

Délibération n° 2025-032 du 15 mai 2025 portant avis sur les conditions de mise en œuvre par la commune de Nice d'un traitement algorithmique de données à caractère personnel « franchissement de ligne » et « zone d'intrusion »

N° de la saisine : n°25000017	Thématiques : caméras « augmentées », analyse algorithmique en temps réel, franchissement de ligne, zone d'intrusion
Organisme(s) à l'origine de la saisine : commune de Nice	Fondement de la saisine : article 90 de la loi « informatique et libertés »

L'essentiel :

- 1. Le traitement « franchissement de ligne » et « zone d'intrusion » est mis en œuvre par la commune de Nice à des fins de police administrative. Il consiste à détecter, par un algorithme, des cas d'usage prédéterminés (entrée dans une zone interdite au public, détection de véhicules, etc.) pour alerter en temps réel le centre de supervision urbaine permettant l'intervention des agents de la police municipale.*
- 2. La CNIL considère que la surveillance algorithmique des entrées des écoles nécessite d'être prévue par la loi en ce qu'elle conduit à analyser, à des fins de police, une partie de la voie publique.*
- 3. Le traitement peut être mis en œuvre, sous réserve du respect des garanties précisées dans cet avis. La CNIL souligne l'exigence de limiter la détection algorithmique aux seules zones pouvant faire l'objet d'une intrusion et de réduire l'analyse des personnes sur la voie publique au strict minimum.*
- 4. Elle accueille favorablement les autres mesures de minimisation et de sécurité mises en place, ainsi que les modalités de conservation des données qui apparaissent proportionnées aux usages et finalités du dispositif.*

La Commission nationale de l'informatique et des libertés,

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (« loi informatique et libertés »).

Après avoir entendu le rapport de M. Claude Castelluccia, commissaire, et les observations de M. Damien Milic, commissaire du Gouvernement,

Adopte la délibération suivante :

I. La saisine

1. La commune de Nice a saisi la CNIL d'une demande de consultation, en application de l'article 90 de la loi du 6 janvier 1978, sur une AIPD relative au dispositif de vidéo algorithmique « franchissement de ligne » et « zone d'intrusion ».

2. Ce dispositif permet l'analyse, en temps réel, d'images issues d'espaces interdits ou fermés au public aux fins de détection de personnes non autorisées y accédant. Le franchissement de lignes prédéfinies fait remonter une alerte au centre de supervision urbain permettant l'intervention des agents de la police municipale afin de faire cesser l'intrusion. Il s'agit d'un dispositif d'analyse automatisée des images issues du système de vidéoprotection (ci-après « caméras augmentées »).

3. Ce traitement étant mis en œuvre à des fins de protection contre les menaces pour la sécurité publique et de prévention, il relève du régime juridique du titre III de la loi « informatique et libertés ». Ce dispositif relevant de la police administrative, il relève des attributions du maire de la commune, laquelle est autorité compétente au sens de la directive « Police-Justice ».

4. Conformément aux dispositions de l'article 90 de la loi « informatique et libertés », applicable à l'ensemble des traitements relevant du titre III de la loi, « *si le traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, notamment parce qu'il porte sur des données mentionnées au I de l'article 6, le responsable de traitement effectue une analyse d'impact relative à la protection des données à caractère personnel (AIPD)* ». Cet article prévoit en outre que « *le responsable de traitement ou son sous-traitant consulte la Commission nationale de l'informatique et des libertés préalablement à la mise en œuvre du traitement de données à caractère personnel [...] 2° lorsque le type de traitement, en particulier en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées* ».

5. Compte tenu de ce cadre juridique, une AIPD a été réalisée et transmise à la CNIL, qui considère que le traitement appelle les observations suivantes.

II. L'avis de la CNIL

A. Sur les finalités du traitement algorithmique

1. Sur les trois cas d'usage concernant des lieux non accessibles au public pendant les heures de fermeture

6. L'AIPD décrit trois cas d'usage concernant des lieux non accessibles au public pendant les heures de fermeture :

- « franchissement de ligne [REDACTED] » ayant pour objet de détecter la présence de personnes pénétrant dans les [REDACTED] de la commune pendant leurs heures de fermeture ;
- « zone d'intrusion [REDACTED] » ayant pour objet de détecter la présence de personnes pénétrant dans [REDACTED] pendant ses heures de fermeture ;
- « zone d'intrusion [REDACTED] » ayant pour objet de détecter la présence de personnes pénétrant dans [REDACTED]

7. Ces cas d'usage du traitement algorithmique apparaissent ne pas nécessiter l'intervention du législateur dès lors que les garanties fondamentales apportées aux citoyens pour l'exercice des libertés publiques ne sont pas affectées, s'agissant de lieux dont l'accès est interdit au public. La finalité essentielle de ce dispositif est la protection de ces espaces contre les intrusions.

