EXPERIMENTATION DE TRAITEMENTS ALGORITHMIQUES D'IMAGES LEGALEMENT COLLECTEES AU MOYEN DE SYSTEMES DE VIDEOPROTECTION

RAPPORT DU COMITE D'EVALUATION

Janvier 2025

SOMMAIRE

Avant-propos 6

Une commande législative et une organisation étroitement précisées par la loi et le décret 6

Un thème d'une sensibilité particulière 6

Un rapport attendu 6

L'objet du rapport 7

Comment dénommer le dispositif ? 7

Introduction 8

Présentation générale 8

Le recours à l'IA en matière de vidéoprotection : des opportunités et des inquiétudes légitimes 8

Une expérimentation très encadrée 8

Le rôle et l'organisation du comité d'évaluation de l'expérimentation 9

Initiatives et investigations sur le terrain du comité d'évaluation 10

Démarche générale du comité 12

Observations générales sur le déroulement de l'évaluation 12

Une évaluation réalisée sur une période relativement brève 12

Une évaluation principalement centrée sur le dispositif de la société Wintics 13

Des conditions d'accueil globalement satisfaisantes 13

Contexte général de l'expérimentation 13

Un calendrier particulièrement serré 13

Un intérêt paradoxalement plus limité pendant la période olympique 14

1ère partie - Organisation et caractéristiques du dispositif de vidéoprotection intégrant l'intelligence artificielle 15

1.1. Historique et contexte de l'expérimentation 15

1.1.1. L'origine de l'expérimentation 15

a) Des initiatives nombreuses avant la loi du 19 mai 2023 15

b) Des dispositifs dont la légalité était interrogée au niveau national 16

1.1.2. Un dispositif à replacer dans le contexte international 18

1.1.3. Le contexte et la préparation de la présente expérimentation 19

1.2. Une expérimentation étroitement encadrée par le droit 20

1.2.1. Un cadre juridique très précis 20

a) Un cadre progressivement resserré à chaque stade de l'élaboration du dispositif 20

b) Finalités, objet et durée de l'expérimentation 21

c) Garanties générales pour le respect des libertés publiques 23

d) Caractéristiques techniques des traitements autorisés 25

e) Conditions de développement et de l'emploi des traitements 25

f) La remise en cause de la légalité des dispositifs de caméras avec IA mis en place avant l'édiction du nouveau cadre juridique 26

1.2.2. Des choix structurants faits au stade de la procédure d'appel d'offres 27

a) Des contraintes techniques encore renforcées 27

b) Un processus de sélection très centralisé et atypique 28

c) Le coût financier et le financement du dispositif 29

1.3. Le dispositif opérationnel mis en œuvre 30

1.3.1. Caractéristiques générales du système de vidéoprotection et des traitements algorithmiques 30
1.3.2. Une phase de calibrage cruciale en vue de l'efficacité du dispositif 31
a) Observations générales 31
b) Des modalités de déroulement différentes selon les opérateurs 32
1.3.3. Les moyens techniques mis en place : des choix différents selon les opérateurs 32
a) Les chiffres-clefs de l'expérimentation 32
b) Préfecture de police 33
c) SNCF 35
d) RATP 37
e) Commune de Cannes 40
1.3.4. Cybersécurité 41
1.3.5. Moyens en personnel déployés dans le cadre de l'expérimentation 43
a) Effectifs 43
b) Formation 44
1.3.6. Suites administratives et judiciaires 45

2. Des performances techniques très variables selon les opérateurs et les cas d'usage 46

2.1. Des performances délicates à apprécier au moyen d'indicateurs statistiques 46
2.1.1. Les indicateurs habituellement utilisés pour évaluer la qualité de la détection 46
2.1.2. Les difficultés rencontrées dans le cadre de l'expérimentation 47
a) De la difficulté de mesurer les « faux négatifs » et les « vrais négatifs » 47
b) Une distinction parfois délicate entre « vrais positifs » et « faux positifs » 48
c) Des résultats qui dépendent du calibrage réalisé 49

2.2. Des performances affectées par les caractéristiques du traitement utilisé 49
2.2.1. Les différences entre les résultats observés lors de la programmation et dans l'environnement réel 49
2.2.2. Les difficultés à définir une zone de détection pertinente 50
2.2.3. Des performances qui dépendent de la qualité du calibrage préalablement réalisé et du bon déroulement du processus itératif avec le prestataire 51
2.2.4. L'absence de visualisation des motifs de signalisation 52

2.3. Des performances variables selon les cas d'usage 52
2.3.1. Des performances globalement satisfaisantes pour l'intrusion, la circulation et la densité de personnes 52
2.3.2. Des résultats encore incertains et à améliorer pour les mouvements de foule 54
2.3.3. Des performances inégales pour la détection d'objets abandonnés et d'armes à feu 55
2.3.4. Des performances très insatisfaisantes pour la détection des départs de feu et de la présence d'une personne au sol à la suite d'une chute 57
2.3.5. Récapitulatif statistique selon chaque opérateur 57
a) Préfecture de police 57
b) RATP 58
c) SNCF 59
d) Commune de Cannes 60

3. Un intérêt opérationnel limité mais réel 63

3.1. Un intérêt variable selon le contexte d'utilisation 63
3.1.1. Un nombre résiduel d'interventions réalisées grâce au recours à l'IA 63
3.1.2. Un intérêt opérationnel, de façon générale, limité en cas de forte présence policière 65
3.1.3. Un intérêt opérationnel qui dépend de la durée d'entraînement de la caméra 66
3.1.4. Un intérêt subordonné à la mise en œuvre du traitement pendant une durée suffisamment longue 66
3.1.5. Un intérêt qui dépend de l'aptitude à mobiliser des effectifs suffisants pour traiter et pour exploiter les alertes déclenchées 67

3.1.6. Les limites en lien avec les catégories d'agents habilités à utiliser le traitement 67
3.1.7. Un intérêt qui dépend du choix des zones à risques 68

3.2. Un intérêt opérationnel variable selon les cas d'usage 68
3.2.1. Un intérêt opérationnel plus marqué pour l'intrusion et la circulation des personnes 68
3.2.2. Un intérêt à ce stade plus limité pour la détection des mouvements de foule, de la densité excessive d'individus, des objets abandonnés et des départs de feu 69
3.2.3. Un intérêt très incertain pour la détection des départs de feu et de la présence d'une personne au sol à la suite d'une chute 70

3.3. Un degré d'attente et de confiance des personnels globalement élevé 70
3.3.1. Observations générales 70
3.3.2. Observations spécifiques à chaque opérateur 71

3.4. Libres propos des différents intervenants 73
Préfecture de police 73
RATP 75
SNCF 77
Ile de France Mobilité 77
Commune de Cannes 79
Délégation interministérielle au Jeux olympiques et paralympiques 80

4. Un public insuffisamment informé mais intéressé 83

4.1. L'information du public 83
4.1.1. Le dispositif général mis en place 83
4.1.2. Les modalités d'information spécifiques à chaque opérateur 83
4.1.3. Une information à améliorer 86
4.1.4. De très faibles remontées du public qui interrogent 87

4.2. L'association à l'expérimentation 87
4.2.1. Les réactions des associations, de la Défenseure des droits et du Conseil national des barreaux 87
4.2.2. Les précédentes études visant à évaluer le degré de confiance du public dans le recours à l'intelligence artificielle en matière de vidéoprotection 89
4.2.3. L'étude quantitative et qualitative réalisée par le comité d'évaluation 90

5. Un dispositif expérimental qui, en l'état, ne heurte les libertés publiques ni dans sa conception ni dans sa mise en œuvre 92

5.1. Conformité aux prescriptions légales et réglementaires 92
5.1.1. Un respect des différentes exigences procédurales globalement satisfaisant 92
5.1.2. Le respect des conditions de fond posées par la loi 92
5.1.3. Le respect des exigences de confidentialité des données conservées 93

5.2. Un dispositif soumis aux exigences du RGPD et de la législation CNIL 94
5.2.1. L'applicabilité du RGPD et de la loi CNIL au dispositif IA 94
5.2.2. Une question de principe : les données peuvent-elles être qualifiées de biométriques ? 95
5.2.3. Le respect du principe de minimisation 96
5.2.4. Droit d'accès aux données personnelles 97
5.2.5. Droit d'opposition, de modification et d'effacement 97

5.3. La question de la conformité du dispositif au règlement européen sur l'IA 98

5.4. Enjeux plus généraux sur les libertés publiques 99
5.4.1. Le principe de liberté d'aller et venir 99
5.4.2. Le respect des finalités légales 100
5.4.3. Le principe de non-discrimination 100
5.4.4. Les conditions d'utilisation dans un cadre judiciaire 102
5.4.5. Les craintes d'un premier pas vers des dispositifs plus intrusifs 102

Conclusion générale ____ *104*

Synthèse des observations du comité ____ **104**

Les perspectives et points d'attention ____ **105**

L'abandon, la prolongation ou la pérennisation : un choix politique qui ne relève pas de la mission du comité d'évaluation ____ 105

Les enseignements en ce qui concerne la méthodologie pour le suivi du dispositif ____ 105

Points d'attention sur les plans juridique, administratif et technique ____ 106

ANNEXES ____ *110*

1°) Composition du comité d'évaluation ____ **111**

2°) Liste des personnes auditionnées ou ayant remis une contribution écrite ____ **113**

3°) Récapitulatif des déplacements des membres du comité dans le cadre des expérimentations ____ **114**

4°) Comparaison européenne et internationale sur les traitements algorithmiques en matière de vidéoprotection ____ **115**

5°) Liste des principaux acronymes ____ **119**

6°) Rappel des phases préalables au plan technique et réglementaire pour la mise en œuvre opérationnelle des solutions logicielles (note de la DEPSA) ____ **120**

7°) Récapitulatif des tests effectués dans le cadre de l'expérimentation ____

8°) Protocole d'évaluation ____

9°) Étude commandée au cabinet Verian ____

10°) Compte-rendu du déplacement à Cannes le 11 décembre 2024 ____

11°) Contribution de la Défenseure des droits ____

12°) Prises de position des associations Quadrature du net et LDH ____

13°) Travail réalisé par les étudiants de l'Incubateur de politiques publiques de Sciences po au sujet de l'information du public ____

14°) Contribution de l'Association des maires de France ____

Avant-propos

Une commande législative et une organisation étroitement précisées par la loi et le décret

C'est le législateur qui a prévu la constitution d'un comité en charge d'évaluer l'expérimentation sur le recours aux traitements algorithmiques en matière de vidéoprotection. Le Sénat a introduit les parlementaires dans le comité d'évaluation[1].

Un décret a ensuite précisé les missions et conditions d'organisation et de fonctionnement de ce comité.

Un thème d'une sensibilité particulière

L'IA suscite des craintes, réelles ou non. Elle renvoie à la reconnaissance faciale et aux usages qui peuvent en être faits dans certains Etats autoritaires.

Les inquiétudes légitimes de l'opinion ont été relayées au Parlement et prises en compte par le Conseil constitutionnel[2].

Le recours à l'IA en matière de vidéoprotection suscite une attention particulière de la part du Conseil d'Etat et de la CNIL, compte tenu des enjeux pour les libertés.

Un rapport attendu

Le comité a conscience du fait que le présent rapport est particulièrement attendu de la part du Parlement, du Gouvernement, de l'administration, des opérateurs, des professionnels et de certaines associations.

Le rapport d'information sur l'application de la loi du 19 mai 2023, remis le 10 avril 2024 par les sénatrices Agnès Canayer et Marie-Pierre de la Gontrie[3], souligne ainsi que, « *compte tenu de la sensibilité de la question et des nombreuses attentes pesant sur ce bilan* », la phase d'évaluation « *ne constituera pas une simple formalité procédurale mais donnera lieu à de nombreux débats pratiques, théoriques et politiques. A l'inverse, elle implique la définition d'un cadre rigoureux, objectif et précis pour rendre compte des réussites et des échecs de l'expérimentation, dont les résultats opérationnels doivent être mesurés comme la mise en œuvre des garanties destinées à encadrer le déploiement des traitements algorithmiques* ».

Il s'agit d'un exercice de « démocratie technologique ».

---

[1] Amendement COM 90 de la commission des lois.
[2] Décision n° 2023-850 DC du 17 mai 2023
[3] Rapport d'information fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur l'application de la loi du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, enregistré à la présidence du Sénat le 10 avril 2024 r23-5271.pdf

L’objet du rapport

Le rapport ne traite que des dispositifs testés dans le cadre de la présente expérimentation.

Pas des solutions techniques alternatives qui auraient pu être mises en œuvre. Et pas non plus des autres fonctionnalités et cas d’usage qui seraient susceptibles d’être développés au moyen de l’intelligence artificielle.

Cette expérimentation a été initiée à l’occasion et dans la perspective de l’organisation d’un évènement d'ampleur exceptionnelle, les Jeux olympiques et paralympiques. Elle a commencé avant et s’est poursuivie après les épreuves olympiques, qui ont nécessité des mesures et des moyens exceptionnels, notamment en matière de sécurité, puisque le risque terroriste en particulier était jugé élevé. Mais ces traitements sont susceptibles, à l’avenir, d’être mis en œuvre en dehors d’un tel contexte. C’est l’une des difficultés abordées dans le rapport.

Comment dénommer le dispositif ?

La terminologie n’est pas neutre.

Le rapport privilégie, de façon générale, les termes utilisés par la loi.

Le comité sait que la loi qui a inventé la vidéo à usage de sécurité sur la voie publique, la loi n °95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, n'utilisait en son article 10 que le terme de « vidéosurveillance », appuyé sur la réalité du dispositif.

C'est la loi ultérieure du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure qui a préféré, en son article 17, le terme plus mobilisateur de « vidéoprotection » avec une affirmation péremptoire « dans tous les textes législatifs et réglementaires, le mot « vidéosurveillance » est remplacé par le mot vidéoprotection ». Dans son rapport n°517 (2009), le sénateur Jean-Patrick Courtois rappelait que cette substitution correspondait « au souhait du gouvernement de souligner le caractère protecteur de cette technologie ».

De manière générale, le comité a privilégié plus que les dénominations « soulignantes », celles fixées par la loi et celles à caractère objectif.

De même, le choix a été fait de privilégier l’expression « traitement algorithmique », de préférence à « caméra augmentée » (l’expression a certes été retenue en concertation avec la CNIL sur la signalétique mais elle est ambigüe en ce qu’elle pourrait être perçue comme marquant une forme de progrès) ou encore à « vidéo intelligente ». Les termes « augmentées » ou « intelligentes » relèvent du commentaire mais ni de la science ni du droit.

D’autres formulations auraient encore pu être envisagées comme « caméra active / activée » en ce que la caméra ne se borne pas à observer ou à enregistrer mais qu’elle sélectionne et alerte.

Il sera également fait référence à « l’intelligence artificielle », dès lors que celle-ci est bien utilisée et que la notion fait désormais l’objet d’un encadrement spécifique au plan européen (cf. *infra*).

Introduction

Présentation générale

Le recours à l'IA en matière de vidéoprotection : des opportunités et des inquiétudes légitimes

▪ Ces dernières années, différents traitements recourant à l'intelligence artificielle ont été conçus afin de renforcer l'efficacité des dispositifs de vidéoprotection, en particulier dans l'espace public.

En effet, la masse des images captées par ces dispositifs est souvent telle qu'elle dépasse les capacités d'attention et d'analyse humaine mobilisables[4].

Les traitements algorithmiques peuvent permettre de faciliter la détection en temps réel des situations que l'expérience des forces de l'ordre permet de regarder comme justifiant une attention particulière, qu'il s'agisse d'objets susceptibles de présenter une dangerosité (armes, colis suspects, véhicule…), d'intrusion de personnes ou de véhicules dans une zone interdite ou de la détection d'une densité excessive d'individus ou de mouvements de foule. La fonction attendue du traitement est de signaler à l'attention des agents en charge du contrôle vidéo l'occurrence et la source de telles images. Il s'agit ainsi d'une aide à la décision, et en aucun cas d'une substitution de l'intelligence artificielle à l'humain.

▪ Ces dispositifs ont cependant suscité nombre d'inquiétudes (cf. point *4.2.1.*) de la part notamment d'autorités administratives indépendantes, d'associations et d'universitaires, quant à l'atteinte qui serait ainsi portée au respect de l'intimité et de la vie privée. Il en est ainsi, en particulier, de ceux qui traitent de données biométriques ou qui recourent à la reconnaissance faciale.

En effet, en l'absence de certitudes du cadre juridique, des fabricants de logiciels ont commercialisé leurs dispositifs auprès des entreprises et des administrations. Des polémiques s'en sont suivies et des instances contentieuses ont été engagées (cf. *infra*). La Défenseure des droits s'est très récemment fait l'écho de ces appréhensions[5].

Une expérimentation très encadrée

▪ Dans ce contexte, l'article 10 de la loi[6] du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions a prévu, à titre expérimental, jusqu'au 31 mars 2025, que les images collectées au moyen de systèmes de vidéoprotection ou de drones pouvaient faire l'objet de traitements algorithmiques en temps réel.

Cette expérimentation est étroitement encadrée :
- Par sa finalité, qui est uniquement « *d'assurer la sécurité de manifestations sportives, récréatives ou culturelles qui, par l'ampleur de leur fréquentation ou par leurs circonstances,*

[4] Ainsi, par exemple, la SNCF dispose d'un total d'environ 70 000 caméras de vidéoprotection, dont 20 000 dans les gares et 50 000 dans les trains, pour seulement quelques dizaines d'opérateurs vidéo.
[5] https://www.lemonde.fr/les-decodeurs/article/2024/11/13/la-defenseure-des-droits-appelle-a-la-vigilance-sur-l-usage-des-algorithmes-par-les-services-publics_6390994_4355770.html
[6] n° 2023-380

sont particulièrement exposées à des risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes » ;

- Par les sites concernés, à savoir *« les lieux accueillant ces manifestations et à leurs abords ainsi que dans les véhicules et les emprises de transport public et sur les voies les desservant* » ;
- Par l'objet des traitements mis en place, qui porte exclusivement sur « *[la détection], en temps réel, des événements prédéterminés susceptibles de présenter ou de révéler ces risques et [sur leur signalement] en vue de la mise en œuvre des mesures nécessaires par les services de la police nationale et de la gendarmerie nationale, les services d'incendie et de secours, les services de police municipale et les services internes de sécurité de la SNCF et de la RATP* » ;
- Par la centralisation de la procédure de sélection du prestataire ;
- Par sa durée – l'expérimentation expire au 31 mars 2025 ;
- Par son évaluation « pluridisciplinaire et objective », le présent comité participe de l'encadrement.

Le rôle et l'organisation du comité d'évaluation de l'expérimentation

Cet article 10 prévoit, en son XI, la remise par le Gouvernement au Parlement d'un rapport d'évaluation sur la mise en œuvre de l'expérimentation, trois mois avant son terme, fixé au 31 mars 2025.

Un décret d'application du 11 octobre 2023[7] confie cette mission à un comité d'évaluation, présidé par une personnalité indépendante désignée par décret. Ce comité comprend un collège des personnalités indépendantes, toutes proposées par des instances indépendantes, où siègent notamment deux députés et deux sénateurs, et un collège des services utilisateurs.

<u>Composition du collège des personnalités indépendantes :</u>
a) Deux députés et deux sénateurs ;
b) Deux personnalités qualifiées pour leurs connaissances en matière de protection des données à caractère personnel désignées par la présidente de la CNIL ;
c) Deux personnalités qualifiées pour leurs connaissances en matière de technologies numériques désignées par l'Académie des technologies ;
d) Quatre personnalités qualifiées dans l'appréciation des enjeux relatifs aux libertés publiques, désignées sur proposition du président du comité ;
e) Le maire d'une commune n'ayant pas participé à l'expérimentation, désigné par le président de l'association des maires de France ;

<u>Composition du collège des services utilisateurs :</u>
a) Le directeur général de la police nationale ou son représentant ;
b) Le directeur général de la gendarmerie nationale ou son représentant[8] ;
c) Le directeur général de la sécurité civile et de la gestion des crises ou son représentant ;
d) Le préfet de police ou son représentant ;
e) Le directeur des entreprises et partenariats de sécurité et des armes ou son représentant ;
f) Le maire d'une commune ayant participé à l'expérimentation désigné par le président de l'association des maires de France ;
g) Le président-directeur-général de la RATP ou son représentant ;
h) Le président-directeur-général de la SNCF ou son représentant ;
i) La présidente d'Ile-de-France Mobilités ou son représentant ;

[7] Décret n° 2023-939 relatif aux modalités de pilotage et d'évaluation de l'expérimentation de traitements algorithmiques d'images légalement collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs.

[8] Les directions générales de la Police nationale et la Gendarmerie nationale n'ont pas procédé elles-mêmes directement à l'expérimentation, même si elles sont représentées dans le comité d'évaluation, comme d'ailleurs dans le comité de pilotage.

j) Le délégué interministériel aux jeux Olympiques et Paralympiques 2024 ou son représentant.

Le président du comité d'évaluation a été désigné par décret du 28 novembre 2023[9] et l'arrêté du ministre de l'intérieur portant désignation de ses membres a été pris le 18 juin 2024[10] et actualisé par arrêté du 10 janvier 2025[11] (cf. annexe n° 1).

Le décret du 11 octobre 2023 précise par ailleurs l'objet du présent rapport[12]. Celui-ci porte sur :
- « *Les performances techniques des traitements algorithmiques mis en œuvre* » ;
- « *Les effets opérationnels du recours aux traitements algorithmiques pour sécuriser les manifestations concernées* » ;
- « *L'impact des traitements algorithmiques sur la sécurité et l'exercice des libertés publiques, ainsi que la perception de cet impact par le public* ».

▪ Le comité d'évaluation est distinct du comité de pilotage de l'expérimentation, chargé, par le décret du 11 octobre 2023 précité[13], d'assurer la coordination et le suivi de l'expérimentation, en associant les utilisateurs des traitements et les services du ministère de l'intérieur compétents.

A l'exception de sa présidente, Mme Julie Mercier, directrice des entreprises et des partenariats de sécurité et des armes (DEPSA)[14], aucun membre du comité de pilotage ne peut ainsi siéger au sein du collège des services utilisateurs du comité d'évaluation[15].

Initiatives et investigations sur le terrain du comité d'évaluation

▪ Le comité d'évaluation a commencé ses travaux dès le mois de février 2024, même si sa constitution officielle a dû être reportée jusqu'au mois de juin dans l'attente de certaines désignations.

Le comité s'est réuni chaque mois, tantôt en formation « plénière », avec la participation des deux représentants de ses deux collèges, tantôt en présence des seuls membres du collège des personnalités indépendantes.

▪ Le comité a examiné les différents **documents recueillis**, et en particulier les travaux parlementaires, les avis du Conseil d'Etat, les rapports de la CNIL et de la Commission nationale consultative des droits de l'homme, les observations de la Défenseure des droits,

[9] Décret du 28 novembre 2023 portant nomination du président du comité d'évaluation de l'expérimentation de traitements algorithmiques d'images légalement collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs, publié au JORF du 29 novembre 2023.
[10] Arrêté du 18 juin 2024 portant nomination des membres du comité d'évaluation de l'expérimentation de traitements algorithmiques d'images légalement collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs, publié au JORF du 22 juin 2024.
[11] Arrêté du 10 janvier 2025 portant nomination des membres du comité d'évaluation de l'expérimentation de traitements algorithmiques d'images légalement collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs, publié au JORF du 12 janvier 2025.
Cette actualisation visait notamment à tenir compte de la désignation, faite par le bureau de l'Assemblée nationale au mois de novembre, de Mme Regol en lieu et place de Mme Bazin-Malgras, qui avait été initialement désignée avant la dissolution de l'Assemblée nationale.
[12] II de l'article 4.
[13] Articles 1er et 2.
[14] Arrêté du 18 juin 2024 précité.
[15] Dernier alinéa de l'article 3 du décret du 11 octobre 2023 précité.

différentes études universitaires consacrées à cette thématique, les documents administratifs préalables à la mise en œuvre des traitements algorithmiques ainsi que les rapports remis par chaque utilisateur à la suite de chaque test ainsi que leur rapport général sur le bilan de l'expérimentation.

▪ De **nombreux déplacements** ont été organisés sur les différents sites et salles de commandement de l'expérimentation, aussi bien avant, pendant qu'après les Jeux olympiques et paralympiques (récapitulatif des visites en annexe n° 3).

Plusieurs membres du comité se sont ainsi rendus au siège de la préfecture de police, île de la Cité, le dimanche 3 mars 2024, dans le cadre du premier test de paramétrage du dispositif, à l'occasion du concert du groupe *Dépêche Mode* au Bercy Arena.

D'autres visites ont été organisées par la suite, dans le cadre d'évènements préparatoires, avant les Jeux, dans les locaux de la SNCF (par ex. suivi du match PSG – Lyon, du 19 au 22 avril 2024), ou encore de la RATP (par ex. concert du groupe *Black Eyes Peas* à l'Arena Défense, le 20 avril 2024).

