » alors qu'elle est beaucoup plus affirmative lorsqu'elle décrit le régime juridique de la vidéosurveillance algorithmique utilisée en temps réel.

28. Le législateur est d'ailleurs lui-même conscient qu'il n'existe aucune base légale permettant de fonder un tel traitement de données en matière de police judiciaire. En effet, il a envisagé un temps d'introduire dans le droit national une telle base légale dans le cadre de la proposition de loi relative au renforcement de la sûreté dans les transports, actuellement en discussion à l'Assemblée nationale sous le numéro 134, qui comportait, jusqu'aux travaux en commission des Lois, un article 9 permettant à la SNCF et à la Régie autonome des transports parisiens de recourir à de telles analyses sur demande de l'autorité judiciaire « *aux seules fins de répondre aux réquisitions mentionnées aux articles 60-1, 60-2, 77-1-1, 77-1-2, 99-3 et 99-4 du code de procédure pénale* ».

29. Enfin, les fonctionnalités de recherches par filtres du logiciel « Briefcam » ne peuvent, contrairement à ce qu'affirme la CNIL, être qualifiées de logiciels de rapprochement judiciaire. En effet, la finalité des filtres du logiciel « Briefcam » est d'accélérer l'analyse des caractéristiques physiques, physiologiques ou comportementales (au sens de la direction d'une personne sur l'image ou de si elle est statique) de personnes physiques pour en tirer des informations sur la manière dont elles ont été filmées. Il s'ensuit qu'il ne s'agit aucunement d'une analyse du « mode opératoire ». En outre, il ressort du manuel d'utilisation du logiciel que celui-ci ne comporte aucune fonctionnalité d'analyse de modes opératoires de délits ou crimes, ni ne prétend poursuivre de telles finalités.

30. En tout état de cause, l'impossibilité pour une commune d'utiliser ce type de logiciel ne saurait être levée par une potentielle qualification en « logiciel de rapprochement judiciaire ». En effet, et comme cela a été démontré, la commune reste, en cas de réquisition des images de vidéosurveillance par l'autorité judiciaire, dépourvue de pouvoir de police judiciaire, donc dans l'impossibilité d'analyser les images de vidéosurveillance.

31. **Il en résulte qu**'il n'existe aucune base légale permettant de fonder l'utilisation des fonctionnalités de filtres du dispositif litigieux en matière de police judiciaire. Au surplus, ces fonctionnalités ne permettent de toute évidence pas de les qualifier de logiciel de rapprochement judiciaire.

PAR CES MOTIFS, M. Bastien le Querrec et l'association La Quadrature du Net, exposants, persistent dans leurs conclusions.

Fait à Paris, le 16 décembre 2024

Alexis FITZJEAN Ó COBHTHAIGH
Avocat au Barreau de Paris

BORDEREAU DES PRODUCTIONS

Pièces déjà communiquées :

Pièce n° 1 : Justificatif de domicile de M. Bastien Le Querrec (occulté des informations non pertinentes) ;

Pièce n° 2 : Statuts de LQDN ;

Pièce n° 3 : Pouvoir spécial pour LQDN ;

Pièce n° 4 : Manuel d'utilisation en version anglaise du logiciel « Briefcam », daté de juin 2020, publié par l'association Electronic Frontier Foundation sur son site Internet : `https://www.eff.org/fr/deeplinks/2020/11/video-analytics-user-manuals-are-guide-dystopia` ;

Pièce n° 5 : Extrait du *Guide de la vidéoprotection de l'association AN2V de 2020* où la ville de Moirans est mentionnée comme étant cliente d'un revendeur du logiciel « Briefcam » ;

Pièce n° 6 : Demande de communication de documents administratifs de M. Bastien Le Querrec à la maire de Moirans à propos de la vidéosurveillance à Moirans et de l'usage du logiciel « Briefcam » datée du 25 juillet 2020 ;

Pièce n° 7 : Accusé de réception de la demande de communication de documents administratifs du 25 juillet 2020 ;

Pièce n° 8 : Cahier des clauses techniques particulières du marché public de vidéosurveillance à Moirans ;

Pièce n° 9 : Premiers comptes-rendus de suivi des travaux d'installation du dispositif de vidéosurveillance à Moirans ;

Pièce n° 10 : Nouveaux comptes-rendus de suivi des travaux d'installation du dispositif de vidéosurveillance à Moirans ;

Pièce n° 11 : Lettre de la maire de Moirans à la CADA datée du 1er décembre 2020 ;

Pièce n° 12 : Lettre de la maire de Moirans à la CADA datée du 9 mai 2021 ;

Pièce n° 13 : Lettre de refus de la maire de Moirans de communiquer le manuel d'utilisation du logiciel « Briefcam » datée du 25 février 2021 ;

Pièce n° 14 : Avertissement de la CNIL à la ville de Valenciennes pour son dispositif d'analyse automatisée des images de vidéosurveillance daté du 12 mai 2021 ;

Pièce n° 15 : Article du site Internet de la CNIL « *Vidéoprotection : quelles sont les dispositions applicables ?* ». URL : `https://www.cnil.fr/fr/videoprotection-quelles-sont-les-dispositions-applicables` ;

Pièce n° 16 : Lignes directrices 3/2019 du CEPD sur le traitement des données à caractère personnel par des dispositifs vidéo, version 2.0, adoptées le 29 janvier 2020 ;

Pièce n° 17 : Courrier de réponse de la CNIL à M. Le Querrec concernant sa demande de communication de documents administratifs détenus par la CNIL concernant la vidéosurveillance à Moirans daté du 26 février 2021.

Pièce n° 18 : CNIL, « Caméras dites "intelligentes" ou "augmentées" dans les espaces publics – Position sur les conditions de déploiement », juillet 2022, URL : `https://www.cnil.fr/sites/cnil/files/atoms/files/cameras-intelligentes-augmentees_position_cnil.pdf` ;

Pièce n° 19 : Manuel d'utilisation en version française du logiciel « Briefcam », daté de juin 2018, communiqué par la commune de Moirans dans l'instance n° 2105327 ;

Pièce n° 20 : EDPB, Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo, version 2.1, 26 février 2020, URL : `https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_fr.pdf` (nouvelle version à jour de la pièce n° 16) ;

Pièce n° 21 : 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° 22 : Clément le Foll, Mathias Destal, « Reconnaissance faciale : Gérald Darmanin veut enterrer "l'affaire Briefcam" », Disclose, 9 avril 2024, URL : https://disclose.ngo/fr/article/reconnaissance-faciale-gerald-darmanin-veut-enterrer-laffaire-briefcam;

Pièce n° 23 : 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.

Nouvelle pièce :

Pièce n° 24 : Robin Medard Inghilterra, « L'instauration d'une "technopolice" administrative en milieu urbain : les droits et libertés sur un fil », *La Revue des droits de l'homme*, 26 | 2024, 17 octobre 2024. URL : http://journals.openedition.org/revdh/20912; DOI : https://doi.org/10.4000/12hr7.