8. Il convient néanmoins de respecter le titre III de la loi « informatique et libertés ».

2. Sur le cas d'usage « [REDACTED] » pendant les horaires d'ouverture

9. L'AIPD fait état d'un cas d'usage consistant en la surveillance algorithmique de la [REDACTED]. Il est précisé qu'il s'agit de « détecter la présence de véhicules stationnant [REDACTED]

10. Les zones analysées par l'algorithme [REDACTED] sont des espaces appartenant à la voie publique. La commune de Nice a confirmé ce point mais a insisté sur le caractère interdit de ces espaces de stationnement en application du Plan Vigipirate. Elle a précisé que l'algorithme est paramétré de manière à ne détecter que des véhicules, à l'exclusion de tout autre objet ou personne physique.

11. La CNIL rappelle sa position de juillet 2022 sur les caméras « augmentées » dans les espaces publics estimant que, lorsqu'il s'agit de réaliser une analyse en temps réel et automatisée d'images de caméras de vidéoprotection en vue d'une intervention immédiate par les services de police ou de l'engagement de procédures administratives ou judiciaires, le traitement algorithmique, y compris lorsque sa mise en œuvre apparaît légitime, emporte des enjeux spécifiques qui conduisent à considérer qu'un encadrement législatif spécifique s'impose.

12. Par leur fonctionnement même, reposant sur la détection et l'analyse en continu et en temps réel des attributs ou des comportements des individus dans un espace ouvert au public, les dispositifs de vidéo « augmentée » présentent, par nature, un risque de surveillance généralisée sur la voie publique. **Ce type de traitements et l'encadrement législatif de leurs risques ont fait l'objet d'une expérimentation dans le cadre de la loi du 19 mai 2023 relative aux jeux Olympiques et Paralympiques (loi JOP). La mise en œuvre d'autres dispositifs algorithmiques présentant des risques similaires n'est actuellement pas permise en l'état de la législation.**

13. L'augmentation des risques d'actions terroristes, invoquée par la commune à l'appui de son dispositif (AIPD p. 1), ne saurait justifier le déploiement de traitements algorithmiques à des fins de police en l'absence de texte l'autorisant. Même lorsque ces techniques concernent un évènement particulier et sont donc circonscrites dans le temps et dans l'espace, leur utilisation pour des finalités de maintien de l'ordre public par les forces de police nécessite un encadrement législatif ainsi que l'a prévu la loi JOP.

B. Sur la minimisation des données analysées par la vidéosurveillance algorithmique

14. La CNIL rappelle l'exigence de limiter le plus possible les zones de détections algorithmiques aux seules zones pouvant faire l'objet d'une intrusion, et de réduire l'analyse des personnes sur la voie publique au strict minimum. Ainsi, si la CNIL approuve le recours à une limite virtuelle limitant les zones de détection, un masquage actif, par le biais d'une obfuscation visuelle des zones de non-détection, pourrait également permettre d'atteindre l'objectif susvisé. Cette limitation devrait, sans que cela ne nuise à la poursuite des finalités prévues, être la plus circonscrite possible pour respecter dans le même temps le principe de minimisation.

15. La CNIL recommande, en outre, d'étudier la mise en place des mesures de minimisation complémentaires, si elles ne nuisent pas à l'efficacité requise du dispositif, notamment :

- la réduction de la résolution et la diminution de la fréquence de capture ;
- l'éventuel recours à des mesures de dégradation algorithmique du flux vidéo (floutage, pixellisation, etc.).