Une visite a également été organisée lors de l'expérimentation du dispositif à Cannes, lors du Festival, le 23 mai 2024.

Pendant les Jeux olympiques et paralympiques, les nombreux déplacements effectués ont permis d'observer le déploiement du dispositif sur différents sites où le traitement algorithmique était mis en œuvre, soit au poste de commandement de la préfecture de police soit dans certains postes de commandement sur place, dans la mesure où le comité était informé de ces tests. Les membres du comité ont ainsi été en mesure d'apprécier son fonctionnement dans des configurations très différentes (opérateur concerné, étendue du site, nombre de caméras…) et à tous les stades de l'expérimentation, aussi bien la phase préparatoire que la phase opérationnelle.

Après les Jeux paralympiques, le comité a effectué d'autres déplacements, par exemple, le 11 décembre 2024 à Cannes, les 14 décembre 2024 et 3 janvier 2025 à la RATP, les 15 et 31 décembre 2024 à la préfecture de police et les 19 décembre 2024 et 6 janvier 2025 à la SNCF.

Le comité d'évaluation a notamment pu échanger directement avec les opérateurs vidéo utilisant les algorithmes afin de recueillir leur appréciation puisqu'ils sont les premiers concernés.

▪ Outre ces visites, les membres du comité ont **auditionné** (cf. annexe n° 2) les différents acteurs du projet :

- Les responsables du déploiement du dispositif au sein des administrations (ministère de l'intérieur, Délégation interministérielle aux Jeux Olympiques, préfecture de police…), de la SNCF et de la RATP ;
- La présidente de la CNIL avec laquelle les échanges ont été réguliers ;
- Les représentants des sociétés Wintics et Videtics, sociétés prestataires qui sont intervenues dans le cadre des dispositifs mis en place, respectivement, au sein de la préfecture de police, de la RATP et de la SNCF, d'une part, et de la commune de Cannes, d'autre part[16] ;

[16] Les conditions de désignation des différents prestataires sont décrites *infra*.

- Des associations de défense des libertés publiques (« La Quadrature du Net » et La Ligue des droits de l'homme).

▪ Ainsi que le prévoyait le décret du 11 octobre 2023, le comité a élaboré un protocole d'évaluation (en annexe n° 8 du présent rapport), validé en formation plénière et définitivement arrêté le 25 juillet 2024.

Ce document énumère, pour chacun des objets de l'expérimentation, un certain nombre d'indicateurs, définis après échange avec les services utilisateurs, tant sur le plan statistique (« fausses alertes », nombre d'interventions réalisées à la suite de signalements…) que qualitatif (perception par le public, qualité de l'information sur l'expérimentation, conformité au Règlement général de protection des données…).

Démarche générale du comité

Pour procéder à l'évaluation demandée, le comité a fait le choix d'une démarche collective, s'appuyant sur la diversité des expériences des personnalités qui en sont membres, autour du rapporteur général et du président.

Il a ensuite été demandé aux utilisateurs de présenter leurs retours sur chacune de ces rubriques, en fournissant les données chiffrées recueillies lors des tests ainsi que des commentaires généraux sur les différents thèmes abordés.

Au vu de leur propre expérience et des observations faites lors des déplacements, les personnalités qualifiées ont également exprimé leur analyse sur l'ensemble des questions posées.

Cette méthode de travail a permis à chaque membre d'exprimer son propre point de vue, tant sur la performance technique et l'intérêt opérationnel du dispositif, que sur le respect des libertés fondamentales et sur la perception de l'impact des traitements algorithmiques par le public.

Observations générales sur le déroulement de l'évaluation

Une évaluation réalisée sur une période relativement brève

Eu égard à la date de sa constitution, le comité d'évaluation n'a pu commencer ses travaux qu'à une période à laquelle plusieurs phases administratives de l'expérimentation avaient déjà eu lieu. En particulier, les conditions de déroulement de la procédure de passation des marchés et les prescriptions techniques avaient été définies et les prestataires avaient été désignés.

Par ailleurs, eu égard à la date de remise prévue par la loi, le présent rapport ne peut porter sur les derniers tests programmés avant la fin de l'expérimentation, fixée, comme il a été rappelé, par le législateur au 31 mars 2025.

L'évaluation s'est ainsi déroulée dans un temps relativement court, de neuf mois environ, qui correspond à celui du calibrage et de la montée en puissance du dispositif, à l'occasion des Jeux et de quelques évènements ultérieurs.

Une évaluation principalement centrée sur le dispositif de la société Wintics

L'évaluation a essentiellement porté sur le traitement algorithmique développé par la société Wintics. En effet, eu égard aux règles retenues pour l'attribution des différents lots du marché national (cf. *infra, 1.2.2.*), Wintics a été, en pratique, le seul prestataire testé par la préfecture de police, la SNCF et la RATP.

Les termes du marché prévoyaient en effet pour chacun des lots que c'est uniquement dans l'hypothèse où l'attributaire de rang 1 du lot concerné aurait décliné certaines interventions qu'il aurait pu être fait appel à un autre prestataire présélectionné. Or, cela ne s'est pas produit. La majorité des déploiements ayant eu lieu en Ile-de-France (lot 1) et dans les transports parisiens (lot 4) et Wintics étant attributaire de rang 1 sur ces deux lots, c'est donc sa solution qui a été majoritairement testée.

Le dispositif concurrent, mis en place par la société Videtics, n'a ainsi pu être évalué que par la commune de Cannes, la seule collectivité qui a choisi de mettre en œuvre l'expérimentation. Une membre du collège des personnalités indépendantes du comité s'est ainsi déplacée sur le site en deux occasions, et a échangé à cette occasion avec les différents acteurs de l'expérimentation (police municipale, agents administratifs, prestataire…).

Des conditions d'accueil globalement satisfaisantes

Le comité a positivement apprécié, à l'occasion de ses différentes visites, l'accueil et la disponibilité des responsables des opérateurs concernés, et ce tout particulièrement lors des épreuves olympiques et paralympiques, pendant lesquelles ils étaient très sollicités.

De façon ponctuelle, des difficultés ont cependant pu être rencontrées, en particulier, au début des Jeux olympiques, avec la préfecture de police[17]. Ces difficultés ont été largement levées au cours des phases suivantes de l'expérimentation (cf. *infra*).

Contexte général de l'expérimentation

Un calendrier particulièrement serré

Le calendrier a également été particulièrement serré pour le déroulement de l'expérimentation.

Les deux décrets relatifs à la mise en œuvre[18] et à l'évaluation[19] de l'expérimentation n'étant intervenus que les 28 août et 11 octobre 2023, l'administration n'a disposé que de quelques mois pour définir les conditions de l'appel à candidatures ainsi que les prescriptions techniques. C'est ce qui explique le choix, dicté par des contraintes de calendrier, de passer un marché

[17] En particulier, le comité d'évaluation n'a pas été informé en temps utile de quelques-uns des sites sur lesquels l'expérimentation a porté pendant la période olympique (en particulier le Château de Versailles et le parc de la Courneuve).
[18] Décret n° 2023-828 du 28 août 2023 relatif aux modalités de mise en œuvre des traitements algorithmiques sur les images collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs, publié au JORF du 30 août 2023.
[19] Décret n° 2023-939 précité.

national, commun à l'ensemble des opérateurs habilités à mettre en œuvre le dispositif, plutôt que de laisser chacun choisir ses propres prestataires.

De même, ce calendrier contraint n'a laissé en pratique que quatre mois environ aux opérateurs pour effectuer de premiers tests destinés à calibrer le dispositif avant le début des épreuves olympiques. C'est ce qui explique en partie que pendant les Jeux olympiques, la préfecture de police ait fait le choix d'un déploiement assez limité du traitement, par manque de moyens et d'expérience pour en assurer une mise en œuvre plus étendue.

La durée des différents tests était, en outre, contrainte par la nécessité, posée par la loi, de ne mettre en œuvre les traitements qu'aux fins d'assurer la sécurité des manifestations sportives, récréatives ou culturelles justifiant qu'il y soit recouru, ce qui ne permettait pas des ajustements en amont. Cela a également participé à des difficultés opérationnelles rencontrées sur certains terrains, notamment au cours des premiers tests.

Un intérêt paradoxalement plus limité pendant la période olympique

- Il ressort de l'ensemble des observations et témoignages recueillis que l'intérêt opérationnel du dispositif d'intelligence artificielle s'est avéré moindre pendant les épreuves olympiques qu'il ne l'a été dans le cadre des évènements sportifs, récréatifs et culturels organisés au quotidien. En effet, les utilisateurs qui voulaient justement réduire les risques au maximum ont misé d'abord sur la densité des effectifs sur le terrain plutôt que sur une expérimentation qui, en tant que telle, comprenait une part d'incertitude. Et ce alors que le législateur avait précisément motivé la mise en place de l'expérimentation par les enjeux particuliers de sécurité pendant le déroulement des épreuves olympiques.

Ce paradoxe apparent s'explique par la présence humaine exceptionnelle (police nationale et gendarmerie nationale, y compris des représentants de l'ordre venant de l'étranger comme pendant tous les JO, militaires, personnels de la RATP et de la SNCF, police municipale, sécurité privée, bénévoles, etc.) pendant les Jeux. Celle-ci a rendu moins prioritaire la mise en place d'un dispositif destiné à détecter automatiquement les évènements indésirables. Et ce d'autant que, mis à part le site de Vaires-sur-Marne, les lieux où il a été déployé étaient d'une dimension relativement réduite[20].

- Certains sites ont, en revanche, été le siège d'expérimentations renouvelées dans le temps, non circonscrites aux seules épreuves olympiques. Tel fut notamment le cas du Stade de France et de la commune de Cannes. Les autorités responsables et, plus largement, les équipes opérationnelles et les sociétés prestataires, ont alors pu adapter le dispositif en procédant à des évolutions organisationnelles, opérationnelles et techniques, ainsi que l'ont observé, au cours de leurs différents déplacements, les membres du comité d'évaluation.

[20] En revanche, le déploiement pendant les Jeux olympiques et paralympiques a permis une exploitation en contenu du dispositif sur un même site pendant plusieurs semaines, ce qui n'était pas envisageable, au regard de l'objet de l'expérimentation, à l'occasion d'évènements plus ponctuels (concert, match de football…).

1ère partie - Organisation et caractéristiques du dispositif de vidéoprotection intégrant l'intelligence artificielle

1.1. Historique et contexte de l'expérimentation

1.1.1. L'origine de l'expérimentation

a) Des initiatives nombreuses avant la loi du 19 mai 2023

▪ Comme il a été dit à titre introductif, le recours à l'intelligence artificielle pour améliorer l'efficacité des dispositifs de vidéoprotection était en réalité effectif avant même l'entrée en vigueur de la loi du 19 mai 2023, généralement en vue d'une détection en temps différé.

L'utilisation de logiciels d'analyse de flux vidéo est ainsi autorisée, en temps différé, dans un cadre de police judiciaire. Elle est encadrée par l'article 230-20 du code de procédure pénale, qui permet, selon des finalités qu'il précise, le recours par la police et la gendarmerie, sous l'autorité du juge, à des logiciels de rapprochement judiciaire (LRJ).

Par délibération du 5 décembre 2024, la CNIL a adressé une mise en demeure au ministère de l'intérieur et à six communes de mettre fin à des manquements constatés à la suite de l'utilisation du logiciel de rapprochement judiciaire Briefcam, à la suite d'une procédure engagée en novembre 2023.
En ce qui concerne le ministère de l'intérieur, la CNIL relève certes que la fonctionnalité de reconnaissance faciale n'était pas utilisée par les services de police mais relève avoir été informée d'un cas ponctuel de recours dans le cadre d'une enquête judiciaire[21]. Il convient de préciser que cette utilisation s'est faite dans le cadre des logiciels de rapprochement judiciaire, et pas dans le cadre de l'expérimentation IA instaurée par la loi du 19 mai 2023.
Si l'utilisation des logiciels d'analyse vidéo en différé est considérée comme licite, la CNIL a constaté que les services du ministère de l'Intérieur n'ont analysé ces dispositifs comme relevant du cadre juridique des LRJ que depuis 2023. En conséquence, les engagements de conformité au « référentiel LRJ » n'ont été transmis que tardivement à la CNIL, parfois plusieurs années après le début de leur mise en œuvre, ou ne l'ont pas encore été.

Cet emploi des traitements algorithmiques doit être distingué de l'utilisation, qui est également susceptible d'en être faite, en temps réel, à des fins de police administrative. Cette utilisation n'est désormais possible que dans le cadre de la présente expérimentation, ce qui exclut notamment le recours à la reconnaissance faciale[22].

Or, de nombreux dispositifs avaient été acquis, dès avant mai 2023, dans le cadre de projets de « safe city », lancés par des communes, comme Nice, Marseille, Saint-Etienne ou Valenciennes[23].

▪ En ce qui concerne les transports publics, la SNCF et la RATP avaient, elles aussi, lancé des programmes destinés à développer le recours aux caméras avec IA, à des fins de sécurisation

[21] La délibération souligne en outre le retard du ministère dans la transmission des engagements de conformité et de l'AIPD.
[22] Par ailleurs, dans le cadre juridique différent des logiciels de rapprochement judiciaire, la préfecture de police participe à l'expérimentation du logiciel d'analyse vidéo « System V », effectuée par l'Agence du numérique de la sécurité intérieure et la direction de la police judiciaire de la préfecture.
Elle dispose par ailleurs d'un dispositif technique d'exploitation des vidéos enregistrées du plan de vidéoprotection pour Paris (PVPP) dans le cadre du droit d'accès aux images, afin de pouvoir retrouver ex-post, dans le cadre du délai légal de conservation, les images concernant le demandeur. Mais ce dispositif est mis en œuvre par des opérateurs humains, sans recours à des dispositifs d'IA.
[23] V. par ex. Convention d expérimentation Safe City ville de Nice.pdf

des infrastructures, et en particulier pour faciliter la détection des objets abandonnés. Ils ont mis en place, à cet effet, des équipes dédiées[24].

Ces initiatives avaient, alors, été mises en place en lien avec la CNIL. Ainsi, par exemple, en 2019, la commission avait émis un avis favorable pour permettre à la SNCF de conduire une expérimentation d'outils de suivi de personnes non biométriques[25].

De même, la SNCF et la RATP avaient pris part au programme européen « *Prevent* ». D'une durée de 36 mois (septembre 2021 – août 2024), ce programme avait pour finalité de développer des technologies capables de détecter des objets délaissés, d'associer ces objets à leur propriétaire par le biais de recherches par similarité[26] sans, en aucun cas, recourir à des données biométriques, et enfin de localiser ce dernier. Regroupant huit pays et 21 partenaires européens (dont 10 acheteurs publics), il porte sur un budget global de 13,3 millions d'euros, financé à 90 % par la Commission européenne. Deux consortiums d'industriels européens ont déployé des prototypes dans le cadre de ce programme[27].

- Enfin, des dispositifs spécifiques, recourant notamment à la reconnaissance thermique ou destinés à faire respecter l'obligation de port du masque, ont été mis en place par décret pendant la crise sanitaire[28].

b) Des dispositifs dont la légalité était interrogée au niveau national

La légalité des dispositifs de traitements algorithmiques en matière de vidéoprotection a cependant été interrogée par différentes prises de position des sections administratives du Conseil d'Etat et de la CNIL faisant apparaître que seule une loi pourrait valablement autoriser le recours à de telles technologies.

- Le Conseil d'Etat avait déjà évoqué ces enjeux dans son étude annuelle de 2014 consacrée au numérique et aux droits fondamentaux[29]. Dans son rapport remis le 31 mars 2022 au Premier ministre sur l'intelligence artificielle, il relève que « *Les systèmes d'IA les plus intrusifs ou coercitifs (dont l'analyse automatisée d'images captées dans l'espace public) pourront nécessiter un assentiment exprès du législateur et la fixation de garanties spécifiques* »[30].

Des positions en ce sens avaient été émises dans le cadre de certains dispositifs spécifiques :
- Avis sur le projet de loi renforçant la lutte contre le crime organisé et son financement, l'efficacité et les garanties de la procédure pénale[31] ;

[24] Exemple du lab IA à la RATP.
[25] Délibération CNIL n°2019-037.
[26] Sans recourir en aucun cas à des données biométriques, la recherche par similarité consiste à identifier une personne à l'aide de données telles que la couleur de ses vêtements, sa forme générale, etc.
[27] A l'origine, 6 consortiums étaient en concurrence.
[28] cf. Délibération CNIL n° 2020-083 du 23 juillet 2020.
[29] https://www.vie-publique.fr/files/rapport/pdf/144000541.pdf (v. en particulier, p. 118 : « *La police utilise déjà des traitements de données, dénommés « traitements d'analyse sérielle », pour recouper les informations dont elle dispose sur les différentes affaires (…). Il est cependant possible d'aller aujourd'hui bien plus loin [par] l'exploitation systématique des données (…) produites par les caméras de vidéosurveillance* ».
[30] « Intelligence artificielle et action publique : construire la confiance, servir la performance », p. 137
[31] « *Le but de ce dispositif est de prévenir les incidents susceptibles de se produire lors de ces interventions et d'aider à la répression des infractions recherchées lors de l'intervention ou incidentes, comme des fautes professionnelles, par la collecte de preuves qui pourront être utilisées dans le cadre de procédures pénales, administratives ou disciplinaires. Le dispositif se rattacherait par conséquent tant à la police administrative que,*

- Avis rendu au Gouvernement relatif à l'usage de dispositifs aéroportés de captation d'images par les autorités publiques[32] ;
- Avis rendu le 12 octobre 2021, non publié[33].

▪ Dans un avis remis en juillet 2022[34], la CNIL a pris position dans le même sens, en estimant que les dispositifs de caméras « augmentées » mis en œuvre à des fins de police administrative générale ou de police judiciaire étaient susceptibles d'affecter les garanties fondamentales apportées aux citoyens pour l'exercice des libertés publiques et qu'ils relevaient, en conséquence, des domaines constitutionnellement réservés à la loi.

Cet avis relève que : « *Même en étant temporaires et limités à la protection de certains évènements ou à des finalités de prévention de troubles graves à l'ordre public, ces traitements sont susceptibles de modifier la façon dont l'action des services de police influe sur l'exercice par les citoyens de leurs libertés et droits fondamentaux, et ne peuvent trouver un fondement juridique suffisant dans les dispositions générales de la loi CNIL ou dans le pouvoir réglementaire du gouvernement ou, a fortiori, des maires. Les traitements algorithmiques de détection de comportements « suspects » ou infractionnels emportent un changement de degré et de nature dans la surveillance à distance de la voie publique que le législateur a souhaité encadrer il y a plusieurs années au sein du CSI pour les caméras de vidéoprotection « classiques ». Les nouveaux dispositifs engendrent des risques accrus pour les personnes dépassant la seule problématique de la protection de leurs données, en touchant à la fois à la sphère pénale (logique répressive) et aux conditions d'exercice de leurs libertés fondamentales* ».

La nécessité de tels dispositifs doit « *être évaluée à un niveau plus général que les seules collectivités publiques décidant de leur mise en place : l'éventuel déploiement de tels dispositifs intrusifs ne doit pas résulter d'une addition d'initiatives locales, nécessairement sans cohérence. Seule une loi spécifique, adaptée aux caractéristiques techniques et aux enjeux en cause, pourrait éventuellement, à l'issue d'un débat démocratique, décider de leur légitimité et, par la fixation de garanties minimales, prévoir une conciliation équilibrée entre l'objectif de sauvegarde de l'ordre public et l'impératif de protection des droits et libertés fondamentaux* ».

c) Des dispositifs sources d'inquiétudes et de polémiques

▪ La mise en œuvre de dispositifs de traitements algorithmiques par certaines administrations avait, en outre, suscité des inquiétudes et des polémiques, relayées par des associations ayant pour objet la protection des libertés individuelles. En particulier, certains de ces dispositifs semblaient comporter des fonctionnalités permettant la reconnaissance faciale.

---

le cas échéant, à la police judiciaire et aux procédures disciplinaires. Au regard des données collectées, de leur mode de collecte et des objectifs en vue desquels elles sont captées, le dispositif envisagé ne se confond pas avec celui de la vidéoprotection (titre V du livre II du code de la sécurité intérieure) et constitue un instrument nouveau ».

[32] Conseil d'État, section de l'intérieur, 20 septembre 2020, n° 401214.

[33] Avis n° 404206 et 404020 cités par le rapport d'information n° 627 (2021-2022) de MM. Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain, fait au nom de la commission des lois, sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles.

[34] « *Caméras dites « intelligentes » ou « augmentées » dans l'espace public – position sur les conditions de déploiement* ».

Des recours avaient été portés devant le juge administratif, qui les avait, pour la plupart, rejetés, mais sans prendre parti sur la légalité de tels dispositifs.

Ainsi, le juge des référés du Conseil d'Etat a rejeté, le 21 décembre 2023, un recours en référé liberté ayant pour objet d'enjoindre à une communauté de communes de cesser l'utilisation d'un de ces logiciels, mais uniquement au motif que la condition d'urgence particulière n'était pas satisfaite, la fonctionnalité reconnaissance faciale n'ayant, notamment, pas été activée[35].

Le tribunal administratif de Marseille a, par ailleurs, rejeté, le 2 juin 2023, un recours tendant à ce qu'il soit mis fin à l'exécution d'un marché entre la commune de Marseille et un prestataire privé portant sur l'acquisition d'un dispositif de « vidéoprotection intelligente ». Au vu de l'état peu avancé de l'exécution du marché, et « *à supposer même que le traitement de données prévu par le dispositif acquis par la commune de Marseille soit inadéquat, non pertinent et manifestement excessif au regard des finalités poursuivies* », « *il ne [résultait] pas de l'instruction que la poursuite de l'exécution du contrat à la date du présent jugement [aurait été] manifestement contraire à l'intérêt général* »[36].

Ce jugement a été annulé, le 14 octobre 2024, par la cour administrative d'appel de Marseille, mais sans prise de position, là encore, sur le fond du litige, mais uniquement au motif qu'à la date du jugement, le marché en litige devait être regardé comme ayant été exécuté[37].

- D'autres inquiétudes portent sur la réalité de l'autonomie des agents humains face aux alertes produites par les traitements algorithmiques. Ainsi, dans un avis de juin 2024[38], la CNCDH évoque « *la propension de chacun à suivre les recommandations ou alertes produites par un programme informatique (parfois appelé « biais d'automatisation »). (...) L'agent humain se trouvera ainsi davantage en position d'exécutant que de contrôleur vis-à-vis de la machine* ».

La commission recommande en conséquence aux pouvoirs publics « *de mener une réflexion sur les moyens de garantir effectivement l'autonomie de l'agent face aux alertes de la machine* ». Le comité d'évaluation accord une grande importance à ce principe de « l'autonomie de l'humain » (cf. ci-dessous).

1.1.2. Un dispositif à replacer dans le contexte international

Au-delà des frontières, nombre d'Etats occidentaux recourent déjà à l'intelligence artificielle à des fins de vidéoprotection. Le plus souvent, comme en Allemagne, ces dispositifs, incluant la reconnaissance faciale, sont utilisés dans le cadre d'enquêtes judiciaires.

Cependant, le recours à de tels traitements à des fins de police administrative est utilisé régulièrement ou expérimenté dans certains Etats, notamment par des polices municipales ou dans les transports publics. C'est, par exemple, le cas au Royaume-Uni, où l'usage de l'intelligence artificielle aux fins d'équiper le dispositif de protection vidéo en temps réel a été réalisé dans le métro de Londres entre octobre 2022 et septembre 2023. D'autres

[35] JRCE, 21 décembre 2023, Communauté de communes Cœur Côte fleurie, n° 489990.
[36] Association La Quadrature du Net, n° 2009485.
[37] CAA Marseille, 14 octobre 2024, n° 23MA02036.
[38] « Surveillance de l'espace public ».
https://www.cncdh.fr/actualite/surveillance-de-lespace-public-la-cncdh-formule-des-recommandations

expérimentations analogues sont encore en cours dans les transports publics londoniens[39]. De même, en Allemagne ou en Espagne, des systèmes de vidéoprotection équipent certaines polices municipales. Les Pays-Bas se sont, quant à eux, dotés en 2023 d'un cadre législatif provisoire permettant le déploiement de ces dispositifs.

Il sera renvoyé sur ce point à la contribution du ministère de l'intérieur et à celle de Mme Lequesne, membre du comité (annexe n° 4), ainsi qu'aux nombreux articles parus ces dernières années sur le sujet dans des revues spécialisées[40].

1.1.3. Le contexte et la préparation de la présente expérimentation

Par leur ampleur et leur durée, les Jeux olympiques et paralympiques constituaient pour l'Etat et pour leurs organisateurs un défi logistique et sécuritaire incomparable. Ils étaient annoncés comme l'organisation simultanée de 42 championnats du monde sportifs dans une cinquantaine de sites, rassemblant plus de 13 millions de spectateurs et 4 milliards de téléspectateurs, ainsi que l'équivalent d'un G20, d'une Assemblée Générale de l'ONU et d'un forum de Davos, en raison de la présence de nombreux chefs d'Etat et de gouvernement. L'ambition d'une cérémonie d'ouverture sur la Seine ainsi que la concentration d'un grand nombre de compétitions dans une zone de 10 km² dans le centre de Paris ajoutaient des contraintes sécuritaires ainsi qu'en matière de gestion de flux à un système déjà fortement en tension.

En complément de la mobilisation massive des policiers et des gendarmes, appuyée par les forces armées et du renforcement de la structuration de la filière de la sécurité privée afin de pourvoir aux besoins inédits et quotidiens évalués à 22 000 agents de sécurité privée, la stratégie interministérielle de sécurité s'est ainsi interrogée, dès les premières années de la préparation, sur le possible déploiement, dans un cadre juridique spécifique, de technologies de sécurité visant à rationaliser les besoins de déploiement de forces de sécurité intérieure et à faciliter l'accomplissement de leurs missions, sans s'y substituer[41].

L'objectif était de disposer d'un dispositif juridique encadrant le développement d'un modèle d'IA française performante et éthique, qui soit motivant pour la filière industrielle française et qui apporte des outils opérationnels, considérés comme nécessaires par les forces de sécurité intérieure en prévision des grands événements sportifs internationaux de 2023 et 2024[42].

---

[39] Pour un regard critique sur le recours à l'IA en matière de vidéoprotection à Londres, il sera renvoyé à ce très récent article, paru dans le journal Le Monde, le 12 janvier 2025 : Londres sous le diktat de la reconnaissance faciale. Il y est souligné que la reconnaissance faciale, qui « *fiche les individus dits « indésirables » gagne commerces ou boîtes de nuit de la capitale britannique* ».
V. également : Reconnaissance faciale : nouvelles polémiques après l'échec cuisant de la police de Londres | TV5MONDE - Informations

[40] New Surveillance Technologies in Public Spaces Challenges and Perspectives for European Law at the Example of Facial Recognition », Report for The Urban Agenda, European Commission, 2021, 96 p.

[41] De plus, la mesure n° 105 du programme d'héritage de l'Etat pour ces jeux, établi sous la responsabilité de la Délégation interministérielle aux Jeux Olympiques et Paralympiques (DIJOP), visait à « *mettre en œuvre, pour les JOP, des technologies liées à la sécurité et à la mobilité en vue de déployer des solutions de sécurité lors de la coupe du monde de rugby 2023, des JOP 2024 et pour les prochains GESI en France ou à l'étranger* ».

[42] Dans la continuité du contrat de la filière des industries de sécurité signé en 2020 par l'Etat avec les industriels du comité stratégique de filière, qui prévoyait de solliciter un budget « sécurité des JOP 2024 et des grands évènements sportifs internationaux » piloté par le ministère de l'intérieur, des échanges ont eu lieu entre la fin de l'année 2020 et l'été 2021 entre la DIJOP, le secrétariat général de la défense et de la sécurité nationale (SGDSN), les services du ministère de l'intérieur (notamment la coordination nationale pour la sécurité des Jeux et la délégation ministérielle aux partenariats, aux stratégies et aux innovations de sécurité, à laquelle a succédé la

Il avait été envisagé, dans un premier temps, de préparer une disposition législative spécifique et excluant tout recours à la reconnaissance faciale[43]. Une disposition en ce sens avait été élaborée en vue du vote de la loi « responsabilité pénale et sécurité intérieure ».

Les problèmes de sécurité rencontrés à l'occasion de la finale de football de la Ligue des Champions le 28 mai 2022 ont conduit le Délégué interministériel aux grands événements sportifs, dans son rapport d'analyse des incidents remis à la Première ministre le 10 juin[44], et les commissions des lois et de la culture, de l'éducation et de la communication du Sénat, dans leur compte-rendu d'enquête[45], à recommander le recours à un cadre juridique adapté rendu encore plus nécessaire en prévision des Jeux olympiques et paralympiques.

Ce sont l'ensemble de ces réflexions qui ont finalement conduit à la rédaction de l'article 10 de la loi du 19 mai 2023.

1.2. Une expérimentation étroitement encadrée par le droit

1.2.1. Un cadre juridique très précis

a) Un cadre progressivement resserré à chaque stade de l'élaboration du dispositif

Le cadre juridique dans lequel s'inscrit la présente expérimentation a progressivement été resserré à chaque stade de son élaboration : au Conseil d'Etat, puis au Parlement, par le Conseil constitutionnel, puis au stade de l'élaboration des décrets. Les conditions dans lesquelles il peut être recouru à l'intelligence artificielle ont encore été restreintes lors de la définition des clauses techniques du marché.

Cet encadrement très fort s'explique par les enjeux pour les libertés publiques de tels dispositifs d'apparition récente.

Dans son avis sur le projet de loi, la CNIL a ainsi relevé que : « *Le recours à ces dispositifs soulève des enjeux nouveaux et substantiels en matière de vie privée en ce qu'ils peuvent conduire à une collecte massive de données personnelles et permettre une surveillance automatisée en temps réel. Le déploiement, même expérimental, de ces dispositifs constitue un*

---

direction des entreprises et des partenariats de sécurité et des armes) et avec la présidente de la CNIL afin de disposer de technologies françaises, utiles aux Jeux et respectueuses des libertés individuelles. Les échanges se sont poursuivis dans le cadre de la mission menée par le député Jean-Michel Mis qui, dans son rapport du 13 septembre 2021 « Pour un usage responsable et acceptable par la société des technologies de sécurité » avait repris la proposition des services compétents dans sa recommandation n°5.

[43] La section de l'intérieur du Conseil d'Etat avait rendu le 12 octobre 2021 un avis sur cet usage de traitements algorithmiques en matière de vidéoprotection. Le Conseil d'Etat avait assorti son avis de recommandations pour encadrer strictement cette mesure, en considérant qu'il était saisi pour la première fois d'une demande portant sur un traitement recourant à l'intelligence artificielle, destinée à assurer une interprétation d'images.

[44] Recommandation 3.3 : Disposer du cadre juridique permettant le recours à des algorithmes (Intelligence Artificielle) appliqués à certains flux vidéo issus des caméras installées sur les emprises des sites de compétition et de célébration et à leurs abords dans l'espace public. Ces algorithmes auraient vocation à assurer le comptage et le suivi des flux, ainsi que la détection de situations anormales, de regroupements ou de mouvements de foule dans un cadre éthique et transparent

[45] Recommandation n° 11 (ministère de l'intérieur, Parlement) : établir, à titre expérimental, la base législative qui permettrait aux opérateurs des systèmes de vidéoprotection dans les espaces accessibles au public de mettre en œuvre des traitements d'images par intelligence artificielle permettant le comptage et la détection de mouvements de foule.

tournant qui va contribuer à définir le rôle général qui sera attribué à ces technologies, et plus généralement à l'intelligence artificielle ».

De même, dans son avis sur le projet de loi, le Conseil d'Etat a souligné que ce « *dispositif inédit »* était *« porteur d'enjeux nouveaux pour les droits et libertés* ». « *Cette expérimentation, limitée dans le temps et dans l'espace, telle qu'elle est régie et encadrée par le projet de loi ainsi précisé, ne se heurte à aucune objection d'ordre constitutionnel ou conventionnel et est susceptible d'assurer une plus grande efficacité du maintien de l'ordre et de la sécurité des manifestations d'ampleur inédites qui vont se dérouler, notamment pendant la période des jeux Olympiques et Paralympiques* ».

Enfin, le Conseil constitutionnel, se prononçant sur l'article 10 de la loi du 19 mai 2023, a rappelé qu'il appartenait au législateur de fixer les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques et qu'il lui incombait également d'assurer la conciliation entre l'objectif de valeur constitutionnelle de prévention des atteintes à l'ordre public et le droit au respect de la vie privée protégé par l'article 2 de la Déclaration de 1789.

Il a considéré que les dispositions contestées ne méconnaissaient pas le droit au respect de la vie privée compte tenu des différentes garanties mises en place :
- La poursuite par le législateur de l'objectif de valeur constitutionnelle de prévention des atteintes à l'ordre public ;
- La restriction tenant aux évènements concernés par l'expérimentation ;
- L'encadrement administratif et la possibilité de recours au juge ;
- Les limites tenant à la durée de l'autorisation. Il a, sur ce point, posé la réserve d'interprétation quant aux pouvoirs du préfet de mettre fin à la mesure (cf. *infra*)[46] ;
- L'information du public ;
- L'utilisation du traitement pour des seuls cas d'usage prédéterminés par décret ;
- L'absence de mise en œuvre de techniques de reconnaissance faciale ou de systèmes d'identification biométrique ;
- L'exigence selon laquelle les traitements ne peuvent fonder par eux-mêmes aucune décision individuelle ni aucun acte de poursuite et demeurent en permanence sous le contrôle des personnes chargées de leur mise en œuvre et la circonstance qu'ils demeurent en permanence sous le contrôle et la maîtrise de personnes humaines.

b) Finalités, objet et durée de l'expérimentation

▪ L'encadrement juridique renforcé se traduit d'abord par le caractère très précis de la finalité de l'expérimentation.

En vertu du I de l'article 10 de la loi, les traitements doivent avoir « *pour unique objet d'assurer la sécurité de manifestations sportives, récréatives ou culturelles qui, par l'ampleur de leur fréquentation ou par leurs circonstances, sont particulièrement exposées à des risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes, dans les lieux accueillant ces manifestations et à leurs abords ainsi que dans les véhicules et les emprises de transport public et sur les voies les desservant* ».

[46] « *si les dispositions contestées prévoient que le préfet ayant autorisé la mesure « peut suspendre l'autorisation ou y mettre fin à tout moment s'il constate que les conditions ayant justifié sa délivrance ne sont plus réunies », elles ne sauraient, sans méconnaître le droit au respect de la vie privée, être interprétées autrement que comme obligeant le préfet à mettre fin immédiatement à une autorisation dont les conditions ayant justifié la délivrance ne sont plus réunies* ».

Le législateur a ainsi notamment entendu fonder le dispositif sur des finalités de sécurité physique des personnes. Ce qui permet néanmoins, dans le respect de ces finalités, de façon incidente, la prise de mesures répressives (retrouver des délinquants ou des contrevenants) ou d'exploitation (par ex. faciliter la fluidité de la circulation des usagers).

La référence à une finalité portant sur la « sécurité des personnes » mérite d'être précisée.

L'expression « dispositif de sécurité » désigne communément les moyens (humains, techniques et organisationnels) de prévention et d'intervention contre les actes de malveillance. La sûreté renvoie, quant à elle, à l'ensemble des moyens de prévention et d'intervention contre les risques à caractère accidentel.

Ces acceptions sont cependant inversées dans le domaine des transports[47]. La sûreté renvoie ainsi à l'ensemble des mesures mises en œuvre pour lutter contre les actes de malveillance alors que la sécurité se réfère à la prévention des accidents[48].

- Les traitements ne peuvent avoir pour objet que de « *détecter, en temps réel, des événements prédéterminés susceptibles de présenter ou de révéler de tels risques et de les signaler en vue de la mise en œuvre des mesures nécessaires* » par les forces de sécurité intérieure, les services d'incendie et de secours, les services de police municipale et les services internes de sécurité de la SNCF et de la RATP dans le cadre de leurs missions respectives.

Ces « évènements prédéterminés » ont été définis à l'article 3 du décret du 28 août 2023 :

- présence d'objets abandonnés ;
- présence ou utilisation d'armes ;
- non-respect par une personne ou un véhicule, du sens de circulation commun ;
- franchissement ou présence d'une personne ou d'un véhicule dans une zone interdite ou sensible ;
- présence d'une personne au sol à la suite d'une chute ;
- mouvement de foule ;
- densité trop importante de personnes ;
- départs de feux.

Le choix de ces cas d'usage interdit le recours à certaines fonctionnalités. Il n'est, par exemple, pas question de pouvoir retrouver le propriétaire d'un objet abandonné, mais seulement de détecter la présence de cet objet.

Ces cas d'usage ont été établis sur la base de l'analyse nationale des risques établie par le centre de renseignement olympique avec le concours de 25 acteurs publics et privés (services spécialisés de l'Etat, opérateurs d'importance vitale, opérateurs de transport et organisateur Paris 2024).

[47] Il sera renvoyé aux intitulés des chapitres 1 et 2 du titre 3 du livre 6 de la première partie du code des transports : chapitre 1 : « organisation de la prévention des atteintes à la sûreté dans les transports » ; chapitre 2 : « dispositif technique de prévention des atteintes à la sûreté des transports ».
C'est dans ce chapitre 2 que sont placées la vidéoprotection dans les transports et les équipes cynotechniques (Respectivement, section 1 et section 2).
[48] cf. pour la sécurité des travaux et des systèmes, articles L. 1613-1 et suivants.

Cette analyse[49] était destinée à établir une cartographie des risques permettant de couvrir l'ensemble des champs concernés susceptibles d'avoir un impact sur la préparation et le déroulement des JOP[50], en les identifiant, en les hiérarchisant selon leur criticité, résultant de leur vraisemblance et de leurs conséquences, et en établissant pour chaque risque des contre-mesures opérationnelles, budgétaires et réglementaires. Elle a fait émerger, parmi les risques les plus critiques pour l'organisation, les attaques terroristes par des individus isolés au moyen d'armes à feu, la présence d'objets abandonnés susceptibles d'être qualifiés en objets suspects nécessitant l'intervention des services de déminage au détriment de l'écoulement des flux de spectateurs, les intrusions frauduleuses sur les sites ou dans des zones réservées accueillant les événements, ainsi que les phénomènes de densité de foule susceptible de générer des mouvements de foule en cas d'incident[51].

▪ Enfin, la durée de l'expérimentation est limitée à quinze mois. Le Parlement n'a pas suivi, sur ce point, l'avis du Conseil d'Etat qui soulignait l'opportunité d'une durée plus longue, portée à 18 mois.

c) Garanties générales pour le respect des libertés publiques

Le législateur et le pouvoir réglementaire ont également institué différentes conditions de fond et de procédure afin de veiller à ce que l'expérimentation se déroule dans un cadre respectueux des libertés publiques.

▪ Ainsi, l'article 10 de la loi :

- Requiert qu'il ne soit fait du traitement qu'un usage « en temps réel » (I), ce qui interdit tout recours à des fins de recherche des auteurs d'un acte délictuel ou contraventionnel ;

- Rappelle l'applicabilité du règlement[52] 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 - (II) ;

- Impose l'information préalable du public sur l'usage du traitement, sauf lorsque les circonstances l'interdisent ou que cette information entrerait en contradiction avec les objectifs poursuivis et prévoit, par ailleurs, l'organisation d'une information générale par le ministre de l'intérieur (III) ;

- Interdit le recours à la biométrie ou à la reconnaissance faciale ainsi que le rapprochement ou d'interconnexion avec d'autres traitements de données à caractère personnel (IV) ;

- Pose, conformément à l'avis du Conseil d'Etat, un « *principe de primauté humaine, assurant qu'à tout instant le traitement ne fonctionne que sous la supervision des personnes qui le mettent en œuvre* ». Il prévoit ainsi que les traitements procèdent exclusivement à un signalement d'attention, strictement limité à l'indication du ou des événements prédéterminés

[49] Réalisée selon la méthode de management du risque reposant sur la norme ISO 31 000.
[50] Terrorisme, cybersécurité, atteintes aux personnes et au biens, atteintes au déroulement des JOP et aux chantiers des ouvrages olympiques, manipulation de l'information, risques naturels, sanitaires, industriels et accidentels.
[51] Ces développements ont été établis sur la base des éléments communiqués par la Délégation interministérielle aux Jeux olympiques et paralympiques.
[52] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.

qu'ils ont été programmés à détecter. Ils ne produisent aucun autre résultat et ne peuvent fonder, par eux-mêmes, aucune décision individuelle ni aucun acte de poursuite. Ils demeurent en permanence sous le contrôle des personnes chargées de leur mise en œuvre (IV).

NOTA : ce principe de primauté humaine a notamment été rappelé par le Conseil d'Etat, dans un autre domaine, en ce qui concerne les dispositifs de géolocalisation utilisés pour la verbalisation du stationnement payant – il appartient ainsi aux autorités saisies d'une contestation sur le lieu précis de stationnement du véhicule constaté sur la base d'un tel dispositif, de vérifier que les photographies prises lors du constat sont de nature à confirmer les mentions portées sur l'avis de paiement. En l'absence de photographies horodatées permettant d'identifier le véhicule dans son environnement ou si les photographies ne permettent pas de se prononcer sur la localisation du véhicule au moment du constat, il leur appartient de faire droit à tout recours assorti d'une argumentation suffisamment étayée[53].

- Le décret du 28 août 2023 introduit des garanties supplémentaires :

- Les données collectées doivent être conservées pendant une durée strictement nécessaire qui ne peut, dans tous les cas, excéder douze mois à compter de l'enregistrement des images et prend fin, dans tous les cas, à la fin de l'expérimentation. Elles ne peuvent, pendant cette durée, être utilisées à d'autres fins que celles prévues pour l'expérimentation (article 8) ;

- Les catégories d'agents autorisés aux signalements du traitement sont limitativement énumérées (article 15[54]) ;

- La délivrance des habilitations est subordonnée au suivi d'une formation (article 15[55]) ;

- Des journaux des opérations de consultation et de communication doivent être établis et conservés pendant 12 mois (article 16) ;

- Les droits d'accès, de rectification, d'effacement et à la limitation des données s'exercent directement auprès du responsable de traitement et les seules restrictions dont ils peuvent faire l'objet sont celles destinées à protéger la sécurité publique ou la sécurité nationale (III de l'article 17). En revanche, le droit d'opposition n'est pas applicable (IV de l'article 17, qui renvoie aux articles 110 de la loi CNIL et 23 du RGPD).

---

[53] CE, 5/6 CHR, 18 novembre 2024, Habans, n°472912, 472918, A.

[54] « 1° *Les agents de la police nationale individuellement désignés et spécialement habilités par le chef du service ;*
2° Les militaires de la gendarmerie nationale individuellement désignés et spécialement habilités par le commandant de l'unité de gendarmerie ;
3° Les personnels des SDIS individuellement désignés et spécialement habilités par le responsable du service ;
4° Les agents de police municipale individuellement désignés et spécialement habilités par le maire ou le responsable du service de police municipale ;
5° Les agents des services internes de sécurité de la SNCF et de la Régie autonome des transports parisiens individuellement désignés et spécialement habilités par les responsables de ces services.

[55] *Formation en matière de protection des données à caractère personnel et formation sur le fonctionnement opérationnel et technique du traitement et sa prise en main* ».

d) Caractéristiques techniques des traitements autorisés

Le VI de l'article 10 de la loi, qui reprend pour partie des préconisations définies par le Conseil d'Etat dans son avis[56], impose que le traitement respecte les exigences suivantes, qui doivent pouvoir être vérifiées à tout moment :

1° Lorsque le traitement repose sur un apprentissage, les données d'apprentissage, de validation et de test choisies doivent être pertinentes, adéquates et représentatives. Leur traitement doit être loyal et éthique, reposer sur des critères objectifs et permettre d'identifier et de prévenir l'occurrence de biais et d'erreurs. Ces données font l'objet de mesures de sécurisation appropriées ;

2° Le traitement comporte un enregistrement automatique des signalements des événements prédéterminés détectés permettant d'assurer la traçabilité de son fonctionnement ;

3° Le traitement permet des mesures de contrôle humain et un système de gestion des risques permettant de prévenir et de corriger la survenue de biais éventuels ou de mauvaises utilisations ;

4° Les modalités selon lesquelles, à tout instant, le traitement peut être interrompu sont précisées ;

5° Le traitement fait l'objet d'une phase de test conduite dans des conditions analogues à celles de son emploi autorisé par le décret, attestée par un rapport de validation ;

[6°] Lorsque le traitement est développé ou fourni par un tiers, celui-ci fournit une documentation technique complète et présente des garanties de compétence, de continuité, d'assistance et de contrôle humain en vue notamment de procéder à la correction d'erreurs ou de biais éventuels lors de sa mise en œuvre et de prévenir leur réitération. Il transmet également une déclaration, dont les modalités sont fixées par décret, des intérêts détenus à cette date et au cours des cinq dernières années.

e) Conditions de développement et de l'emploi des traitements

La procédure administrative permettant le développement et l'emploi des traitements est également très précisément définie. Elle est entourée de diverses garanties et extrêmement centralisée.

- Le décret qui autorise le recours au traitement est ainsi pris après avis de la CNIL et accompagné d'une analyse d'impact relative à la protection des données personnelles – ci-après AIPD (V de l'article 10 de la loi).

[56] « *définir les exigences auxquelles le développement du traitement doit répondre : attention particulière au choix des données d'apprentissage (adéquation, pertinence, loyauté, prévention des biais éventuels), enregistrement automatique des événements permettant d'assurer la traçabilité de son fonctionnement, mécanisme permettant son arrêt immédiat, phase de test et validation avant la mise en service, et, si un fournisseur externe est choisi, garanties de compétence et de continuité d'activité de celui-ci* ».

L'Etat peut soit assurer le développement du traitement, soit en confier le développement à un tiers soit l'acquérir (VI de l'article 10 de la loi[57]). Ni les collectivités territoriales, ni les autres opérateurs, telles la RATP ou la SNCF, ne disposent donc d'attribution en la matière dans le cadre de l'expérimentation.

Ainsi que l'a souligné le Conseil d'Etat dans son avis sur le projet de loi : « *compte tenu des enjeux que comporte cette première expérimentation du recours à l'intelligence artificielle pour l'assistance au maintien de l'ordre* », le choix a été fait de « *réserver l'initiative du développement de ces logiciels à l'Etat sans interdire de les mettre à disposition de services qui le demanderaient, moyennant le cas échéant rémunération* ».

Le traitement ainsi développé est ensuite mis à disposition des services utilisateurs (collectivités, SNCF, RATP), dans le cadre d'une convention avec l'Etat (article 12 du décret).

- Ces considérations se retrouvent en ce qui concerne le suivi de la mise en œuvre du dispositif. Ainsi, les phases de programmation et de calibrage du traitement doivent s'effectuer sous la supervision d'un agent du ministère de l'intérieur, qui est pour cette phase responsable du traitement (article 7 du décret[58])[59].

Une fois ces phases intervenues, l'emploi du traitement pour une manifestation sportive, récréative ou culturelle déterminée est soumis à l'autorisation préalable du préfet, qui s'assure de sa proportionnalité à la finalité poursuivie (VII de l'article 10 de la loi)[60].

Après la délivrance de l'autorisation, les services de la police et de gendarmerie, les services de police municipale et les services internes de sécurité de la SNCF et de la RATP ont la qualité de responsables des traitements, qu'ils sont ainsi chargés de mettre en œuvre (article 13 du décret).

Le responsable du traitement doit, au préalable, transmettre à la CNIL un engagement de conformité aux dispositions légales et procéder à l'actualisation de l'AIPD au vu des caractéristiques particulières des traitements (VII de l'article de la loi et article 14 du décret).

f) La remise en cause de la légalité des dispositifs de caméras avec IA mis en place avant l'édiction du nouveau cadre juridique

La loi du 19 mai 2023 et les textes pris pour son application ont ainsi eu pour effet de remettre en cause la légalité éventuelle des dispositifs développés avant cette date.

---

[57] Cet article précise que dans ces deux derniers cas, il veille à ce que prestataire soit prioritairement une entreprise qui répond aux règles de sécurité définies par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) s'agissant du respect des exigences relatives à la cybersécurité.

[58] « *Sont seuls autorisés à accéder au traitement pendant la phase de conception, à raison de leurs attributions et dans la limite du besoin d'en connaître, les agents du ministère de l'intérieur dûment désignés et habilités* ».

[59] Il est à noter que ces phases ne sont, en revanche, pas soumises à autorisation préalable du préfet, contrairement à ce qui est le cas de l'exploitation opérationnelle. Toutefois, en pratique, dans la plupart des cas, quand des paramétrages ont été réalisés pendant plus d'une semaine, des AIPD ont également été rédigées, même si elles n'ont pas été transmises à CNIL, en l'absence d'obligation en ce sens dans le décret.

[60] Cette autorisation, qui doit être communiquée à la CNIL, précise notamment le périmètre géographique concerné, les modalités d'information du public et la durée de l'autorisation (au maximum, d'un mois).

Le juge des référés du Conseil d'Etat l'a confirmé dans une ordonnance du 21 juin 2024, qui rejette une demande d'une société contre une décision de la CNIL constatant la non-conformité au RGPD du logiciel qu'elle avait développé[61].

Ce nouvel état du droit a notamment conduit la RATP et la SNCF à annuler les tests opérationnels prévus en 2024 dans le cadre du programme européen Prevent[62]. En effet, d'une part, la procédure de passation des marchés ayant pour objet de tels traitements a, dans le cadre de l'expérimentation, été centralisée au niveau de l'Etat et seules les solutions sélectionnées dans le cadre du marché national peuvent être testées dans le cadre de la loi, et, d'autre part, le programme Prevent permet l'identification d'individus par le moyen de recours à des données non-biométriques, à l'exception de toute autre, par recherche, de similarité[63], telles que la couleur de vêtement ou la forme générale. Or, la loi du 19 mai 2023 ne prévoyait pas une telle possibilité.