16. Concernant spécifiquement le cas d'usage « [REDACTED] », **elle accueille favorablement le recours à des capteurs distincts de caméras classiques ([REDACTED]), conforme au principe de minimisation et qui apparaît comme une alternative moins intrusive.**

17. Néanmoins, à l'appui des captures d'écran du champ de vision des zones concernées par l'analyse algorithmique transmises par la commune, la CNIL relève que certaines caméras de ce dispositif permettent également de détecter des personnes se déplaçant sur la voie publique jusqu'à la zone d'intrusion. En particulier, une des caméras orientées sur les zones couvrant la [REDACTED] filme directement un trottoir, donc la voie publique (capture n° 0521-[REDACTED] du 04-09-2025), ce qui soulève des difficultés particulières quant à l'encadrement de ce dispositif dès lors que des personnes y circulent librement.

18. La CNIL invite la commune à s'assurer que l'analyse algorithmique ne conduise ni à la détection de présence humaine ni à la qualification de comportements de personnes se trouvant sur la voie publique.

C. Sur les durées de conservation

19. Selon l'AIPD transmise :

- les images de vidéoprotection sont conservées pendant dix jours ;
- la surcouche algorithmique fonctionne uniquement en temps réel et l'image comportant la délimitation de la zone et/ou l'objet détecté faisant l'objet d'une alerte ne fait l'objet d'aucune conservation.

20. La CNIL accueille favorablement ces modalités de conservation qui apparaissent proportionnées aux usages et finalités du dispositif.

21. Il ressort des éléments apportés dans le cadre de la demande de complément d'informations que les logs d'accès et de détection sont conservés trois ans :

- les logs « techniques » correspondent aux informations relatives aux connexions des opérateurs sur le logiciel de main courante opérationnelle, dans le cadre de leur mission de gestion du système de vidéoprotection de la ville de Nice (opérations de collecte, de modification, de consultation, de communication et d'effacement des données traitées). Leur durée de conservation a été déterminée conformément à l'article R. 253-5 du code de la sécurité intérieure ;
- les logs « d'alertes » correspondent aux informations relatives à la réception et au traitement des alertes émises par le système de traitement automatisé d'images. Celles-ci sont utilisées pour l'établissement de statistiques relatives à l'état de la délinquance sur le territoire de la ville de Nice et à son évolution.

22. **La CNIL estime que cette durée de conservation commune de trois ans est justifiée.** Elle souligne que ces statistiques ne peuvent être réalisées que sur la base de données agrégées ne permettant pas la réidentification des personnes concernées. À ce titre, s'agissant d'un dispositif de police administrative circonscrit à la protection des espaces communaux contre les intrusions, elle prend acte de ce que les données saisies dans les zones de commentaires libres du logiciel de main courante opérationnelle ne sont pas identifiantes.

D. Sur les mesures de sécurité

23. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]. **L'AIPD devrait être mise à jour en ce sens.**

24. Concernant la revue de gestion des droits et des habilitations, la commune a indiqué que le « *sous-traitant dispose d'un accès permanent au système de vidéoprotection pour en assurer la maintenance* » et que ces collaborateurs sont « *habilités à se connecter sans autorisation préalable* ».

25. La CNIL s'interroge sur les mesures organisationnelles et techniques mises en œuvre afin de limiter les accès du sous-traitant uniquement pour les finalités précédemment évoquées ainsi que les modalités de revue des habilitations pour l'ensemble des sous-traitants. La CNIL invite notamment la commune à s'assurer que ses sous-traitants n'ont pas accès à distance aux flux vidéo sans autorisation préalable et uniquement dans le cadre d'une intervention de maintenance prédéfinie.

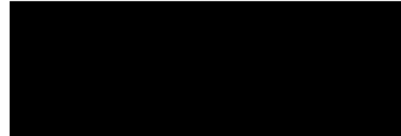
E. Sur la base légale du traitement

26. Le traitement s'inscrit dans le cadre de l'exercice des missions d'intérêt public poursuivies par la commune à des fins de protection contre les menaces pour la sécurité publique et de prévention. Ce traitement peut être créé par une collectivité territoriale, autorité compétente, et relève des dispositions du titre III de la loi « informatique et libertés ».

27. **La CNIL rappelle, à ce titre, qu'un acte réglementaire devra être adopté par la commune à l'issue de la notification du présent avis afin d'autoriser le dispositif de détection des intrusions au sein des zones fermées au public et d'exclure notamment le droit d'opposition, en application de l'article 87 et de l'article 110 de la loi « informatique et libertés », sous réserve de la mise en œuvre des garanties précisées au présent avis.**

28. Les autres conditions de mise en œuvre de ce traitement, tel que décrit dans l'AIPD, n'appellent pas d'observations.

La présidente,



M.-L. Denis