Certains éléments recueillis font cependant apparaître que des collectivités persisteraient à recourir, depuis lors, à des traitements illicites, qui continueraient de leur être proposés par les prestataires non retenus dans le cadre de la présente expérimentation. C'est ainsi le cas du département de Loire-Atlantique, qui a équipé le pont de Saint-Nazaire d'un tel dispositif de sécurisation en juin 2023 et qui conteste devant le tribunal administratif l'opposition de la préfecture à l'autorisation du traitement[64].

1.2.2. Des choix structurants faits au stade de la procédure d'appel d'offres

a) Des contraintes techniques encore renforcées

Au regard des délais particulièrement serrés de l'expérimentation, le comité constate que le choix a été fait par l'Etat d'acquérir les traitements auprès de prestataires privés, plutôt que de les développer ou les faire développer.

Deux décisions majeures, prises dans le cadre de l'élaboration des documents d'appel d'offres, ont limité la portée de l'expérimentation :

- La renonciation à la possibilité, pourtant ouverte par le législateur, de recourir aux traitements algorithmiques des images collectées au moyen de drones, en raison de la maturité

[61] JRCE, 21 juin 2024, société Veesion, n° 495153, C .
Le moyen tiré de ce que ces dispositions du code de la sécurité intérieure issues du décret du 27 novembre 2023 s'appliqueraient aux caméras augmentées au sens de la position du 19 juillet 2022 et, en particulier, à la solution développée par la société Veesion, qui constitue un traitement algorithmique d'analyse des images collectées par les caméras, n'est pas de nature à créer un doute sérieux. D'autre part, si l'article 10 de la loi du 19 mai 2023 dispose que « à titre expérimental (...) les images collectées au moyen de systèmes de vidéoprotection autorisés sur le fondement de l'article L. 252-1 du code de la sécurité intérieure (...) peuvent faire l'objet de traitements algorithmiques », c'est « à la seule fin d'assurer la sécurité de manifestations sportives, récréatives ou culturelles qui, par l'ampleur de leur fréquentation ou par leurs circonstances, sont particulièrement exposées à des risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes », alors que le dispositif développé et commercialisé par la société Veesion ne poursuit pas une telle fin. Dans ces conditions, il est manifeste qu'aucun des moyens soulevés à l'appui de la présente requête n'est de nature à créer un doute sérieux sur la légalité du courrier contesté constatant, en l'état des textes, la non-conformité de sa solution de détection des gestes suspect

[62] Les solutions développées dans le cadre du projet ont pu être testées techniquement et déployées dans le métro de Lisbonne, de Gênes et Barcelone ains que dans les transports régionaux de Catalogne.

[63] Sans recourir en aucun cas à des données biométriques, la recherche par similarité consiste à identifier une personne à l'aide de données telles que la couleur de ses vêtements, sa forme générale, etc.

[64] https://www.lefigaro.fr/nantes/la-videosurveillance-augmentee-des-cameras-du-pont-de-saint-nazaire-fait-debat-20241213

insuffisante des solutions techniques. L'expérimentation a ainsi été limitée aux seuls traitements associés à des dispositifs de vidéoprotection ;
- La renonciation à des traitements automatisés reposant sur l'auto-apprentissage (à savoir l'aptitude à améliorer leurs performances en fonction des données collectées, au fur et à mesure de leur utilisation par les opérateurs). Les traitements ont été certes « entraînés » par le prestataire à identifier certaines situations à risque, mais une fois fournis aux opérateurs et mis en place à des fins opérationnelles, ils ne continuent pas de « s'entraîner ». Leurs performances intrinsèques demeurent donc, à partir de ce moment, inchangées.

Le fait d'exclure de l'expérimentation les technologies recourant à une telle possibilité d'auto-apprentissage trouve son origine dans des choix politiques, administratifs et techniques.

Ces contraintes techniques ont pu dissuader certains prestataires ayant développé des solutions techniques plus sophistiquées de se porter candidats à la passation du marché[65].

b) Un processus de sélection très centralisé et atypique

▪ Les contraintes de calendrier ont conduit à privilégier un processus de sélection des prestataires centralisé et très atypique, limitant, en pratique, le nombre de solutions testées.

Le marché public est articulé autour de trois lots géographiques[66] et d'un lot thématique, consacré aux transports en commun et infrastructures associées. La procédure a été lancée en août 2023 et les avis d'attribution ont été notifiés en décembre 2023.

Les soumissionnaires devaient présenter des solutions capables de détecter :
- A titre obligatoire, pour l'ensemble de slots, le franchissement ou la présence d'une personne ou d'un véhicule dans une zone sensible ou interdite, des mouvements de foule ou d'une densité anormale de population ;
- A titre optionnel, les objets abandonnés, les armes, les personnes au sol et les départs de feu.

▪ Afin de garantir la mise à disposition du traitement au moment voulu, plusieurs attributaires, classés par rang, ont été désignés pour chaque lot du marché. Ainsi, si le prestataire de rang 1 n'était pas disponible, le prestataire de rang 2 était sollicité. Si lui-même déclinait la sollicitation, il était fait appel au prestataire de rang 3.

Dans une tentative de diversification des solutions retenues, les lots géographiques ont été conçus de façon interdépendante : un même titulaire ne pouvait être titulaire de rang 1 que sur l'un des lots afin de pouvoir tester plusieurs solutions. Cependant, cette démarche s'est révélée, dans les faits, inopérante, dans la mesure où, à l'exception de la commune de Cannes, le traitement n'a été mis en œuvre qu'en Ile-de-France.

▪ Les solutions proposées par les différentes entreprises dont la candidature a été jugée recevable ont été testées par le laboratoire national de métrologie et d'essai (LNE), sur la base d'un référentiel concerté avec les services de la CNIL.

[65] Les nouvelles générations d'outil semblent s'orienter sur l'utilisation de LLM (Large Language Model, type ChatGPT, Gemini, etc...) couplés à des VLM (Vison Language model), pour construire des IA générative multimodale, qui seront certainement très performantes techniquement mais également complexes à encadrer.
[66] Lot 1 : Ile-de-France ; lot 2 : Rhône-Alpes, PACA, Corse, outre-mer ; lot 3 : autres régions.

Cinq solutions concurrentes ont ainsi fait l'objet de deux campagnes de tests sur des jeux d'images conçus à cet effet par le ministère de l'intérieur et ont ensuite été expertisées par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) au regard des exigences en matière de cybersécurité.

Les critères de choix ont reposé à 60 % sur la valeur technique (sur la base de deux critères évalués en test[67] pour 56,67 % de la note et de trois critères évalués sur dossier[68]) et à 40 % sur le prix.

- La société Wintics a été désignée attributaire de rang 1 pour les lots Ile-de-France et transport. Ne pouvant l'être également, ainsi qu'il a été dit, pour les autres lots géographiques, c'est la société Videtics qui a été désignée de rang 1 pour le lot comprenant la région PACA. De même, le troisième lot géographique ne pouvant être attribué aux sociétés Wintics et Videtics, c'est la candidature d'une troisième société, Chapvision, qui a été retenue. Cependant, aucune expérimentation n'ayant finalement été conduite dans ce périmètre géographique, son traitement et sa solution technique n'ont pu être testés.

- Il pourra être ici regretté que la procédure d'attribution des lots n'ait permis à la grande majorité des utilisateurs de ne tester qu'un seul prestataire, la société Wintics. La solution développée par la société Videtics n'a pu l'être que de façon limitée, à l'occasion de plusieurs tests réalisés par la commune de Cannes, et celle mise au point par la société Chapvision ne l'a pas été du tout.

c) Le coût financier et le financement du dispositif

L'article 12 du décret prévoit que la SNCF, la RATP et les collectivités territoriales utilisatrices concluent une convention avec l'Etat en vue de déterminer leur participation financière à la mise en œuvre du dispositif.

Le marché public conclu est porté par le programme budgétaire 176 « Police nationale ». Conformément l'article 12 du décret du 28 août 2023, la mise à disposition de ces solutions pour le ministère de l'intérieur au profit de la SNCF, la RATP et des collectivités territoriales utilisatrices est encadrée par des conventions qui prévoient notamment le remboursement intégral par ces opérateurs des montants avancés par le ministère de l'intérieur.

[67] Qualité de l'ergonomie et facilité d'utilisation (20 %) ; qualité de la performance de la solution en test (36,67 %)
[68] Proportion d'évènements optionnels détectés (10 %) ; qualité de la solution proposée (25 %) ; qualité de l'organisation proposée (8 %)

Au 6 janvier 2025, les autorisations et crédits de paiement étaient ventilés comme suit :

		Données	
BUDGET	BENEFICIAIRES	Somme de Montant AE	Somme de Montant CP
2024	PP	220 849,25	207 823,85
	RATP	357 441,17	353 426,68
	SNCF	229 125,70	220 502,90
	VILLE DE CANNES	40 825,34	27 625,54
Total 2024		**848 241,46**	**809 378,97**
2025	PP	1 544,50	1 544,50
	RATP	27 216,92	27 216,92
	SNCF	8 622,98	8 622,98
Total 2025 t		**37 384,40**	**37 384,40**
REPORT CP 2025	(vide)		**35 104,09**
Total général		**885 625,86**	**881 867,46**

Ce dispositif financier a donné lieu à la conclusion de :
- Sept conventions entre le ministère de l'intérieur et la SNCF ;
- Cinq conventions entre le ministère de l'intérieur et la RATP ;
- Quatre conventions entre le ministère de l'intérieur et la commune de Cannes.

1.3. Le dispositif opérationnel mis en œuvre

1.3.1. Caractéristiques générales du système de vidéoprotection et des traitements algorithmiques

▪ Afin de comprendre les dispositifs techniques mis en place par chacun des opérateurs dans le cadre de l'expérimentation, il convient, au préalable, de rappeler les caractéristiques générales de tels équipements.

L'architecture d'un système de vidéoprotection est composée de trois niveaux :
- Les caméras qui fournissent les flux vidéo ;
- Les serveurs, qui permettent le stockage des images et hébergent la partie logicielle du système (le VMS) ;
- Les postes et le réseau informatique utilisés par les opérateurs de vidéoprotection.

Dans le cadre de la vidéoprotection équipée par l'IA, des algorithmes ont été entraînés pour réussir à caractériser dans un flux vidéo le moment où se produisent les évènements à détecter. Ces algorithmes peuvent être intégrés directement sur les caméras ou être exécutés sur des flux vidéo issus de caméras classiques.

Des métadonnées complémentaires sont calculées pour chaque flux vidéo. Elles indiquent notamment, via une estampille temporelle, le moment où un évènement particulier a été détecté[69]. Ces estampilles peuvent ensuite être utilisées pour déclencher des alertes auprès des opérateurs et les inciter à observer un flux vidéo particulier.

[69] Par ex. un flux vidéo issu de la caméra C100 portera l'estampille 31 juillet 2024, 12 :15, « mouvement de foule »

▪ La partie spécifique du traitement IA s'effectue sur les serveurs sous le contrôle des entités effectuant l'expérimentation.

Aucune autre donnée que le fait qu'un évènement ait été détecté n'est signalée. Par exemple, dans les systèmes utilisés, il n'y a pas de fonction permettant d'indiquer quelle est la partie de l'image qui a conduit au déclenchement de l'alerte[70].

Certes, un opérateur observant l'image pourrait ensuite manuellement essayer de suivre une personne qui aurait été identifiée à la suite d'une alerte transmise par le biais du traitement algorithmique, mais la décision est alors prise par un humain (il en est de même du suivi). Et cela fait partie de l'exploitation classique de la vidéoprotection encadrée par le code de la sécurité intérieure.

▪ Les algorithmes sur lesquels repose le dispositif d'IA ont été, préalablement à leur couplage avec les dispositifs de vidéoprotection, entraînés à reconnaître des situations. A cette fin, il leur a été présenté un ensemble de données (dites « d'entraînement »), en l'espèce de courts extraits de vidéos, et il leur a ensuite été donné l'information selon laquelle une situation a été détectée ou non. Par exemple, on a pu présenter à l'algorithme une vidéo avec un individu qui chute et indiquer qu'il s'agit d'une situation de chute.

Un volume très important de données (dans l'exemple précédent, de nombreux exemples de chutes) doit être utilisé pour entraîner l'algorithme de manière satisfaisante. Cette phase d'entraînement a, en l'espèce, été exclusivement réalisée de manière préalable par les éditeurs des solutions de vidéoprotection algorithmique – le logiciel ne continue pas de s'entraîner sur les images captées par les caméras de vidéoprotection.

L'expérimentation aurait certes pu permettre le recueil de données complémentaires qui auraient permis une potentielle amélioration de la qualité de l'entraînement des algorithmes. Toutefois, un tel recueil ne rentrait pas dans le cadre légal et donc n'a pas été réalisé.

▪ Les traitements sélectionnés ne permettent ni l'analyse comportementale ni émotionnelle. Ils ne permettent à aucun moment l'identification ou la catégorisation d'individus mais se bornent à signaler des situations présentant un risque pour l'intégrité humaine (personne au sol, sens de la circulation, densité de foule, …).

1.3.2. Une phase de calibrage cruciale en vue de l'efficacité du dispositif

a) Observations générales

▪ La phase de calibrage est destinée à paramétrer le dispositif. Utilisant une interface proposée par les éditeurs logiciels, elle vise à définir, pour chaque caméra sur laquelle il est prévu d'activer la détection par IA, la ou les zones de détection et le ou les évènements à détecter.

Cette phase est ainsi destinée à vérifier, pour l'ensemble des caméras, la qualité de la programmation initiale, en conditions réelles, mais sans exploitation. Elle permet notamment de déterminer les zones dans le champ de vision des caméras (« polygones ») où sont détectés

[70] On aurait pu imaginer, par exemple, d'entourer la partie de l'image qui indique qu'une personne a pénétré dans une zone interdite.

les évènements et les seuils de détection associés (par ex. nombre de personnes dans une zone ou au m²).

Pour plus de détails sur le déroulement de ces phases aux plans technique et réglementaire, Il sera renvoyé à la note de synthèse de la DEPSA figurant en annexe n° 6.

b) Des modalités de déroulement différentes selon les opérateurs

Au-delà de ces caractéristiques générales, les modalités de mise en œuvre de la phase de calibrage ont été différentes selon les opérateurs.

- La préfecture de police a procédé uniquement, dans un premier temps, à des opérations de calibrage à l'occasion d'évènements concentrés sur une période de moins de trois jours (concert, salon), sans exploitation opérationnelle.

- La SNCF a fait le choix, au début de l'expérimentation, de paramétrer les solutions pendant près de deux semaines en amont d'évènements ciblés, d'une durée d'un à trois jours.

La phase de paramétrage a, par la suite, pu être raccourcie lorsque les gares concernées avaient déjà fait l'objet de calibrage lors de manifestations précédentes.

Six opérations de calibrage[71] ont, au final, été réalisées. Chacune a été conduite en lien avec le ministère de l'intérieur. Le nombre d'interventions de la société Wintics a varié, selon les cas, de deux à six.

- Les modalités de calibrage retenues par la RATP ont été analogues à celles de la SNCF.

La centralisation du dispositif est apparue, de façon générale, excessive à l'opérateur. La RATP aurait souhaité disposer d'un accès direct au prestataire, la société Wintics, notamment pour réaliser des simulations et, le cas échéant, des entraînements de la solution sur le cas de détection des mouvements de foules, afin de faciliter l'évaluation du fonctionnement de l'algorithme sur ce cas d'usage.

- La commune de Cannes a, quant à elle, dû se limiter, dans le cadre du test réalisé lors du Festival, à un nombre réduit de jours de paramétrage, compte tenu de la nécessaire présence d'agents du ministère de l'intérieur pendant cette phase. La phase de calibrage a ainsi eu lieu les 7, 9, 10 et 13 mai 2024, en présence d'un agent du commissariat central de Cannes, représentant le ministère de l'intérieur.

Dans le cadre de la seconde salve d'expérimentation, un paramétrage plus efficient a pu être opéré en tenant compte de ces enseignements.

1.3.3. Les moyens techniques mis en place : des choix différents selon les opérateurs

a) Les chiffres-clefs de l'expérimentation

- Avant les épreuves olympiques, une quinzaine de tests ont été réalisés (cinq par la préfecture de police, cinq par la RATP, quatre par la SNCF et une par la commune de Cannes).

[71] Sans « ré-entraînement » du traitement au vu des premiers tests

Ces tests ont concerné 43 lieux (un pour la préfecture de police, 27 pour la RATP, 14 pour la SNCF et un pour la commune de Cannes).

Pendant les épreuves olympiques, l'expérimentation a concerné 69 lieux, tous situés en Ile-de-France (12 pour la préfecture de police, 46 pour la RATP et 11 pour la SNCF) et 68 pendant les Jeux paralympiques (12 pour la préfecture de police, 46 pour la RATP et 10 pour la SNCF).

Après les épreuves olympiques, et jusqu'au 31 décembre 2024, 16 tests, portant sur 16 évènements distincts, ont été réalisés (11 par la préfecture de police, un par la RATP, un par la SNCF et trois par la commune de Cannes). 21 lieux étaient concernés.

▪ De la première exploitation opérationnelle le 19 avril 2024 (Concert des *Black Eyes Peas*) à fin décembre 2024, on dénombre des tests à l'occasion de 33 évènements différents (14 par la préfecture de police, huit par la RATP, sept par la SNCF et quatre par la commune de Cannes)[72].

▪ La préfecture de police a utilisé, pour un même test, jusque 190 caméras environ, la RATP et la SNCF jusqu'à 300 chacune et la commune de Cannes 17. Soit un total de 800 caméras environ[73].

Dans son amplitude maximale, et tous opérateurs confondus, le dispositif aura ainsi été testé sur une trentaine d'évènements, dans environ 70 lieux différents et au moyen d'environ 800 caméras.

b) Préfecture de police

▪ Quand elle ne s'appuyait pas, avec leur accord, sur le réseau vidéoprotection préexistant d'un opérateur, la préfecture de police a déployé des caméras dédiées à l'IA, non équipées de zoom optique, distinctes et décorrélées du plan de vidéoprotection pour Paris (PVPP), selon quatre configurations :

- Des caméras dites « tactiques », classiquement utilisées par la préfecture de police pour sécuriser des événements. Il s'agissait de caméras nomades, déployées à la demande et qui transmettent leurs images en utilisant le réseau 4G. Pour les mettre en place, il suffit de trouver une source de courants forts (réseau électrique). Les caméras tactiques disposent de leur propre support de fixation qui permet de les apposer sur un toit, un balcon, etc. ;
- Pour le site de Vaires-sur-Marne, une installation spécifique a été déployée, avec pose de mâts, qui ont dû être alimentés spécifiquement en courants forts. Les images étaient transmises via des faisceaux hertziens ;
- Pour le site du stade de France, dans un contexte de saturation des réseaux 4G, il a été fait usage de caméras positionnées à distance des sites visés. La transmission des images s'est faite en réutilisant de la fibre noire[74] non utilisée par le PVPP ;
- Pour le site Arena Sud Paris (porte de Versailles), une interconnexion avec le dispositif de vidéoprotection du gestionnaire du site a été réalisée. Ce sont ainsi les caméras de la société d'économie mixte (SEM) Viparis qui ont été utilisées. Cette option présentait l'avantage de ne

[72] Les déploiements les plus longs ont été ceux réalisés par la préfecture de police, la RATP et la SNCF à l'occasion des Jeux olympiques, puis des Jeux paralympiques, en ensuite ceux qui l'ont été dans le cadre des marchés de Noël à Paris et Cannes.
[73] Ainsi que cela ressort du récapitulatif des différents tests figurant en annexe n° 7.
[74] Ce terme désigne une infrastructure à fibres optiques (câbles et répéteurs) installée mais encore inutilisée.

pas à avoir à procéder à la pose de caméras sur la voie publique et permettait de recourir au système vidéo interne de la société exploitante.

- La première exploitation opérationnelle a eu lieu lors du tournoi de Roland-Garros, au mois de mai 2024. Le comité a cependant constaté, lors de sa venue, que le dispositif mis en place était très modeste, au regard du nombre limité de caméras et de cas d'usage testés. En effet, pour obtenir une vue périmétrique des centres d'intérêt pour les forces de sécurité intérieure (essentiellement les entrées et sorties), peu de caméras étaient requises.

Pendant les Jeux olympiques, le dispositif a été déployé sur treize sites. Le nombre de caméras équipées d'IA a cependant été très variable selon les cas, et, le plus souvent limité (moins d'une dizaine), à l'exception, toutefois, du test réalisé Porte de Versailles. De même, seuls un à trois cas d'usage ont le plus souvent été testés :

- **Site : Roland Garros**

2 caméras ont été déployées. 3 cas d'usage ont été implémentés : densité de foule, mouvement de foule, départ de feu.

- **Site : Stade de France**

20 caméras ont été déployées. 6 cas d'usage ont été implémentés : densité de foule, mouvement de foule, contresens, franchissement, personne au sol, départ de feu.

- **Site : Vélodrome national de Saint-Quentin-en-Yvelines (Montigny-le-Bretonneux)**

8 caméras ont été déployées. 3 cas d'usage ont été implémentés : densité de foule, mouvement de foule, départ de feu.

- **Site : Stade nautique de Vaires-sur-Marne**

15 caméras ont été déployées. 1 cas d'usage a été implémenté : franchissement

- **Site : Aréna Bercy**

7 caméras ont été déployées. 4 cas d'usage ont été implémentés : densité de foule, mouvement de foule, départ de feu, franchissement.

- **Site : Château de Versailles**

8 caméras ont été déployées. 3 cas d'usage ont été implémentés : densité de foule, mouvement de foule, départ de feu.

- **Site : Aréna La Défense**

5 caméras ont été déployées. 3 cas d'usage ont été implémentés : densité de foule, mouvement de foule, départ de feu.

- **Site : Aréna Paris sud**

108 caméras ont été déployées.6 cas d'usage ont été implémentés : franchissement, mouvement de foule, objet abandonné, personne au sol, départ de feu, contresens piéton.

- **Site : Place de la Concorde**

2 caméras ont été déployées. 3 cas d'usage ont été implémentés : densité de foule, mouvement de foule, départ de feu.

- **Site : Fanzone de Créteil**

4 caméras ont été déployées. 4 cas d'usage ont été implémentés : densité de foule, mouvement de foule, départ de feu, franchissement.

- **Site : Parc de la Courneuve**

2 caméras ont été déployées. 3 cas d'usage ont été implémentés : densité de foule, mouvement de foule, départ de feu.

- **Site : Abords du village olympique**

3 caméras ont été déployées. 3 cas d'usage ont été implémentés : densité de foule, mouvement de foule, départ de feu.

▪ Les modalités techniques de mise en œuvre du dispositif ont été analogues pendant les jeux paralympiques, même si l'implication de la préfecture de police dans la mise en œuvre de l'expérimentation a alors été nettement plus forte.

▪ Parmi les différents tests réalisés, deux présentent certaines singularités :

1°) En ce qui concerne le test réalisé porte de Versailles, le nombre de caméras déployées a été significativement plus élevé que dans les autres sites. Par ailleurs, au regard de l'identité de l'exploitant, la SEM Viparis, ces caméras ont, cette fois, pu être disposées à l'intérieur du site, et non seulement à ses abords.

2°) En ce qui concerne le test à Vaires-sur-Marne, une autorisation a dû être demandée à la région IDF qui gère le site et qui est classé site naturel. L'autorisation a été accordée mais soumise au fait que la préfecture de police devait, à l'issue de l'expérimentation, retirer ses installations.

Le choix a, par ailleurs, été fait de recourir à l'IA non pas aux abords des gares et sur le site même mais pour la surveillance de zones interdites au public, sur l'autre berge de la Marne, ce qui a rendu le dispositif plus utile sur le plan opérationnel (cf. *infra*).

c) SNCF

▪ La SNCF a fait le choix de ne recourir au traitement que pour identifier quatre cas évènements indésirables, les seuls qui correspondent, pour l'établissement, à un véritable besoin opérationnel : la pénétration dans une zone non autorisée, les mouvements de foule, la densité de personnes et les objets délaissés.

▪ Le dispositif recourt au réseau de caméras fixes des gares d'Île de France, qui comprend 11 000 caméras, raccordées et centralisées en data center, et interconnectées via un réseau dédié basé sur des infrastructures en fibre optique.

Un maximum de 300 analyses (flux vidéo) a été analysé en simultané. Cette limite s'explique par des considérations :
- Opérationnelles, dans la mesure où un nombre supérieur d'analyses aurait nécessité un renforcement de l'infrastructure de serveurs ainsi que des phases de calibrages complémentaires. Plus de caméras analysées de façon simultanée implique, en effet, davantage de caméras à paramétrer et donc un temps de paramétrage / calibration plus long ;
- Économiques, dans la mesure où le prix du marché conclu avec le prestataire dépend du nombre de licences acquises[75].

Pendant les Jeux olympiques, il a été procédé à un total de 420 analyses[76] :
- 109 analyses de détection d'intrusion ;
- 161 de détection d'objet délaissé ;
- 50 de densité de personnes ;

[75] Une licence logicielle correspond à la mise en œuvre d'un nombre « illimité » de cas d'usage sur une même caméra. Pour des raisons de coûts, SNCF a fait le choix de se limiter à un nombre maximum de 300 caméras analysées en simultané, soit 300 licences acquises. Chaque cas d'usage appliqué à un flux vidéo correspond à une analyse. C'est pourquoi le nombre d'analyse, excède le nombre de flux.
[76] sur 316 caméras.

- 100 de mouvements de foule.

Aucune caméra disposant de zoom optique n'a été utilisée pour l'expérimentation. En effet, le paramétrage des algorithmes nécessite, comme il a été dit, la définition de zones de détection pour chacune des analyses paramétrées[77].

Les caméras utilisées dans le cadre des expérimentations de vidéo augmentée mises en œuvre par la Direction de la Sûreté SNCF sont les suivantes :

Constructeur et modèle	Panasonic WV-NP502	Bosch DINION IP 5000 / 7000 et FLEXIDOME 4000 / 5000
Type de caméra	Numérique IP / fixe	Numérique IP / fixe
Définition d'image	1280x960 (HD)	1280x720 (HD)
Nombre images/sec	30 fps	25 fps
Codec	H.264	H.264
Débit moyen	2,1 Mbps	1,3 Mbps

À noter que le niveau de définition est un paramétrage de ces caméras et que certaines pourraient monter jusqu'à un niveau Full-HD (1980x1080) suivant les évolutions de capacité d'encodage.

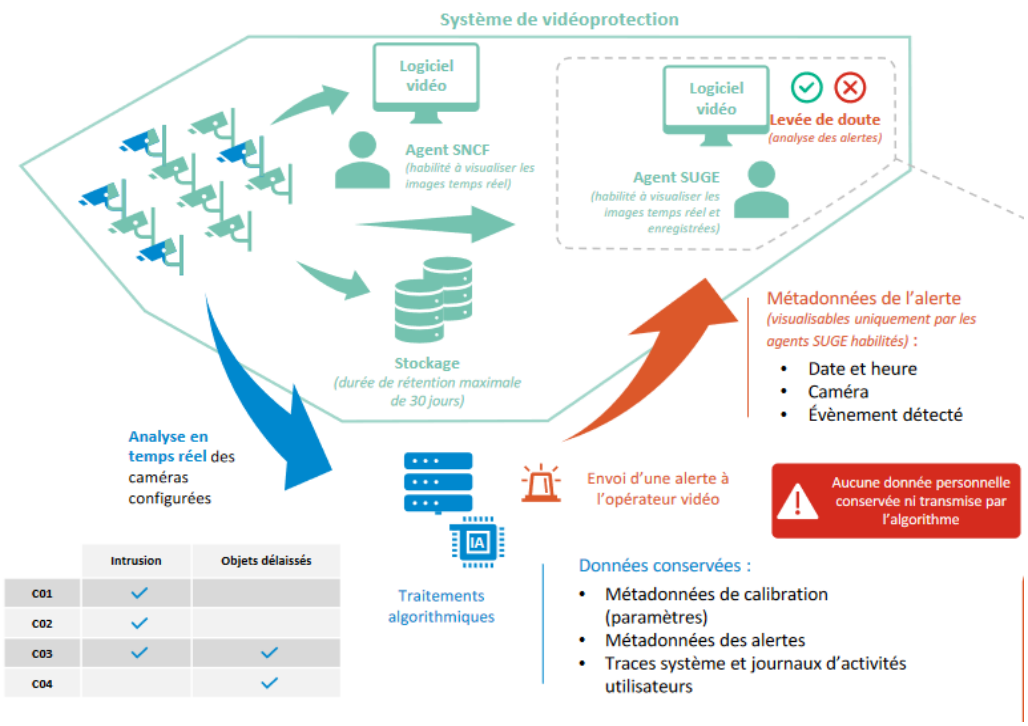
Toutes les caméras exploitées étaient installées préalablement aux expérimentations et appartiennent au système de vidéoprotection des gares d'Île de France. Aucune caméra n'a été ajoutée ou installée spécifiquement pour les expérimentations conduites.

- Les flux vidéo analysés par l'IA (contenant par exemple des détourages d'objets et des personnes, ou encore les zones d'analyse) sont uniquement utilisés instantanément pour vérifier si les conditions d'un signalement sont réunies. Ils sont donc immédiatement supprimés. Seule la génération d'un signalement est remontée au VMS avec des données limitées (caméra, date, heure, type d'évènement)

Ainsi, les opérateurs vidéo de la SNCF auxquels les alertes sont remontées utilisent uniquement leur système vidéo habituel. Lorsque la mention d'un évènement indésirable est signalée, ils peuvent accéder à l'ensemble des 11 000 caméras. Ils s'appuient ainsi sur les images des autres caméras à proximité de celle ayant signalé l'évènement, même si celles-ci ne sont pas équipées d'IA. Aucune image supplémentaire n'est ainsi enregistrée en dehors de ce système.

En outre, l'élément à l'origine du signalement n'est pas mis en évidence, pas plus qu'il n'est en enregistré : c'est à l'opérateur, par sa seule analyse, de vérifier le motif et la pertinence du signalement remonté par les traitements algorithmiques.

[77] Ces caméras pouvant être pilotées, ceci peut, en effet, induire, suivant le paramétrage de l'algorithme, soit : qu'aucune analyse ne soit effective car aucune zone n'est visible dans le champ de vision de la caméra après déplacement (pour des zones figées) ou que les zones d'analyses se déplacent avec le mouvement de la caméra et que des zones non-souhaitées soient alors analysées et remontent ainsi un nombre important de fausses alertes (pour des zones mobiles avec la caméra.



d) RATP

▪ Le système de vidéoprotection de la RATP est constitué de plus 14 000 caméras installées dans les infrastructures de transport du réseau francilien exploité par la RATP.

Ce système de vidéoprotection traite les données vidéo captés dans les espaces ouverts au public, qui, sauf réquisitions judiciaires, sont conservées pendant trois jours, à l'exception d'un parc de 1500 caméras pour lesquelles la durée de rétention des images est de sept jours.

L'ensemble de ce système vidéo est ensuite exploité en temps réel par des agents individuellement désignés et habilités à traiter les données vidéo via des postes opérateurs positionnés :
- Au PC sécurité (levée de doute faisant suite à des remontées d'alarme sur le terrain, vidéo patrouille) ;
- Au centre de coopération opérationnelle de la sécurité (CCOS) de la préfecture de police ;
- Au niveau de la permanence générale de la RATP (levée de doute et gestion des flux de personne).

Les données vidéos sont également exploitées en temps différé sur des postes positionnés :
- Au poste de commandement de la sécurité dans le cadre des levées de doutes et des enquêtes environnementales faisant suite à la découverte d'un objet délaissé ;
- Au niveau du centre de traitement des images vidéo de la RATP pour le traitement des réponses aux réquisitions judiciaires et des demandes de droit d'accès.

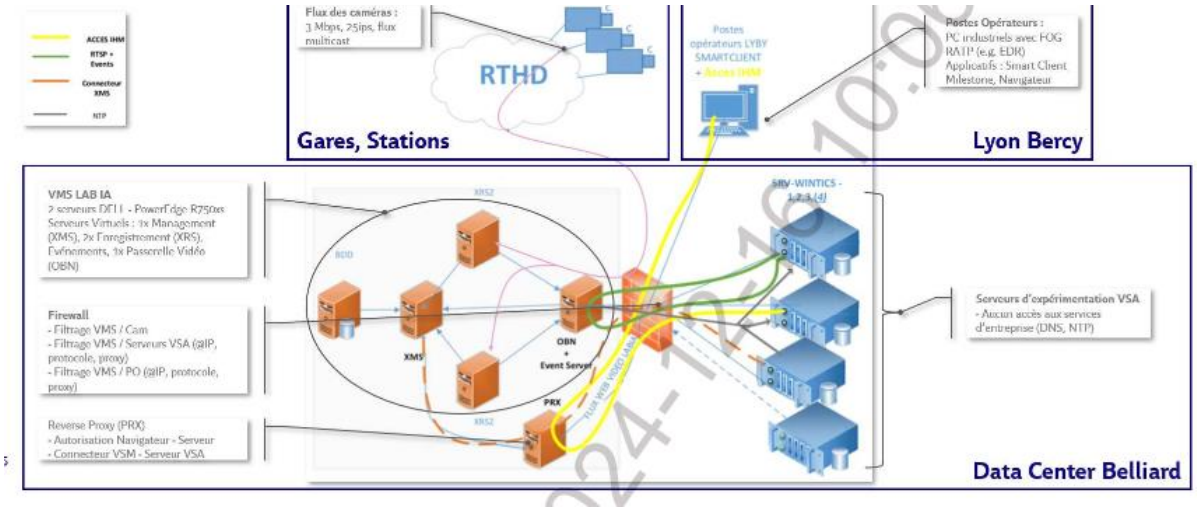
▪ Dans le cadre de la présente expérimentation, le dispositif mis en place par la RATP présente nombre d'analogies avec celui prévu par la SNCF :

- La RATP s'est également appuyée sur le parc de caméras existant et installé sur son réseau, dont les images sont utilisées à des fins internes (sûreté, exploitation des espaces). Aucune caméra n'a été ajoutée ou installée spécifiquement pour l'expérimentation ;
- Les quatre évènements indésirables détectés sont les mêmes que pour la SNCF ;
- Le nombre maximal de flux vidéo pouvant être visualisés simultanément est, comme pour la SNCF, de 300.

▪ Les caractéristiques techniques du dispositif sont les suivantes :
- Un réseau dédié, isolé et sécurisé pour les expérimentations ;
- Deux serveurs de gestion vidéo pour visualiser les flux vidéo ;
- 24 heures d'enregistrement ;
- Trois serveurs d'IA pour l'analyse des flux - contrairement à la SNCF, la RATP a ainsi fait le choix d'investir dans des serveurs spécifiques.

Les opérateurs en charge du suivi des alertes ont été installés dans une salle dédiée. A chaque signalement, ils procèdent à une première analyse. Si celle-ci confirme le risque ou la possibilité de survenue d'un évènement indésirable, ils contactent le PC sécurité, en signalant le type d'évènement et la caméra concernée. Le PC sécurité décide alors de déclencher ou non l'intervention.

Le PC sécurité n'est donc pas saisi directement de l'ensemble des alertes[78].



▪ Dans le cadre des Jeux olympiques et paralympiques, le dispositif a été mis en œuvre dans 48 stations et au moyen des images collectées par 830 caméras.

Le choix a été fait de sélectionner 250 à 300 caméras tous les deux à trois jours pour s'adapter à la programmation des évènements.

La RATP utilise des caméras à focale fixe, sans pilotage du zoom. La focale et l'angle de la caméra sont définis selon les contraintes d'aménagement des espaces et de maintenance des équipements. En règle générale, les caméras sont positionnées à 2,50 / 2,70 mètres maximum de haut et à 2,70 / 3,00 mètres du bord des quais.

[78] Ce choix a été fait pour des raisons matérielles : une remontée directe au PC sûreté aurait nécessité de l'équiper d'écrans supplémentaires, ce qui était difficile sur le plan pratique dans le cadre de cette expérimentation.

Les caméras utilisées dans le cadre des expérimentations de vidéo augmentée mises en œuvre par la RATP sont les suivantes :

Constructeur et modèle	▪ **HIKVISION** (DS-2ZCN2007) ▪ **M2M** (DS-2ZCN2007 M2M) *Connecté à des encodeurs Vidéo* ▪ **SIQURA** (S-64 E, S60E, S68E, S60D64E, S64E V2)	▪ **AXIS** (Q7414, P7701, M1125, Q1615 MK II, Q1615 MK III) ▪ **HIKVISION** (DS-2DE3204W-DE, DS-2XM6212FWD-IM, DS-2ZCN0407-SDI, DS-2ZCN2007, DS-2XM6222FWD-I, DS-2XM6222GO-IM, DS-2CD6425G1-20, DS-2XM6222G0-ID(AE), DS-2XM6222G1-ID) ▪ **VIVOTEK** (FD836BA-HTV, SD 9362-EHL)
Type de caméra	*Caméra Analogique connectée à un encodeur vidéo*	*Caméra IP*
Définition d'image	*4CIF*	*HD (1980x1020)*
Nombre images/sec	*24ips*	*24ips*
Codec	*H264*	*H264*
Débit moyen	*2 Mb/s*	*3 Mb/s*

Le tableau suivant récapitule le dispositif déployé pour les Jeux olympiques et paralympiques.

	Jeux olympiques	Jeux paralympiques
Durée de la phase de calibrage	10 jours	0 jours
Durée d'exploitation opérationnelle	20 jours	12 jours
Nombre de flux vidéo	300	300
Caméras utilisées	830	558

Dans le cadre de l'expérimentation, les images vidéo sont conservées 24 heures pour permettre la levée de doutes suite aux remontées d'alarmes des algorithmes. Seules les personnes habilitées ont accès à ces données vidéos. Les logs du serveur du VMS sont conservées un an dans la limite de l'expérimentation.

Le système vidéo IA est distinct de celui utilisé au quotidien au niveau du poste de commandement de RATP sûreté (en l'absence de réquisition judiciaire, ce dernier conserve ses propres données vidéo pour une durée de 72 heures, voire jusqu'à sept jours).

En cas de doute, les vérifications sont systématiquement effectuées en binôme et les agents opérant le PC sûreté sont, le cas échéant, consultés.

Les erreurs remontées font l'objet systématiquement d'une levée de doute à l'aide de la visualisation des caméras adjacentes permettant de disposer d'un angle de vue diffèrent. En cas de doute, les équipes du PC étaient systématiquement mobilisées, une fiche alarme créée et potentiellement une équipe terrain (agent de station ou du groupe de protection et de sécurité des réseaux - GPSR) en proximité était mobilisée selon la qualification nécessaire pur diligenter l'intervention.

Une hotline permettant de joindre l'équipe projet était disponible en permanence, et, en cas de difficulté technique, une astreinte du prestataire avait été organisée pour permettre à l'opérateur de disposer d'une réponse à ses questions techniques.

Chaque dysfonctionnement a fait l'objet d'une analyse a posteriori avec l'équipe technique, avec le concours éventuel du prestataire en cas de besoin.

Un registre des dysfonctionnements a été mis en place pendant les expérimentations (cahier disponible au poste de travail) ainsi que la possibilité d'échanges de courriel. Lors de chaque étape de paramétrage, un bilan des dysfonctionnements constatés était fait à la société Wintics pour intervention.

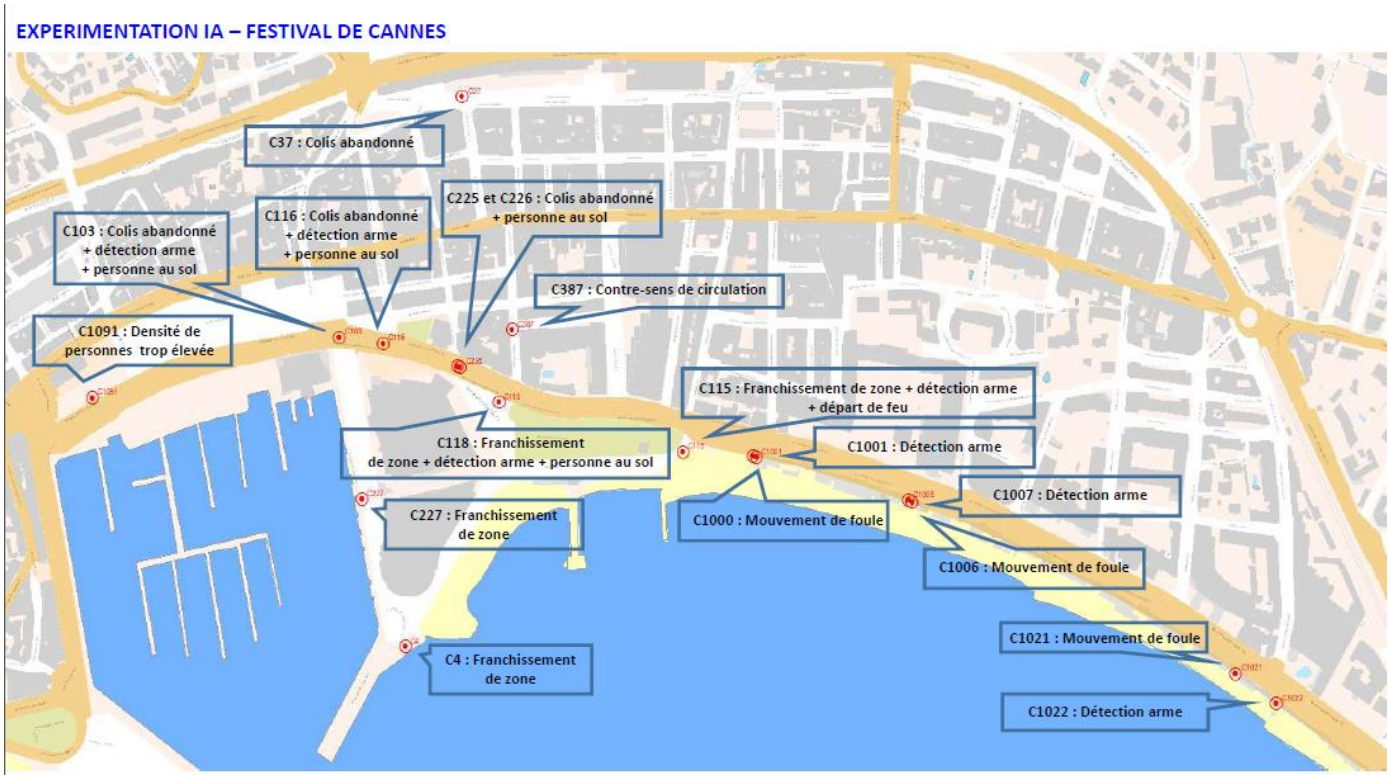
e) Commune de Cannes

Le dispositif a été une première fois testé dans le cadre du Festival de Cannes, du 14 au 26 mai 2024.

Il l'a été ensuite au second semestre dans le cadre de plusieurs autres évènements : les NRJ Music Awards, le marathon Nice-Cannes et le Marché de Noël.

17 caméras ont ainsi été sélectionnées pour le Festival de Cannes et les autres manifestations[79]. Il s'agissait de caméras fixes[80]. Aucune caméra n'a été ajoutée ou installée spécifiquement pour les expérimentations.

Un système dédié, comprenant un serveur spécifique et un poste informatique, a été installé dans une pièce séparée du centre de vidéoprotection, de façon à garantir la confidentialité et la sécurité des accès.



[79] Le réseau de vidéoprotection de la commune de Cannes compte 997 caméras, dont 815 installées sur la voie publique. La majeure partie sont des caméras mobiles. Or, l'utilisation d'algorithmes nécessite d'avoir des images fixes.
[80] Ou de caméras mobiles pouvant être « figées ».

1.3.4. Cybersécurité

▪ Lorsque les données circulent sur des réseaux publics, un VPN (Virtual Private Network) permettant de garantir leur confidentialité via des techniques de chiffrement de bout en bout a été utilisé. Cette technique permet de garantir que même si les flux de données entre les caméras et le VMS sont interceptés, ils seront inexploitables. Chaque opérateur a ainsi dû prendre des précautions afin de s'assurer du respect de ces exigences.

▪ En ce qui concerne la SNCF, l'ensemble des intervenants externes ont signé un engagement individuel de confidentialité et une doctrine d'exploitation de la plateforme et un registre de présence lors de leurs interventions.

D'un point de vue technique, des mesures de protection de la plateforme d'expérimentation ont été déployées, et notamment un firewall permettant le filtrage des flux réseaux.

Le choix a été fait de ne pas autoriser les patrouilleurs vidéo à accéder à la solution logicielle fournie par la société Wintics, ce qui a permis de limiter les risques associés.

Un audit cybersécurité de la plateforme a, en outre, été réalisé et a permis d'identifier plusieurs mesures correctrices. Certaines d'entre elles, relevant du prestataire, ont été partagées avec ce dernier.

Enfin, l'ensemble des actions réalisées au travers du logiciel sont tracées afin d'identifier les utilisateurs ayant traité et acquitté les alertes générées par les traitements.

- En ce qui concerne la RATP, les accès au Lab IA ont été restreints au seul personnel de sûreté dûment habilité par le responsable de la business unit (BU) RATP sûreté. Les agents en question ont été formés à l'usage de la plateforme vidéo.

Du point de vue traçabilité des accès, les agents travaillant sur le Lab IA signent un registre de présence à chaque prise de service, ce qui permet d'identifier les agents en charge des différentes phases opérationnelles de l'expérimentation.

D'un point de technique, les serveurs et systèmes de la plateforme Lab IA sont isolés des environnements vidéo de production, notamment au travers d'un firewall dédié et d'une configuration réseau spécifique (cloisonnement), permettant la maitrise des flux réseau.

L'entreprise est dotée d'un pôle cyber dédié en charge de la réponse à toute tentative d'attaque cyber. Les agents en charge de l'expérimentation ont été sensibilisés aux bons réflexes en cas de survenance d'une attaque de type cyber.

- Concernant la préfecture de police, une séparation stricte des flux vidéo IA a été réalisée, conformément aux consignes de l'ANSSI. Un VMS dédié a donc été utilisé pour collecter les flux vidéo dédiés à l'IA. Parallèlement, il a été demandé à la société Wintics de fournir un serveur dédié pour héberger les solutions algorithmiques.

Les opérateurs vidéo formés étaient tous déjà habilités au PVPP, ils agissaient sur des consoles dédiées depuis les salles des centres d'information et de commandement de la préfecture de police. Dans tous les cas, pénétrer dans ces lieux requiert une habilitation.

Enfin, chaque utilisation de l'IA est tracée, notamment dans un fichier rempli par l'opérateur vidéo.

- Concernant la commune de Cannes, la société Videtics a fourni un serveur dédié afin de séparer les flux vidéo. Seuls les flux vidéo des caméras concernées par l'expérimentation ont été envoyés depuis les serveurs de la ville sur ce serveur dédié étanche. Conformément aux exigences de la commune, aucune communication du serveur vers l'extérieur n'a été autorisée, y compris pour le personnel de la société, qui devait se rendre sur place pour les opérations de maintenance.

De même, aucun interfaçage n'a été effectué entre le logiciel d'exploitation du centre de vidéoprotection et celui de gestion des algorithmes.

Afin de respecter les exigences réglementaires, un poste informatique dédié à l'exploitation des remontées d'alertes a été installé dans une salle séparée du centre de vidéoprotection, afin d'en limiter l'accès aux seuls policiers municipaux.

Chaque agent a été doté d'un identifiant et d'un mot de passe individuel, de façon à sécuriser les connexions et à retracer les actions individuelles de traitement des alertes dans le registre informatisé.

1.3.5. Moyens en personnel déployés dans le cadre de l'expérimentation

a) Effectifs

Préfecture de police :

L'expérimentation a mobilisé à la fois du personnel technique (ingénieurs et techniciens de la direction de l'innovation, de la logistique et des technologies) pour déployer et les caméras et les algorithmes, poser également les affichettes d'information du public, et du personnel opérationnel de police pour utiliser ensuite l'IA (opérateurs vidéo).

La préfecture a mobilisé en tout une vingtaine d'agents pour mener l'ensemble du projet en amont des épreuves olympiques

Pendant les Jeux olympiques, peu d'opérateurs vidéo (moins d'une dizaine) ont été formés. Dans le cadre des Jeux paralympiques, une vingtaine d'opérateurs supplémentaires l'ont été.

La préfecture de police a également formé les opérateurs des directions interdépartementale de la police nationale (grande couronne), en particulier celle de Seine-et-Marne, dans le cadre de l'expérimentation sur le site de Vaires-sur-Marne.

L'IA était mise à disposition des opérateurs vidéo uniquement pendant les épreuves sportives, elle était activée trois heures avant le début des épreuves et désactivée deux heures après la fin, afin de se caler sur les horaires d'arrivée / départ du public.

RATP :

L'ensemble des agents de sûreté des réseaux du PC de RATP sûreté, ainsi qu'une partie des agents de la BU sûreté, ont été habilités à exploiter les données du traitement, afin de permettre une couverture maximale de tous les créneaux nécessaires à la couverture des événements.

Des renforts des effectifs avaient été préalablement planifiés en prévision des épreuves olympiques pour venir compléter les effectifs déployés dans le cadre de la présente expérimentation.

SNCF :

Onze agents, tous volontaires, ont été habilités dans le cadre de l'expérimentation :
- Huit opérateurs vidéo, mobilisés durant la phase d'exploitation opérationnelle ;
- Trois agents en charge du pilotage du projet.

L'IA a été déployée 7 jours sur 7 pendant les épreuves et les plages de service étaient les suivantes : de 6h30 à 14h30, de 14h30 à 22h30 et de 18h à 2h.

L'expérimentation n'a nécessité aucun renforcement des effectifs de la patrouille vidéo, au regard du nombre limité de signalements constaté pendant les premiers tests. Les alertes pouvaient être traitées par les agents déjà présents. Les seuls renforts apportés aux équipes de surveillance vidéo l'avaient été en prévision des épreuves olympiques, mais sans lien avec le recours à l'IA.

Cannes

Seuls des policiers municipaux, habilités à accéder au logiciel, ont été mobilisés. Pour le Festival de Cannes, neuf l'ont été, ce qui a permis d'assurer un suivi 24 heures sur 24 pendant les plages de service suivantes (à raison d'un policier par vacation) : de 5h à 12h, de 12h à 20h et de 20h à 5h, pendant toute la période de la manifestation.

Pour les autres manifestations, les effectifs ont été réduits à deux policiers dans la mesure où les événements se sont déroulés sur quelques heures pour les NRJ Awards et le Marathon des Alpes Maritimes Nice-Cannes, ou sur des plages horaires limitées en journée pour le Marché de Noël (7 jours sur 7, de 11h à 20h).

b) Formation

▪ Dans le cadre de la mise en œuvre de l'expérimentation, une formation sur l'utilisation du traitement a été dispensée par chaque prestataire au bénéfice des différents opérateurs. Les agents ayant reçu cette formation l'ont ensuite dispensée en interne aux autres agents habilités à utiliser le logiciel.

De façon générale, il ressort de l'ensemble des éléments recueillis que la formation a été assez brève sur le plan technique, la prise en main du logiciel s'étant avérée assez aisée.

▪ En ce qui concerne la préfecture de police, les opérateurs ont été formés dans un module de 2 heures au paramétrage des cas d'usage et à la tenue des journaux d'événements. Ils avaient déjà tous déjà reçu une formation dans le cadre du dispositif PVPP, qui comporte un volet SSI et RGPD.

Les agents n'ont pas reçu de formation spécifique consacré aux libertés publiques et à l'éthique. La préfecture indique que ces questions font partie de la formation de base de tout policier.

▪ En ce qui concerne la SNCF, la formation comportait trois modules de deux heures. Deux d'entre eux étaient requis au titre du décret du 28 août 2023 : le contexte et prise en main de l'outil et la sensibilisation RGPD et SSI.
Un troisième, portant sur la sensibilisation éthique, a été mis en place à l'initiative de l'établissement.

▪ En ce qui concerne la RATP, des formations d'une heure environ ont été réalisées auprès de chacun des agents habilités à opérer la solution Wintics.

Une trentaine d'agents a été formée aux seules fins d'exploitation du logiciel.

Un complément de formation RGPD a également été dispensé pour sensibiliser les équipes aux risques liés à la protection des données à caractère personnel en lien avec l'usage des supports vidéo.

Les agents en charge ont été formés pour éviter tout constat discriminatoire.

- En ce qui concerne la commune de Cannes, les agents ont reçu la formation prévue par les textes.

La société Videtics a effectué à chaque événement une session de formation d'une journée à l'utilisation du logiciel pour tous les utilisateurs, ainsi qu'un rappel concernant la protection des données, qui a été complété en interne par le responsable du centre de vidéoprotection.

Un document concernant le respect de la vie privée et la protection des données personnelles a également été réalisé en interne et a été affiché dans les locaux à chaque manifestation.

1.3.6. Suites administratives et judiciaires

Les cas où le recours à l'IA a permis une interpellation ont été très rares.

SNCF

Seul un procès-verbal a été établi à la suite du signalement de la pénétration dans un tunnel interdit au public, d'une personne non habilitée. L'opérateur vidéo ayant reçu le signalement a pu constater l'infraction en flagrance sur la base des images en temps réel de la caméra concernée par la détection et solliciter une équipe de la sûreté ferroviaire (SUGE). La verbalisation réalisée mentionne l'identité de l'opérateur ayant constaté l'infraction, mais pas l'usage du traitement algorithmique. Ce qui s'explique par la circonstance que la détection a bien été réalisée par un opérateur humain.

De même, dans le cas d'une personne détectée sur les voies en zone Eurostar à la Gare du Nord, repérée par un opérateur vidéo ayant reçu une alerte par le traitement algorithmique, les agents de sécurité en gare ont été alertés. La personne a finalement été interpellée plus loin par les agents de la police nationale.

RATP

Dans le cas de la RATP, aucun procès-verbal n'a été établi à la suite d'une détection initialement réalisée au moyen de l'IA.

Commune de Cannes

Aucune interpellation n'a été effectuée par la police municipale à la suite d'une alerte.

2. Des performances techniques très variables selon les opérateurs et les cas d'usage

Ainsi que le prévoit le décret du 11 octobre 2023, l'évaluation porte d'abord sur les performances techniques des traitements algorithmiques mis en œuvre. Si le II de l'article 4 de ce texte prévoit que le collège des services utilisateurs émet, sur ce point, un « avis propre », une telle prise de position spécifique n'est pas apparue nécessaire, les développements qui suivent ayant été approuvés par l'ensemble des membres des deux collèges du comité.

2.1. Des performances délicates à apprécier au moyen d'indicateurs statistiques

2.1.1. Les indicateurs habituellement utilisés pour évaluer la qualité de la détection

L'une des difficultés soulevées par l'évaluation de l'expérimentation consiste à élaborer des indicateurs pertinents pour apprécier l'efficacité du dispositif d'IA.

▪ La qualité de la détection peut être mesurée à partir de quatre hypothèses possibles : « vrai positif », « vrai négatif », « faux négatif » et « faux positif ».

Par exemple, dans l'hypothèse de la détection d'un objet abandonné, quatre situations sont envisageables :
- Il y a bien un objet abandonné et une alerte est remontée par le système (« vrai positif ») ;
- Il n'y a pas d'objet abandonné et aucune alerte n'est remontée par le système (« vrai négatif ») ;
- Il y a un objet abandonné et aucune alerte n'est remontée par le système (« faux négatif ») ;
- Il n'y a pas d'objet abandonné et une alerte est remontée par le système (« faux positif »)[81].

VRAI POSITIF	L'évènement attendu est présent ET une alarme est déclenchée. Ex. : un objet qui semble abandonné est détecté et une alarme est remontée par l'IA. Ex. : une personne entre dans une zone interdite et une alarme est remontée par l'IA.
VRAI NEGATIF	L'évènement attendu n'est pas présent ET aucune alarme n'est déclenchée. Ex. : Il n'y a pas d'objet et l'algorithme ne détecte rien. Ex. : La densité est faible et l'algorithme ne détecte pas de surdensité.
FAUX POSITIF	L'évènement attendu n'est pas présent MAIS une alarme est déclenchée. Ex. : un objet est détecté et une alarme est remontée par l'IA mais il n'est pas abandonné ou ce n'est pas un objet. Ex. : une personne est détectée dans la zone interdite et une alarme est remontée par l'IA mais ce n'est pas le cas.
FAUX NEGATIF	L'évènement attendu est présent MAIS aucune alarme n'est déclenchée. Ex. : un objet est abandonné mais aucune alarme n'est remontée par l'IA. Ex. : un mouvement de foule est visible mais il n'est pas détecté par l'IA.

[81] Le tableau ci-dessous est inspiré d'un tableau élaboré par la RATP.

Les deux premiers cas représentent le comportement espéré et attendu du dispositif. Les deux cas suivants représentent des erreurs. L'objectif poursuivi par l'utilisateur consiste donc à maximiser les « vrais positifs » et les « vrais négatifs » et à minimiser les « faux positifs » et les « faux négatifs ».

Chaque erreur correspond à un problème différent :
- Les « faux positifs » conduisent à remonter des alertes inutiles et à accaparer pour rien le temps des opérateurs. Leur nombre excessif conduit à une perte de confiance des opérateurs et nécessite de comprendre pourquoi l'algorithme s'est trompé ;
- Les « faux négatifs » signifient que le système n'a pas réussi à détecter un évènement, alors que celui-ci a bien eu lieu. Pour les évaluer, il faut disposer de retours d'opérateurs qui ont décelé un cas que l'IA n'a pas identifié[82].

▪ Sur la base de ces considérations, chacun des opérateurs a mis au point ses propres indicateurs, en fonction de son expérience antérieure plus ou moins développée et des caractéristiques d'exploitation qui lui sont propres.

2.1.2. Les difficultés rencontrées dans le cadre de l'expérimentation

a) De la difficulté de mesurer les « faux négatifs » et les « vrais négatifs »

▪ Pour identifier les « faux négatifs » et les « vrais négatifs », il est nécessaire que des opérateurs humains observent l'ensemble des flux vidéo et comparent leur taux de détection avec ceux des algorithmes.

Dans le cadre de la présente expérimentation, les moyens mis en œuvre n'ont que rarement permis d'effectuer de telles mesures. Une évaluation sur un échantillonnage aurait pu être envisagée, comme le comité en avait émis le souhait à plusieurs reprises, mais elle n'a été réalisée que par certains opérateurs et de façon ponctuelle.

Ainsi, la SNCF a réalisé a posteriori des analyses sur la base des fiches évènements signalés au poste de commandement mais aucun cas correspondant aux cas d'usage paramétré sur les périodes et caméras concernées par l'expérimentation n'a été remonté.

Une analyse a notamment été réalisée sur le cas d'usage de densité anormale à l'occasion des difficultés rencontrées à Gare de Lyon le 30 juillet 2024, mais aucune des caméras paramétrées pour ce cas d'usage ne pouvait effectivement détecter de surdensité après analyse des champs de vision et des situations observées.

▪ En revanche, la préfecture de police n'a procédé à aucun test de ce type. Ainsi, par exemple, lors d'un déplacement à Vaires-sur-Marne dans le cadre des Jeux paralympiques, le comité a constaté que l'IA avait permis d'identifier deux patrouilles de police qui avait pénétré dans la zone de détection. Il aurait été utile et aisé de s'assurer que d'autres patrouilles ne s'étaient pas également rendues sur les lieux mais cela n'avait pas été fait.

[82] Dans les deux cas, une façon d'y remédier consisterait à enrichir le jeu de données. Mais on a vu qu'aucun « auto-apprentissage » n'était possible en l'espèce.

Finalement, à la suite d'une demande en ce sens du comité, les vérifications ont été faites et il s'est avéré que les deux patrouilles détectées étaient bien les seules à s'être rendues sur place ce jour-là.

- Les explications évoquées tiennent au manque de temps et de moyens disponibles. Cela se conçoit pour certains cas d'usage, comme les mouvements de foule, mais moins pour d'autres.

La présence d'une personne au sol à la suite d'une chute a été testée par la préfecture de police pendant la phase initiale de paramétrage. Mais l'algorithme n'était pas assez précis et confondait une personne avec tout objet de taille similaire sur la voie publique, ce qui générait de nombreux « faux positifs ». La préfecture a donc décidé de ne pas le tester pendant la phase opérationnelle.

Le comité aurait souhaité que des agents des opérateurs pratiquent des tests en conditions réelles, en reproduisant des situations donnant lieu à des remontées d'alertes (simulation d'abandon d'objet, de départ de feu, ou d'intrusion, …), afin d'observer si le traitement algorithmique les détectait ou non.

b) Une distinction parfois délicate entre « vrais positifs » et « faux positifs »

Un point délicat dans l'évaluation de la qualité des résultats de l'expérimentation est de s'accorder sur ce qu'est la valeur attendue de la détection.

Il convient de distinguer entre deux types de « faux positifs » :

- Les « faux positifs » techniques, qui relèvent d'erreurs d'appréciation du traitement et correspondent donc à une aberration d'un point de vue opérationnel ;
- Les « faux positifs » opérationnels, qui ne présentent pas d'intérêt particulier pour les opérateurs vidéo mais correspondent à des situations conformes avec le paramétrage réalisé (par ex., la présence d'un agent habilité sur les voies).

Ainsi, par exemple, la détection d'agents de maintenance dans des zones interdites peut être considérée comme une détection correcte au plan technique (l'algorithme signale un événement qu'il est programmé pour signaler), même si l'intérêt de cette détection doit être relativisé au plan opérationnel.

De même, si le traitement détecte une valise abandonnée sur une caméra, car il n'y a personne à son côté pendant une minute, une alerte pourra être levée. Or, si le propriétaire de la valise se trouve à côté de la valise, mais hors champ de la caméra, l'objet n'est pas réellement abandonné. Toutefois, il peut également être considéré dans ce cas que la détection a bien fonctionné, et qu'il n'est pas gênant qu'une alerte soit remontée, afin que l'opérateur humain procède à la vérification.

Par ailleurs, comment distinguer les objets abandonnés de l'ensemble de ceux qui sont détectés ?

Chaque opérateur a dû définir ses propres critères d'analyse. Ainsi, pour la SNCF, la réponse dépend de la nature du matériel considéré. Les objets dont le contenu est visible ou n'ayant pas de contenu sont considérés comme « non pertinents » (comme un seau d'entretien, un balai, un

poteau, un appareil d'entretien, …)[83]. En revanche, ceux dont le contenu n'est pas visible ou qui sont considérés comme dangereux par nature sont potentiellement pertinents pour réalisation d'une levée de doute (par ex. les différents bagages, sacs poubelles opaques, bonbonnes de gaz, ...).

c) Des résultats qui dépendent du calibrage réalisé

▪ Certains évènements peuvent être à l'origine d'une multiplicité de signalements. Il en est ainsi, par exemple, de présence dans une zone non autorisée au public d'agents de maintenance ou d'objets spécifiques à l'environnement considéré, que le traitement assimile à des bagages abandonnés.

Cette situation peut influer sur les résultats du test, en surestimant les « faux positifs ». Et, surtout, elle peut perturber le travail des opérateurs, en les contraignant à des vérifications inutiles.

D'où la nécessité de prévenir cette situation par un paramétrage optimal du traitement :
- Soit en définissant un délai minimal suffisamment significatif entre deux signalements (avec toutefois un risque de non-détection de certains évènements si ce délai est trop long) ;
- Soit en définissant des plages horaires d'analyse, afin notamment de limiter la remontée d'alertes pendant les périodes non pertinentes (par exemple, la nuit, lorsqu'aucun patrouilleur n'est présent pour traiter les signalements).

▪ Afin de limiter ces signalements multiples, susceptibles de biaiser les résultats des tests, il aurait été utile que les traitements expérimentés disposent d'une fonctionnalité qui aurait permis directement aux opérateurs de mettre en pause des analyses sur une ou plusieurs caméras pendant une durée définie, sans besoin de faire appel aux administrateurs du traitement. Cette fonctionnalité leur a fait défaut dans le cadre de l'expérimentation.

2.2. Des performances affectées par les caractéristiques du traitement utilisé

2.2.1. Les différences entre les résultats observés lors de la programmation et dans l'environnement réel

▪ De façon générale, les résultats obtenus dans l'environnement réel diffèrent de ceux recueillis en laboratoire, au cours de la phase d'essai préalable à la passation du marché[84].

Les algorithmes de détection des évènements des cas d'usage sont, en effet, dépendants des données utilisées pour les entraîner, comme la taille des individus sur une image. Les différences d'emplacement des caméras utilisées par les opérateurs peuvent, dès lors, conduire

[83] Ce qui souligne l'intérêt d'un apprentissage spécifique dans le cas des équipements de la SNCF.
[84] Rapport d'information de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale du 10 avril 2024 précité : « *la performance réelle des traitements algorithmiques dépend autant de la représentativité des données d'apprentissage sur lesquels ils ont été bâtis que des conditions dans lesquelles ils ont été testés. Ainsi, l'environnement d'un laboratoire ou d'une phase de tests pour choisir l'entreprise attributaire n'est pas comparable à celui d'une gare ou d'un aéroport, alors même que celui-ci évolue en fonction des conditions météorologiques, impliquant un nécessaire déploiement en conditions réelles afin de mesurer d'éventuelles différences de résultats et de mesurer la fiabilité, dans le temps, des dispositifs ainsi mis en œuvre* ».

à des qualités de détection des évènements très variable, pour un même algorithme : moins la caméra est éloignée, plus le taux de « faux positifs » sera limité.

Le débit entre la caméra et les serveurs d'analyse IA peut également être problématique. En effet, les flux vidéo (même compressés) nécessitent une bande passante relativement importante, et parfois, lorsque la caméra est connectée via la 4G, ce débit peut ne pas être suffisant pour envoyer assez d'images par seconde pour que l'algorithme de détection fonctionne correctement.

- De même, il est fréquent que les images sur lesquelles le traitement a été « entraîné » ne prennent pas en compte toutes les configurations susceptibles de se rencontrer dans l'environnement réel. En particulier, la météo, la luminosité, l'affluence, la présence de matériels et mobiliers spécifiques peuvent affecter les performances du traitement.

Ces variations possibles se retrouvent entre la phase de calibrage et la phase d'exploitation opérationnelle. En particulier, avant les épreuves olympiques, le paramétrage a été réalisé par période de beau temps, ce qui a altéré la détection de certains cas d'usage, au début des épreuves olympiques, en raison des fortes intempéries constatées. Certaines caméras ont ainsi dû être momentanément désactivées pour ce motif.

- Par ailleurs, si le traitement a été conçu pour fonctionner également en période nocturne, même en l'absence d'éclairage, via un dispositif infra rouge, son efficacité est alors nettement moindre. Cela a notamment été constaté par la préfecture de police lors des épreuves olympiques.

- Il a encore été constaté que le traitement donnait des résultats plus pertinents dans les espaces clos ou semi clos, notamment dans les couloirs du métro ou des gares, par rapport à ceux observés dans les espaces ouverts. Cela peut notamment s'expliquer par le positionnement différent des caméras dans l'un ou l'autre cas.

- Il peut également arriver que la caméra bouge, à la suite d'un choc accidentel, d'une action malveillante ou encore d'une opération de maintenance. Au-delà de la perte de service et des coûts engendrés, la caméra ne procède plus à la détection demandée dans la zone initialement définie, ce qui génère un grand nombre de faux positifs et négatifs.

Les agents doivent alors procéder à un nouveau calibrage, ce qui peut se révéler fastidieux. Afin de prévenir ces difficultés, le choix pourra souvent être fait de placer des caméras en hauteur, afin de mieux les protéger, en particulier, de la détérioration ou du vol quand sur la voie publique, mais la qualité de détection pourra alors être moindre, car la précision des images sera réduite du fait de la distance et de l'angle de vue.

2.2.2. Les difficultés à définir une zone de détection pertinente

Un grand nombre de « faux positifs » enregistrés au cours des différents tests, en particulier les premiers, tient à la difficulté, dans le cadre des opérations de calibrage, de déterminer la zone de détection des évènements à risque.

Ainsi, la définition de la zone de détection doit tenir compte des effets de perspective (passage de trois à deux dimensions). Par exemple, lorsqu'une personne se trouve sur un quai, le traitement pourra identifier à tort sa présence sur la voie, dans la mesure où sur l'image en 2D,

son torse et sa tête paraissent s'y trouver. D'où la nécessité, en pratique, de définir des périmètres de détection mieux ciblés sur les intrusions réellement dangereuses. Une personne assise sur le bord du quai est ainsi en situation dangereuse alors même que la caméra le détectera à la fois sur le quai et sur la voie.

Le paramétrage doit ainsi être affiné grâce aux expérimentations successives et à la connaissance de l'outil.

2.2.3. Des performances qui dépendent de la qualité du calibrage préalablement réalisé et du bon déroulement du processus itératif avec le prestataire

- De façon générale, les opérateurs ont constaté que la phase de calibrage était primordiale et devait être suffisamment longue pour pouvoir prendre en considération le plus grand nombre de variations (phénomènes météorologique, luminosité, flux variable de personnes…)[85].

Ainsi, par exemple, à Cannes, les tests réalisés sur un temps restreint ou dans le cadre d'un événement ponctuel (comme par exemple, le marathon) ont rendu le paramétrage plus incertain et permis plus difficilement de procéder à des réajustements dans le temps imparti.

Au contraire, ceux qui l'ont été sur une durée plus longue (comme par exemple, le marché de Noël) ont permis de procéder à un recalibrage plus fin. Une telle durée a, en outre, contribué à renforcer l'implication des agents de terrain ainsi que la qualité de la collaboration avec le prestataire technique.

- Dans le cadre de cette phase de calibrage, il a été constaté qu'un processus itératif était nécessaire afin de pouvoir observer les multiples situations en fonction de différentes variables (problèmes de météo, comme la pluie avant le début des JO, flux de voyageurs, travaux, …) et ainsi d'optimiser le paramétrage des analyses.

Ainsi, par exemple, dans le cas de la RATP, le prestataire a réalisé un paramétrage permettant de fixer un délai minimum entre deux alertes successives (même caméra, même cas d'usage, même zone de déclenchement). Compte tenu de l'affluence sur le réseau, ce délai a ainsi été réduit à 30 secondes, afin de ne pas risquer de passer à côté d'évènements importants.

[85] Même si, comme il a été dit, le traitement n'a pas été « réentraîné » à la suite des premiers tests.

Certaines limites dans la détection d'évènements ont certes été remontées aux éditeurs qui ont pu améliorer l'entraînement de leurs algorithmes. Mais ces mises à jour n'ont pu être mises en place sur le système testé lors des Jeux olympiques que de manière partielle, compte tenu des contraintes de temps.

2.2.4. L'absence de visualisation des motifs de signalisation

Le traitement utilisé par la société Wintics fait uniquement remonter à l'agent chargé de la surveillance vidéo la nature de l'évènement indésirable signalé mais n'est pas identifié sur l'image que l'agent consulte. Il en va de même pour le système Videtics. Une telle visualisation n'est en fait possible que pour le calibrage et non dans la phase opérationnelle. Or, elle aurait pu simplifier la détection ou permettre de mieux comprendre le motif qui aurait conduit à tort le traitement à faire remonter une alerte injustifiée.

Les opérateurs sont cependant divisés sur l'opportunité d'un tel affichage à l'écran. Ainsi, la RATP aurait été intéressée par cette fonctionnalité alors que la SNCF, qui préfère que les agents analysent eux-mêmes l'image sans être influencés par le traitement, n'était pas demandeuse.

De même, la police municipale de Cannes insiste sur l'importance de la proactivité des agents dans la surveillance qui permettrait s'assurer un contrôle humain effectif.

2.3. Des performances variables selon les cas d'usage

2.3.1. Des performances globalement satisfaisantes pour l'intrusion, la circulation et la densité de personnes

- Au vu des constats réalisés dans le cadre de l'exploitation opérationnelle, il apparaît que les performances techniques du dispositif sont globalement satisfaisantes pour certains cas d'usage : l'intrusion d'individus ou de véhicules dans une zone non autorisée, la circulation dans un sens non autorisé, la densité de personnes et les mouvements de foule.

Et, en ce qui concerne la pénétration d'un individu dans une zone non autorisée, la SNCF a, par exemple, été en mesure de détecter, entre autres, la traversée de voies ferroviaires ou encore, dans un degré de gravité bien moindre, le passage de personnes dans une zone interdite pour uriner.

De même, lors d'un déplacement sur le site des épreuves olympiques, les membres du comité ont constaté qu'un simple pas dans la mauvaise direction pouvait suffire à faire remonter l'alerte de circulation en sens non autorisé.

- Pour tous ces cas d'usage, le taux de détection de « faux positifs » a, en outre, été assez limité.

Ainsi, par exemple, dans le cas de la densité de personnes, la SNCF fait ainsi état, pendant les épreuves olympiques d'un taux de précision de 100 % - 5 regroupements ayant notamment pu être détectées à l'entrée des gares.

- Le constat doit toutefois être nuancé.

D'une part, dans certains cas, le calibrage a délibérément été défini de façon à limiter le nombre de fausses alertes, afin de ne pas perturber le travail des opérateurs.

En ce qui concerne la densité de population, les opérateurs ont fréquemment défini un seuil de densité élevée (par ex. présence de plus de 10 personnes avec un nombre supérieur à 5 / m²). C'est ce qui explique, par exemple, qu'aucun évènement de ce type n'ait été détecté pendant le Festival de Cannes.

D'autre part, certaines difficultés ponctuelles, à l'origine d'un certain nombre de « faux positifs » ou de « faux négatifs », ont pu être relevées pour ces différents cas d'usage :

1°) En ce qui concerne la densité de personnes, le logiciel a parfois eu du mal à comptabiliser un nombre d'individus trop resserrés. C'est le cas, en particulier, des tests réalisés par la préfecture de police, en raison de la hauteur d'emplacement des caméras.

Le dispositif apparaît moins efficace lorsque les caméras sont trop proches du public, les corps n'étant pas entièrement visibles.

La définition d'un taux pertinent de densité habituellement constaté peut, en outre, être délicate et implique une observation préalable suffisamment fine.

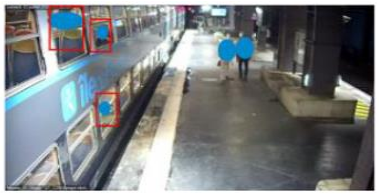
2°) En ce qui concerne la pénétration dans une zone autorisée, la principale difficulté, déjà évoquée *supra*, tient aux effets de perspective. Ainsi, le logiciel peut croire à tort qu'une personne a franchi une zone autorisée alors qu'elle s'est arrêtée juste devant celle-ci.

D'autres erreurs ont pu être causées par des reflets ou des ombres (ce qui met en évidence le besoin d'un entraînement plus poussé du traitement en amont).

Erreurs de classification liées à la détection de personnes : animaux, reflets, ombres, …

Par ailleurs, dans le cas du déplacement sur le site de Vaires-sur-Marne, le comité a relevé un grand nombre de fausses alertes ayant différentes origines (mouvement de branches causés par le vent, animaux ou insectes confondus avec l'intrusion d'individus).

Dans le cas particulier de la SNCF, comme cela est mis en évidence sur les captures d'écrans ci-dessous, il est apparu initialement difficile de discriminer précisément les contours des trains et de neutraliser en conséquence les personnes qui en montent et qui en descendent – le traitement signalant alors à tort leur présence dans la zone de détection définie.



De même, une densité importante de personnes peut masquer certains d'entre elles, pourtant présentes dans la zone de détection[86].

2.3.2. Des résultats encore incertains et à améliorer pour les mouvements de foule

Les performances techniques du traitement en ce qui concerne les mouvements de foule sont difficiles à évaluer. En effet, les opérateurs ont fréquemment choisi des paramètres de calibrage limitant très fortement le nombre d'alertes remontées.

Ainsi, pendant les épreuves olympiques, la RATP avait programmé une vitesse importante de mouvements de foule, de sorte qu'aucune alerte n'a été enregistrée (une seule l'avait été auparavant, dans le cas du concert de Taylor Swift).

La SNCF relève, de même, que seuls deux mouvements de ce type ont été repérés, ce qui ne permet pas de conclure quant à la performance technique du dispositif sur ce point.

De même, lors du Festival de Cannes, aucun évènement indésirable de ce type n'a été détecté.

Les quelques retours font, en outre, état des difficultés rencontrées dans l'identification des véritables mouvements. Le traitement peut, en particulier, assimiler des groupes de personne se déplaçant dans le même sens, sans précipitation particulière. Il est délicat de définir des mouvements de regroupement ou de dispersion rapides[87].

Exemple donné par la SNCF d'un mouvement détecté à tort :

[86] Dans le cadre de l'expérimentation menée à Cannes avec le prestataire Videtics, une autre difficulté ponctuelle a été signalée : dans le cas d'une progression lente d'un véhicule ou d'un demi-tour, si le flux de l'image venait à sauter (ce qui pouvait arriver selon l'état du réseau ou de la caméra), l'algorithme, en récupérant l'image, n'arrivait pas à définir correctement l'état de la progression du véhicule et donc s'il s'agissait ou non d'un contre-sens.
[87] Observations de la SNCF.

2.3.3. Des performances inégales pour la détection d'objets abandonnés et d'armes à feu

▪ Les performances obtenues en ce qui concerne la détection d'objets abandonnés sont très inégales.

Les sources d'erreur possibles sont nombreuses :

- L'absence d'identification du propriétaire de l'objet, lorsque celui se trouve à proximité ;

Outre le cas où cette personne est hors caméra, il peut arriver que le logiciel ne la détecte pas car elle est en position assise ou porte une tenue vestimentaire de couleur proche de celle du sol ou du mur. La difficulté se retrouve lorsque le propriétaire est partiellement dissimulé (notamment lorsque ses jambes sont dissimulées par les bagages).

- L'absence d'identification d'un objet délaissé par son propriétaire au motif qu'une autre personne s'est, entre-temps, trouvée à proximité immédiate.

Le traitement ne pouvant identifier les personnes, il ne peut faire la distinction entre les différents individus qui se sont successivement trouvé à proximité de l'objet.

Ainsi, les bagages personnels sont, le plus souvent, correctement détectés lorsque la zone autour de l'objet est complètement vide – ce qui n'est pas la situation la plus fréquente dans une gare ou une station de métro ou aux abords d'un stade ou d'une salle de concert accueillant un nombreux public.

- La confusion entre les objets sans surveillance et ceux dont la présence sur les lieux n'a rien d'anormal au regard de la configuration habituelle de ces derniers.

Le traitement y assimile ainsi régulièrement le mobilier urbain (bancs, panneaux) ou encore les matériels de nettoyage (poubelles, seaux et machines de nettoyage) et autres objets fixes ou usuels.

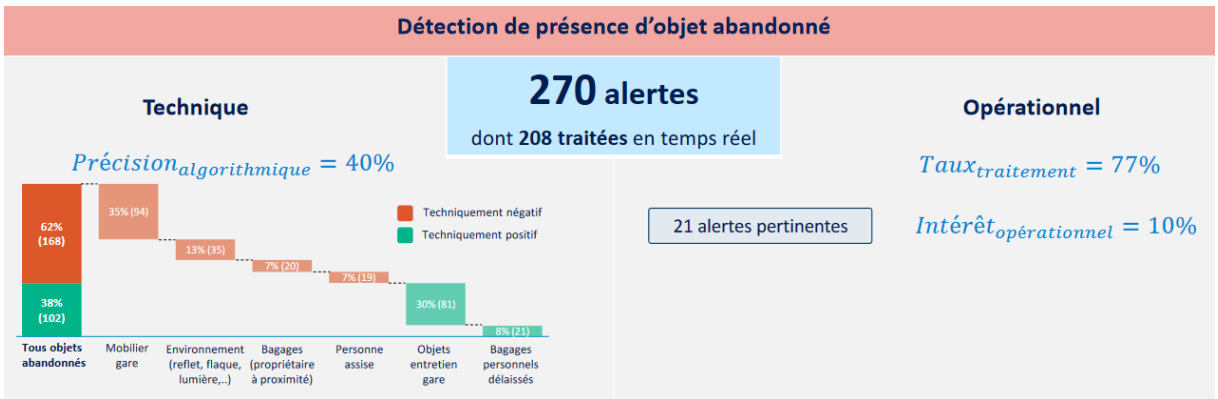
Plus grave, il lui arrive d'assimiler des personnes assises ou statiques, notamment des sans domicile fixe.

D'autres confusions peuvent survenir avec des éléments sombres (absence d'éclairage suffisant, ombre, reflets, flaque d'eau).

Les changements d'environnement intervenus entre les phases de calibrage et d'exploitation ont pu aggraver ce risque d'erreur.

La SNCF cite ainsi l'exemple des « faux positifs » constatés à la gare de Paris Nord pendant les Jeux, en raison du mobilier rajouté en gare ainsi que des intempéries, à l'origine de flaques d'eau.

La SNCF recense ainsi, pour ce cas d'usage, 62 % de faux positifs (168 / 270), le plus souvent du fait d'une confusion avec le mobilier de la gare (94) et l'environnement (reflet, flaque, lumière... – 35). Cette part est d'autant plus importante que parmi les 102 « vrais positifs » détectés, 81 correspondent à des objets d'entretien, dont la détection, même correcte sur le plan technique, est sans intérêt sur le plan opérationnel. Seules 21 alertes ont été considérées comme pertinentes par la SNCF.



Le même constat a été fait lors du Festival de Cannes : de nombreuses fausses alertes ont été déclenchées en raison de la difficulté à identifier les véritables objets délaissés dans le périmètre défini. Aucune alarme probante n'a ainsi été remontée.

- En ce qui concerne la détection d'armes à feu, qui n'a été testée que par la commune de Cannes, seul le traitement développé par la société Vidétics étant opérationnel pour ce cas d'usage[88], les performances techniques ont été variables au cours du temps.

Lors du test réalisé dans le cadre du Festival, la commune a relevé le grand nombre de fausses alertes liées à des mouvements corporels (bras tendu, personne qui se gratte le nez…). Certaines armes portées légalement par les policiers n'ont pas été détectées, notamment lorsqu'elles étaient collées au corps.

[88] La société Wintics avait choisi de ne pas développer cette fonctionnalité, estimant que son traitement n'était pas suffisamment performant sur ce point. De façon plus générale, pour mémoire, au vu de la connaissance de l'état de l'art sur ce cas d'usage, le ministère de l'intérieur a choisi dans le cadre du marché national de ne pas faire figurer ce cas d'usage parmi les cas d'usage obligatoires (cf. 1.2.2).

La commune a toutefois relevé des améliorations de la pertinence des résultats dans la seconde salve d'expérimentations, notamment à l'occasion du marché de Noël. Ainsi, par exemple, les armes des forces sentinelles ont, cette fois-ci, été repérées, ainsi qu'une arme factice (lot gagné sur un stand de la fête foraine). Ces meilleures performances s'expliquent par un meilleur positionnement des caméras, situées moins en hauteur, et par les progrès réalisés dans les opérations de paramétrage et les relations plus fluides avec le prestataire.

Le nombre de faux positifs demeure cependant significatif, en raison notamment de la confusion avec d'autres objets (notamment les bandoulières de sac et les poussettes) ou de difficultés techniques en lien avec la superposition d'images.

2.3.4. Des performances très insatisfaisantes pour la détection des départs de feu et de la présence d'une personne au sol à la suite d'une chute

- En ce qui concerne les départs de feu et la présence d'une personne au sol à la suite d'une chute, qui n'ont été testés que par la préfecture de police et la commune de Cannes, les performances des dispositifs testées sont très nettement insatisfaisantes.

- Concernant les départs de feu, les deux traitements testés y assimilent les feux de voiture, les gyrophares mais aussi, plus généralement, les enseignes lumineuses et les réverbérations sur la voie publique ou les fontaines lors des levers ou couchers de soleil.

- Concernant les personnes au sol à la suite d'une chute, la difficulté tient à la distinction avec les personnes qui le font délibérément. Dans le cas de la commune de Cannes, le logiciel a même pu assimiler le trottoir à une personne au sol.

La société Wintics reconnaît les limites du dispositif testé par la préfecture de police en ce qui concerne la détection de ce cas d'usage, tout en soulignant que celles-ci étaient connues dès la passation du marché. Pour le ministère de l'intérieur, il était néanmoins utile de tester ce cas d'usage en dépit des lacunes du traitement sur ce point.

2.3.5. Récapitulatif statistique selon chaque opérateur

Comme il a été dit, les données statistiques fournies par les opérateurs pour évaluer la performance technique du traitement sont à interpréter avec précaution en ce qu'elles dépendent de la nature des indicateurs utilisés ainsi que de divers éléments de contexte (positionnement des caméras, calibrage, type d'évènements). Cependant, elles confirment les principales constatations précédemment effectuées.

a) Préfecture de police

Pendant les Jeux olympiques, la préfecture de police a choisi de ne pas procéder à des évaluations statistiques au motif que l'IA « n'était pas suffisamment appropriée par les forces de l'ordre ».

En ce qui concerne les Jeux paralympiques, les données recueillies sont les suivantes :
- Densité de foule : 401 détections, 42 faux positifs ;
- Contresens : 21 détections, 0 faux positifs ;
- Départ de feu : 7 détections, 3 faux positifs ;

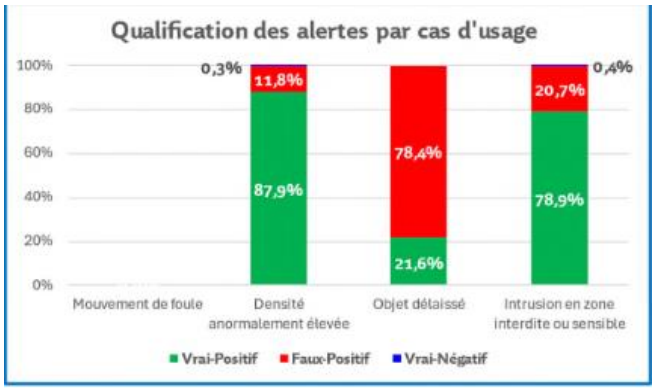
- Mouvement de foule : 2 détections, 0 faux positifs.

Sur ces détections, 55 ont eu un intérêt opérationnel et ont permis à la salle de commandement de déclencher une action.

Contrairement aux opérateurs de transport, la préfecture de police n'a pas eu recours au cas d'usage « présence d'objets abandonnés », qu'elle a considéré comme ayant un intérêt opérationnel faible sur la voie publique.

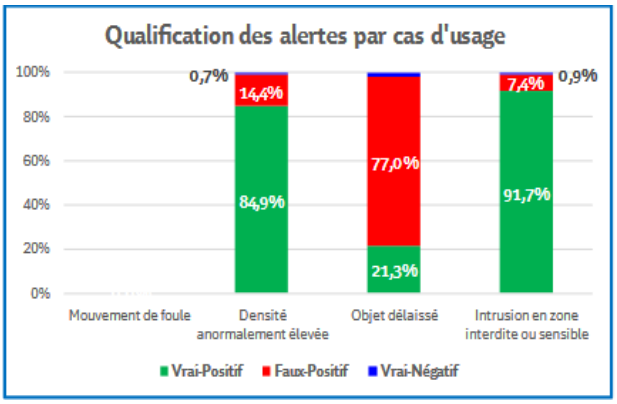
b) RATP

Dans le cadre de la mise en œuvre du traitement pendant les Jeux olympiques, la RATP a recensé plus de 78 % de faux positifs pour les objets délaissés, mais seulement 12 % pour la densité de personnes et 20 % pour l'intrusion en zone non autorisée.



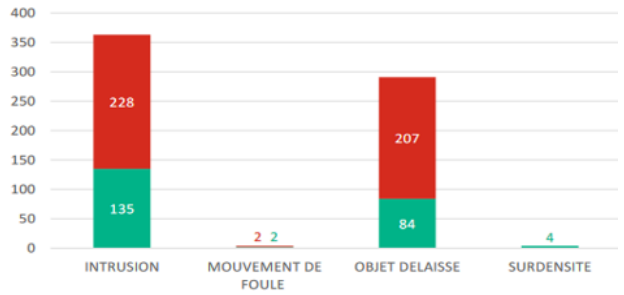
En données brutes :
- Intrusion en zone interdite : 1222 vrais positifs / 324 faux positifs / 11 cas pertinents au plan opérationnel ;
- Objets délaissés : 42 vrais positifs / 151 faux positifs / 2 cas pertinents au plan opérationnel ;
- Densité de population : 305 vrais positifs / 41 faux positifs / 1 cas pertinent au plan opérationnel.

Ces résultats se retrouvent en ce qui concerne les Jeux paralympiques.



c) SNCF

Pendant les 23 jours de la phase de conception (avant les Jeux), la SNCF a recensé grâce au traitement 662 détections, dont 437 constituaient des faux positifs.



Ces résultats se sont ensuite logiquement améliorés pendant la phase opérationnelle.

Un nombre total de 1 552 signalements ont été générés durant les 56 jours d'expérimentation répartis sur les six événements détaillés dans le tableau ci-dessous, dont 58 % pour les intrusions et 40 % pour les objets abandonnés (les 2 % restants correspondant à la surdensité).

Le tableau ci-dessous synthétise le nombre de signalements générés à l'occasion de chacune des expérimentations ainsi que le nombre de signalements traités par les opérateurs vidéo SNCF en service de 6h30 à 22h30, et jusqu'à 2h00 du matin pendant les Jeux Olympiques et Paralympiques.

	Nombre de caméras analysées en simultané	Nombre de jours d'expérimentation	Intrusion		Objet abandonné		Mouvement de foule		Surdensité		Tous cas d'usage	
			Total	*Traités en temps réel*	*Total*	*Traités en temps réel*	*Total*	*Traités en temps réel*	*Total*	*Traités en temps réel*	*Total*	*Traités en temps réel*
PSG - OL	104	3	29	7	62	38	0	0	0	0	91	45
Roland- Garros	30	14	36	35	15	13	0	0	1	1	52	49
Solidays	22	3	12	12	0	0	0	0	0	0	12	12
Flamme Olympique	282	4	46	13	31	19	1	0	4	0	82	32
Jeux Olympiques	300	20	714	388	270	208	0	0	5	5	989	601
Jeux Paralympiques	298	12	56	51	251	205	1	1	18	16	326	273
Total	-	**56**	**893**	**506**	**629**	**483**	**2**	**1**	**28**	**22**	**1552**	**1012**

Il se confirme que la qualité des signalements est nettement plus faible pour les objets délaissés que pour les autres cas d'usage, même si elle est logiquement supérieure dans la phase de programmation. Un nombre total de 206 vrais positifs a été décompté sur 629 alertes, soit environ 2/3 de « faux positifs ».

Au contraire, pour les intrusions, 660 vrais positifs ont été recensés, contre 233 faux positifs, soit environ seulement ¼ de « faux positifs ».

Le tableau ci-dessous synthétise les résultats « techniques » pour l'ensemble des signalements générés pour chacune des expérimentations, notamment le nombre de faux signalements ou faux positifs remontés.

	Nombre de caméras analysées en simultané	Nombre de jours d'expérimentation	Intrusion		Objet abandonné		Mouvement de foule		Surdensité		Tous cas d'usage	
			Positif	*Faux-positif*	*Positif*	*Faux-positif*	*Positif*	*Faux-positif*	*Positif*	*Faux-positif*	*Positif*	*Faux-positif*
PSG - OL	104	3	21	8	21	41	0	0	0	0	42	49
Roland- Garros	30	14	4	32	13	2	0	0	1	0	18	34
Solidays	22	3	0	12	0	0	0	0	0	0	0	12
Flamme Olympique	282	4	34	12	14	17	0	1	4	0	52	30
Jeux Olympiques	300	20	575	139	102	168	0	0	5	0	682	307
Jeux Paralympiques	298	12	26	30	56	195	1	0	18	0	101	225
Total	-	**56**	**660**	**233**	**206**	**423**	**1**	**1**	**28**	**0**	**895**	**657**

Dans le cas plus spécifique des Jeux olympiques, la SNCF a recensé grâce au traitement un nombre total de 989 alertes, dont plus de 80 % constituaient des « vrais positifs ». Celles-ci se répartissent comme suit : 714 intrusions ; 270 objets délaissés ; 5 densités de personnes ; 0 mouvement de foule.

La SNCF a ainsi synthétisé les différents paramètres susceptibles d'influer sur les performances techniques du traitement :

	Favorable à la pertinence technique des alertes	Défavorable à la pertinence technique des alertes
Angle de caméra	• Voie parallèle à la caméra	• Angle d'une caméra vers la voie opposée
Détection de trains	• Trains entièrement dans le champ de vision de la caméra	• Trains partiellement coupés du champ de vision, et/ou ayant des passagers visibles à la caméra
Détection d'humains	• Humains entièrement visibles dans les zones d'intrusion (de la tête aux pieds)	• Humains ayant une partie de leur corps superposant la zone d'intrusion • Objets étrangers à la solution positionnés dans la zone (feuilles, animaux, ombres, reflets, eau,...)
Modifications des caméras		• Les zones d'intrusion ne se modifient pas lors de modifications du champ de vision (caméra déplacée)

Quelques exemples

- **Détection fiable de trains** pour le contexte de la sécurité ferroviaire
- Angles de caméras donnant une **vision adéquate sur les voies et zones interdites** au public
- **Gestion des occultations d'une partie des personnes présentes** sur des plans superposés aux zones de détection
- **Reconnaissance des objets** autres que des humains et trains
- Capacité à **gérer les changements, dysfonctionnements** (caméra bougée, travaux, conditions météo,...)
- **Gestion par les opérateurs d'un arrêt temporaire** d'une analyse sur une caméra pour éviter des répétitions d'alertes inutiles

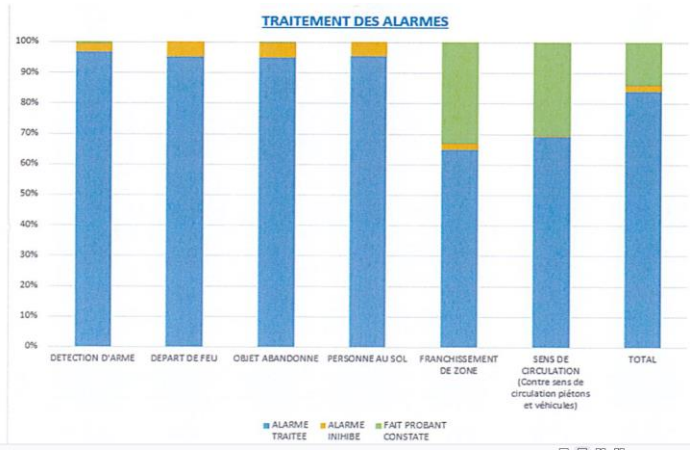
d) Commune de Cannes

▪ En ce qui concerne la commune de Cannes, il importe de bien distinguer les performances techniques du traitement constatées dans le cadre de l'expérimentation réalisée lors du Festival et celles qui l'ont été à l'occasion des expérimentations ultérieures.

▪ Dans le cas du Festival, les performances ont été jugées globalement insatisfaisantes.

Ainsi, sur les 37 194 alarmes signalées, 25 639 ont pu être traitées par les opérateurs mais aucune n'a nécessité l'intervention d'un agent de terrain.

Seuls ont fonctionné les algorithmes détectant les franchissements de zone et les sens de circulation, les autres n'étant pas performants dans le cas de mises en situation réelles avec un fort volume de flux et d'évènements à gérer.



▪ Dans le cas des expérimentations ultérieures, les résultats se sont révélés plus concluants. Comme cela a pu être constaté dans le cadre du déplacement effectué par Mme

Lequesne, membre du comité, le 11 décembre, les échanges avec le prestataire, la société Videtics ainsi que les enseignements de l'expérimentation réalisée lors du Festival, ont, en effet, permis des avancées opérationnelles, l'intégration des systèmes dans le continuum de sécurité de la ville et la coordination des différentes parties prenantes.

Les progrès réalisés sont de trois types :
- Les ajustements ont rendu l'outil plus mature et fiable ;
- Le nombre d'alertes parasites a été réduit, permettant un fonctionnement plus fluide ;
- Les alertes sont mieux gérées et mieux ciblées, ce qui aide les agents à se concentrer sur leur mission principale.

a. Paramétrage et opérationnalisation en amont

Le paramétrage mis en place à l'occasion de ces secondes expérimentations s'est révélé beaucoup plus pertinent que pour le Festival. Ces résultats procèdent d'une convergence de facteurs techniques et opérationnels qui dessine un modèle de bonne pratique :
- Bonne coordination des équipes en amont ;
- Meilleure identification et sélection stratégiques des caméras (fixes, pas trop hautes, résolution adaptée au logiciel) ;
- Optimisation du paramétrage technique des algorithmes et des alertes par le prestataire.

b. Fonctionnalités du système

- Mise en place d'un journal de traitement électronique avec l'ajout d'une fenêtre dédiée au traitement des alertes ;
- Amélioration du poste de travail à destination des agents en charge : présence d'écran multiples, possibilité d'être parallèlement mobilisé sur des tâches parallèles (optimisation du personnel qui soulevait des difficultés et du découragement lors de la première expérimentation) ;
- Création de logs personnels ;
- Possibilité d'identifier un dysfonctionnement technique (pas d'alerte, mais une page de renseignement).

c. Gestion des alertes

- Réduction des fausses alertes, rendant le système plus soutenable pour un traitement humain (levée de doute). Le seuil de déclenchement des alertes a été augmenté pour alléger le travail des agents. Les responsables comme les agents ont souligné à cet égard une évolution décisive.
- Les alertes comportent encore de nombreuses erreurs mais les résultats font « davantage sens » selon les opérationnels. Tel est notamment le cas pour la détection des armes : les armes des militaires de l'opération Sentinelle ont été repérées contrairement à la première expérimentation, tout comme les « pistolets » pour enfants.

d. Collaboration interservices

Ce point a été particulièrement décisif et le chef de service, comme son adjoint, a pointé une forte amélioration sur ce terrain.

La coordination entre la police municipale, la police nationale et le prestataire technique a été plus efficace. Cela tient notamment, selon les opérationnels, à la nomination d'un agent de la police nationale qui connaissait le terrain, ses problématiques, et les agents. Cela procède encore des temporalités : le temps de préparation a été plus adapté que pour la première expérimentation.

Le prestataire a également amélioré ses modes de communication : mise en place d'un service d'astreinte dédié, adaptation technique, adaptation à l'environnement et aux exigences spécifiques en matière policière.

Les chefs de service ont également souligné la fluidité dans les échanges et la collaboration (prise en compte de la réalité et de la maîtrise du terrain).

e. Problèmes techniques et organisationnels

- Algorithme inversé sur la détection du sens de circulation lors du marathon ; le problème a été résolu mais pas dans le temps imparti du marathon, ce qui atteste de l'importance des tests techniques en amont ;
- Si les aspects organisationnels ont été améliorés, on peut toutefois relever le manque de coordination avec les organisateurs des NRJ Music Awards qui ont grevé un bon paramétrage opérationnel (zones d'alerte inappropriées notamment pour le franchissement de zone).

La commune estime qu'il serait souhaitable d'associer plus en amont les organisateurs des manifestations, afin que la police municipale et le prestataire puissent connaître plus précisément les installations logistiques (barrières, barnum, signalisation, etc.) susceptibles d'influencer la détection et ainsi de mieux identifier les besoins sécuritaires et planifier les caméras à équiper d'algorithmes.

3. Un intérêt opérationnel limité mais réel

Au regard de l'ensemble des éléments recueillis, l'intérêt opérationnel du dispositif expérimenté apparaît tout à la fois limité et réel.

Limité, en raison de ses performances techniques inégales et de la difficulté, parfois rencontrée, à faire en sorte que les alertes pertinentes permettent ensuite aux agents sur place d'intervenir en temps utile pour faire cesser la menace détectée.

Mais néanmoins réel, en ce qu'il a pu permettre à certains opérateurs vidéo de se concentrer sur ce qui pouvait être des situations à risque et de procéder à une meilleure répartition des agents présents sur le terrain. Et surtout, il comporte des potentialités. Le faible nombre d'interventions ne suffit pas pour apprécier l'intérêt opérationnel. Avant l'intervention, l'IA a pu amener un examen et une levée de doute qui participent utilement à la prévention des incidents.

L'intérêt opérationnel varie, à la fois, en fonction du contexte d'utilisation et des différents évènements indésirables dont la détection est recherchée.

3.1. Un intérêt variable selon le contexte d'utilisation

3.1.1. Un nombre résiduel d'interventions réalisées grâce au recours à l'IA

De façon générale, le nombre de situations à risque, ayant nécessité des interventions opérationnelles qui n'auraient pas été détectés sans l'IA, apparaît extrêmement faible, au regard des moyens techniques et financiers déployés :

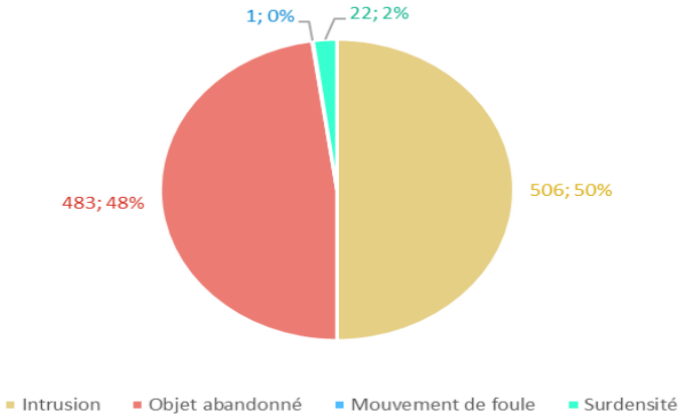
- En ce qui concerne la préfecture de police, une seule intervention à Vaires-sur-Marne (intrusion) ;
- En ce qui concerne la SNCF, trois interventions ont été réalisées durant les Jeux olympiques (il s'agissait, à chaque fois, d'intrusions dans des zones non autorisées) et une durant les jeux paralympiques (détection d'objet abandonné).

Trois autres interventions avaient été effectuées lors des expérimentations préalables aux épreuves olympiques.

Le tableau ci-dessous présente le nombre de signalements générés et traités par les agents opérationnels par cas d'usage pour chacune des expérimentations réalisées.

	Nombre de caméras analysées en simultané	Nombre de jours d'expérimentation	Intrusion		Objet abandonné		Mouvement de foule		Surdensité		Tous cas d'usage	
			Total	*Traités en temps réel*	*Total*	*Traités en temps réel*	*Total*	*Traités en temps réel*	*Total*	*Traités en temps réel*	*Total*	*Traités en temps réel*
PSG - OL	104	3	29	7	62	38	0	0	0	0	91	45
Roland- Garros	30	14	36	35	15	13	0	0	1	1	52	49
Solidays	22	3	12	12	0	0	0	0	0	0	12	12
Flamme Olympique	282	4	46	13	31	19	1	0	4	0	82	32
Jeux Olympiques	300	20	714	388	270	208	0	0	5	5	989	601
Jeux Paralympiques	298	12	56	51	251	205	1	1	18	16	326	273
Total	-	56	893	506	629	483	2	1	28	22	1552	1012

Le graphique ci-dessous illustre la répartition des signalements traités par cas d'usage.



Le tableau ci-dessous détaille, parmi les signalements traités, le nombre de signalements pertinents ou non ainsi que le taux d'intérêt opérationnel correspondant pour chaque cas d'usage et chaque expérimentation.

	Intrusion			Objet abandonné			Mouvement de foule			Surdensité		
	Pertinent	*Non-pertinent*	*Intérêt opérationnel*	*Pertinent*	*Non-pertinent*	*Intérêt opérationnel*	*Pertinent*	*Non-pertinent*	*Intérêt opérationnel*	*Pertinent*	*Non-pertinent*	*Intérêt opérationnel*
PSG - OL	3	4	43%	1	37	3%	0	0	N/A	0	0	N/A
Roland- Garros	3	32	9%	7	6	54%	0	0	N/A	1	0	100%
Solidays	0	12	0%	0	0	N/A	0	0	N/A	0	0	N/A
Flamme Olympique	5	8	39%	5	14	26%	0	0	N/A	0	0	N/A
Jeux Olympiques	251	137	65%	21	187	10%	0	0	N/A	5	0	100%
Jeux Paralympiques	27	24	53%	12	193	6%	0	1	0%	16	0	100%
Total	**289**	**217**	**57%**	**46**	**437**	**10%**	**0**	**1**	**0%**	**22**	**0**	**100%**

Enfin, le tableau ci-dessous synthétise quant à lui ces indicateurs tous cas d'usage confondus et montre un taux d'intérêt opérationnel global de 34%.

	Nombre de signalements générés	Nombre de signalements traités	Taux traitement	Tous cas d'usage		
				Pertinent	*Non-pertinent*	*Intérêt opérationnel*
PSG - OL	91	45	49%	4	41	9%
Roland- Garros	52	49	94%	11	38	23%
Solidays	12	12	100%	0	12	0%
Flamme Olympique	82	32	39%	10	22	31%
Jeux Olympiques	989	601	61%	269	332	45%
Jeux Paralympiques	326	273	84%	54	219	19%
Total	**1552**	**1012**	**65%**	**348**	**664**	**34%**

- En ce qui concerne la RATP, 62 cas ont été remontés au PC sûreté pour une levée de doute complémentaire et le lancement d'une intervention opérationnelle. Quelques-unes de ces remontées ont donné lieu à des interventions de l'exploitant ou des équipes du GPSR pour des intrusions en zones interdites ou des objets délaissés.

- En ce qui concerne la commune de Cannes, une seule levée de doute a été effectuée à la suite d'une détection algorithmique sur l'ensemble des manifestations. Celle-ci s'est déroulée dans le cadre du Marché de Noël : une détection d'arme a été signalée au niveau de la fête foraine et des policiers municipaux se sont rendus sur site. Après vérification il s'agissait d'une arme factice (katana non aiguisé) qui avait été gagné comme lot sur un stand.

Ce nombre très restreint d'interventions s'explique par la forte présence policière (cf. *infra*) mais aussi par le choix de demander aux opérateurs vidéo de procéder à leur métier de police en procédant, toutes les fois où cela était nécessaire, à une levée de doutes.

3.1.2. Un intérêt opérationnel, de façon générale, limité en cas de forte présence policière

L'une des explications à cet apport limité des traitements algorithmiques sur le plan opérationnel lors de l'expérimentation tient au nombre exceptionnellement élevé d'agents déployés sur les différents sites pendant la période olympique (policiers, gendarmes, policiers municipaux ou encore bénévoles). Cette présence humaine garantissait à elle seule des capacités de détection hors normes.

Ce constat a notamment été fait par la RATP, qui relève, dans ses retours d'expérience, que l'écart entre le nombre élevé d'alertes positives et le nombre limité de celles ayant donné lieu à une remontée au poste de commandement en vue d'une éventuelle intervention[89] s'explique par la présence, dans les espaces voyageurs, de très nombreuses équipes de sécurisation et de gestion de l'évènement.

Sur certains emplacements, la mise en place d'une caméra équipée d'IA était ainsi dépourvue de plus-value sur le plan opérationnel. Elle ne pouvait avoir d'autre utilité que de tester la performance du logiciel, mais pas d'apporter une assistance réelle aux patrouilleurs vidéo et aux agents sur le terrain.

Ainsi, par exemple, lors du test réalisé le 29 juillet au stade Yves du Manoir, une caméra avait été positionnée devant une entrée latérale, non destinée au public, alors que des policiers en contrôlaient l'accès. Le même constat a pu être fait, notamment, lors des tests réalisés au stade Roland-Garros.

Le comité n'a observé, en ce qui concerne les tests réalisés par la préfecture de police pendant les épreuves olympiques, un réel intérêt opérationnel que dans certains contextes particuliers, et notamment lorsque l'étendue de la zone à couvrir ne permettait pas d'assurer une présence humaine suffisante. Il en a été ainsi sur le site de Vaires-sur-Marne, en l'absence de patrouilles positionnées en permanence sur une vaste zone sur une île non habitée à proximité du site des épreuves.

De même, l'intérêt très limité du traitement pour les évènements où les effectifs déployés permettent de quadriller le site de façon suffisamment efficace a conduit la SNCF à ne pas l'utiliser dans des gares disposant du plus grand nombre d'agents opérationnels de la SUGE et

[89] Pour les Jeux olympiques, 1 569 alertes signalées par l'IA mais seulement 14 remontées au PC ; pour les Jeux paralympiques, 472 alertes et 7 remontées.

d'agents de police. Le traitement n'a, ainsi, pas été déployé, pendant les épreuves olympiques, dans les gares à proximité du Stade de France. Les gares où il l'a été, comme celle de Saint-Quentin-en-Yvelines, sont celles où les effectifs ne pouvaient couvrir toutes les zones.

Par ailleurs, ainsi que cela ressort en particulier de l'expérimentation réalisée par la préfecture de police, par rapport au processus classique d'installation d'une caméra du PVPP (environ un an de travail entre la recherche de l'emplacement idéal, les autorisations et les travaux), la mise en place d'une caméra tactique pour l'expérimentation, sur un évènement déterminé, se fait en quelques jours seulement. La couverture vidéo n'a donc pas la même finesse et l'intérêt opérationnel du dispositif peut être plus limité.

3.1.3. Un intérêt opérationnel qui dépend de la durée d'entraînement de la caméra

Ainsi que cela ressort en particulier de l'expérimentation réalisée par la préfecture de police, l'intérêt opérationnel du dispositif est nécessairement plus limité lorsque sont utilisées des caméras tactiques déployées spécialement pour un évènement déterminé.

La préfecture souligne à cet égard que leur nombre était nécessairement plus restreint que celui des caméras permanentes du système PVPP et que le délai dont disposaient les services pour les positionner était beaucoup plus court qu'il ne l'est en ce qui concerne les caméras du PVPP.

3.1.4. Un intérêt subordonné à la mise en œuvre du traitement pendant une durée suffisamment longue

L'intérêt opérationnel du traitement IA, extrêmement limité pendant les premières phases de test, s'est progressivement accru au fil du temps.

Cette évolution n'est pas liée la technologie utilisée : ainsi qu'il a été rappelé, les traitements IA mis en œuvre ne sont pas auto-apprenants. Leurs performances techniques intrinsèques ne s'améliorent pas sur la durée, par une meilleure identification des évènements qu'il leur est demandé de détecter.

L'amélioration constatée par l'ensemble des opérateurs résulte en fait d'une meilleure utilisation de cet outil par les agents, tant en ce qui concerne le paramétrage, l'appropriation de l'outil par les opérateurs vidéo que les relations avec le prestataire (cf. *supra*, *2.2.3*.)

D'où l'importance qui s'attache à ce que les tests soient réalisés sur une durée suffisamment longue, et non sur quelques jours seulement comme c'était le cas pour la plupart des évènements

exceptionnels ayant justifié le recours au traitement dans le cadre de la présente expérimentation.

En ce sens, il a été noté par le comité une progression dans l'utilisation et la maîtrise de l'outil entre le début et la fin de l'expérimentation.

3.1.5. Un intérêt qui dépend de l'aptitude à mobiliser des effectifs suffisants pour traiter et pour exploiter les alertes déclenchées

- Le traitement faisant l'objet de l'expérimentation implique que plusieurs agents se relaient en vue du recueil et du traitement des alertes, en utilisant un poste informatique distinct, dédié à cet effet. Comme l'a notamment souligné la préfecture de police, le fait de devoir mobiliser un agent pour cette seule tâche pendant une certaine durée peut soulever des difficultés pour le fonctionnement du service, en particulier en période de forte activité en lien avec un évènement exceptionnel.

- En outre, l'intérêt opérationnel du traitement algorithmique n'est réel que si des effectifs peuvent être mobilisés pour garantir une capacité d'intervention dans un temps limité, lorsque l'IA détecte une situation à risque.

Tel était, par exemple, le cas à Vaires-sur-Marne, où des patrouilles, notamment cyclistes, étaient en mesure de se rendre sur place assez rapidement ou à la RATP qui a divisé par deux son temps d'intervention à partir de l'alerte.

Lors du test à Vaires-sur-Marne, l'efficacité du traitement IA a encore été renforcée par le choix, alors fait, de coupler l'IA à l'utilisation de drones, afin de lever plus rapidement les doutes en cas d'alerte remontée par le traitement algorithmique.

A l'inverse, la SNCF n'a pas utilisé l'IA dans les gares où aucun agent n'était en mesure d'intervenir efficacement une fois l'alerte remontée. En effet, si une personne traverse les voies alors que le premier agent disponible ne peut se rendre sur les lieux avant plusieurs minutes, la remontée d'information, même techniquement pertinente, n'en sera pas moins inutile. En l'absence de tels effectifs, le traitement pourrait certes permettre aux opérateurs de collecter des données afin de mettre en place ensuite des équipes à titre préventif dans les lieux concernés. Mais il ne s'agirait alors pas d'une détection « en temps réel », ainsi que le prévoit la loi.

3.1.6. Les limites en lien avec les catégories d'agents habilités à utiliser le traitement

Pour les collectivités territoriales, seuls les agents de police municipale peuvent être habilités par l'article 15 du décret du 28 août 2023 à utiliser le traitement. Pas les agents administratifs. Or, les collectivités peuvent préférer déployer tous leurs agents de police municipale sur le terrain, en particulier dans le cadre d'évènements d'ampleur, comme c'était le cas pour le Festival de Cannes.

Les agents et responsables de la commune interrogés par le comité ont exprimé leur regret que des personnels administratifs en charge du contrôle vidéo ne soient pas légalement habilités à cette fin. Bien que ces personnels n'appartiennent pas au cadre d'emploi de la police municipale, ils leur apparaissent aptes à remplir ces missions, du fait de leur formation (connaissance du terrain, des caméras, entraînement à la surveillance), de leur intégration au

sein des centres de protection urbains / centres de supervision urbains ainsi que de leur habilitation et des différentes responsabilités qui leur sont déjà confiées.

Ce débat devra avoir lieu en tenant compte du fait que la mission de contrôle devant les écrans est au cœur de la mission de police. Il ne s'agit pas d'une mission d'administration classique mais bien d'une mission de surveillance, de déclenchement de la force publique et possiblement de constitution de preuve. Le code de la sécurité intérieure a posé des règles à son article L. 252-2, y compris pour Paris[90].

3.1.7. Un intérêt qui dépend du choix des zones à risques

L'intérêt opérationnel dépend enfin du choix des zones de détection. Le lieu même de l'évènement n'est pas le seul à être exclusivement pertinent. On a vu que les transports publics qui desservent le site le sont aussi.

Il en est de même en matière d'incendies. Ainsi, par exemple, à Cannes, les zones à risque susceptibles de perturber les événements sont, pour ce cas d'usage, les zones boisées, pourtant situées à une certaine distance géographique du lieu des manifestations justifiant le recours à l'IA.

3.2. Un intérêt opérationnel variable selon les cas d'usage

3.2.1. Un intérêt opérationnel plus marqué pour l'intrusion et la circulation des personnes

- Au vu des technologies expérimentées, la pénétration de personnes et de véhicules dans des zones non autorisées ou leur circulation dans un sens interdit constituent les deux types d'évènements pour lesquels le traitement algorithmique s'avère le plus utile pour les opérateurs.

Il en est ainsi, en particulier, pour la SNCF et la RATP, à qui il permet de détecter de façon plus régulière la présence de personnes sur les voies, en prévenant ainsi des risques pour la sécurité des personnes ou du matériel (en cas de tentative de sabotage) et, accessoirement, en limitant les perturbations causées à l'exploitation du réseau.

La commune de Cannes a fait le même constat lors du Festival, même si aucune intervention n'a été nécessaire dès lors que les individus repérés étaient tous des agents de sécurité du Palais des Festivals.

- Cet intérêt du dispositif pour ce cas d'usage apparaît particulièrement marqué en période nocturne.

S'appuyant notamment sur le test réalisé porte de Versailles pendant les épreuves olympiques, la préfecture de police souligne qu'il constitue un complément utile aux détecteurs anti-intrusion, en ce qu'il permet de visualiser l'intrusion avant de décider d'une éventuelle intervention.

Le caractère insuffisant de l'éclairage, sans lequel le dispositif est beaucoup moins performant (cf. *supra*), a cependant limité une telle utilisation.

[90] art. L. 531-1 et suivants.

De même, pour les transporteurs, les intrusions en zone interdites ou sensibles sont observées en grande majorité de nuit sur les voies et sur les cheminements donnant accès aux voies. Le traitement algorithmique peut donc permettre de dépêcher ponctuellement une équipe afin d'interpeller les individus.

▪ Le test réalisé par la préfecture de police porte de Versailles constitue une autre illustration opérationnelle. Les forces de l'ordre devaient identifier des télépilotes de drone qui en faisaient un usage non autorisé. Afin de réduire les zones de recherche, le cas d'usage « pénétration en zone interdite » a été utilisé pour surveiller automatiquement la partie du périmètre couverte par les caméras tactiques IA, même si, dans le cas d'espèce, aucune alerte n'a été relevée.

3.2.2. Un intérêt à ce stade plus limité pour la détection des mouvements de foule, de la densité excessive d'individus, des objets abandonnés et des départs de feu

▪ L'intérêt opérationnel du dispositif n'est pas négligeable en ce qui concerne la détection des mouvements de foule, de la densité excessive d'individus, des objets abandonnés et des départs de feu.

Cependant, il demeure encore limité pour différentes raisons, qui tiennent au caractère insuffisamment mature de la technologie et/ou aux besoins encore limités des opérateurs d'un tel appui en l'état des effectifs déployés sur place.

▪ Ainsi, les densités anormalement élevées n'ont pas nécessité d'intervention.

En effet, comme il a été dit, les paramètres avaient été définis de façon à limiter ce type d'alertes. Seuls quelques rares cas ont été signalés par l'IA et, même s'il s'agissait de « vrais positifs », le contrôleur n'a pas estimé utile de dépêcher une équipe sur le terrain.

Par ailleurs, on peut penser qui si une densité vraiment anormale avait vraiment nécessité une intervention, les agents présents sur place auraient spontanément réagi, sans qu'ils aient besoin que l'IA ne le leur signale. Contrairement à la pénétration dans des zones non autorisées, ces cas de densité sont généralement constatés à des endroits très fréquentés, où des personnels sont présents, telles les sorties des évènements et les lieux à proximité des zones de vente de billet.

Certes, pour la RATP est la SNCF, le cas d'usage permet d'identifier des problèmes de circulation des voyageurs causés par des machines de compostage en panne ou présence d'un obstacle. Mais il s'agit alors davantage de perturbations dans l'exploitation que de risques pour la sécurité, qui, en l'état actuel du droit, justifient seuls le recours à l'IA.

Il est à noter que la RATP a encore évoqué un intérêt potentiel d'un tel dispositif pour mieux identifier les zones où sévissent les pickpockets. Il ne semble pas, toutefois, que l'IA ait été utilisée à cette fin.

Pour autant, même s'il n'a pas été éprouvé lors des expérimentations, ce cas d'usage n'en demeure pas moins pertinent au regard des enjeux de sécurité publique associés.

▪ En ce qui concerne les mouvements de foule, le constat est le même. Le cas d'usage n'a été que peu testé et n'a pas justifié d'intervention. Les difficultés rencontrées par le traitement pour identifier de tels mouvements ont encore restreint son utilisation.

▪ En ce qui concerne la détection d'objets abandonnés, les attentes des opérateurs, en particulier la RATP et la SNCF, sont particulièrement fortes.

La SNCF rappelle ainsi que, chaque année, 14 000 objets délaissés en moyenne justifient la mise en place d'un périmètre de sécurité (chiffre en hausse depuis octobre 2023 et le passage en risque « urgence attentat »).

Cependant, le nombre encore excessif de remontées d'alertes injustifiées limite encore l'intérêt opérationnel du dispositif (même si la SNCF souligne que le nombre de véritables erreurs doit être relativisé et insiste sur leur bonne acceptabilité par les opérateurs – cf. *infra*).

La SNCF ne fait ainsi état que d'un cas d'objet abandonné signalé lors des Jeux paralympiques en gare du Nord, qui a fait l'objet d'une intervention opérationnelle (mise en place d'un périmètre de sécurité et intervention d'une équipe cynophile).

▪ En ce qui concerne la détection d'armes à feu, la commune de Cannes forme beaucoup d'espoir en vue de la protection de certaines zones urbaines, en particulier celles touchées par le trafic de drogue.

Toutefois, il ne s'agit pas de l'objet de la présente expérimentation, qui portait uniquement sur certaines manifestations particulières, et l'intérêt opérationnel véritable peut, dans tous les cas, être interrogé, dès lors que seules les armes visibles de l'extérieur peuvent être détectées et que seule une intervention policière très rapide pourrait alors prévenir le risque identifié.

3.2.3. Un intérêt très incertain pour la détection des départs de feu et de la présence d'une personne au sol à la suite d'une chute

Pour les deux autres cas d'usage (départs de feu, détection d'armes à feu et de la présence d'une personne au sol à la suite d'une chute), le caractère très insuffisant des performances techniques du traitement par l'IA a rendu pratiquement nul l'intérêt opérationnel du dispositif.

Ces cas n'ont ainsi été que peu testés sur la longue durée, de façon à ne pas submerger les contrôleurs vidéo d'alertes injustifiées.

3.3. Un degré d'attente et de confiance des personnels globalement élevé

3.3.1. Observations générales

Concernant le degré de satisfaction et de confiance des personnels, le comité s'est attaché, par ses visites sur site, en délégation restreinte, d'apprécier la réception des outils de la part des agents chargés de leur déploiement (agents opérationnels, mais aussi autorités hiérarchiques, responsables de la passation des marchés et de l'élaboration des AIPD).

Les agents de la RATP et de la SNCF ont exprimé des opinions favorables quant aux modalités d'usage de ce nouvel outil, sur sa simplicité d'utilisation et sur ses conséquences sur leurs conditions de travail. Et ils se sont également, presque tous, déclarés favorables à son déploiement pérenne.

Il en a été de même, dans une moindre mesure, des agents de la préfecture de police et de la commune de Cannes. Un certain nombre d'entre eux ont pu éprouver, lors des premiers tests, une certaine forme de découragement face à la remontée d'un trop grand nombre d'alertes, généralement non pertinentes. Cependant, leur regard a ensuite évolué de façon plus positive au fur et à mesure de l'expérimentation, du fait des progrès réalisés dans l'utilisation du traitement et dans les relations avec les prestataires.

3.3.2. Observations spécifiques à chaque opérateur

▪ En ce qui concerne la préfecture de police, les réactions des agents sont plutôt bonnes mais néanmoins contrastées. Interrogé lors d'un déplacement pendant les Jeux olympiques, l'un d'entre eux, résumant sans doute le sentiment de nombre de ses collègues, a indiqué : « c'est peut-être l'avenir, pas le présent »

Les potentiels d'amélioration qu'ils ont identifiés sont les suivants :
- Usage de l'outil peu aisé avec ses trois interfaces différentes ;
- Intérêt à ce que la remontée d'alertes par l'IA s'accompagne d'un signal sonore afin que l'opérateur vidéo ne soit pas obligé de regarder en permanence l'écran où elle apparaît ;
- Regret quant au cantonnement de l'usage de cette technologie pour des évènements exceptionnels, alors qu'elle serait peut-être plus utile pour le quotidien, voire dans le cas du maintien de l'ordre (exemple du cortège qui change brutalement de direction lors d'une manifestation.

Le préfet de police a été amené à évoquer ce sujet devant la Commission des lois de l'Assemblée nationale[91] et à faire part de son opinion : « *Le Gouvernement vous proposera ou non une reconduction, mais vous avez compris que j'y suis très favorable à titre personnel et que nous pousserons en ce sens* ».

▪ Les agents de la RATP ont fait part de leur vive adhésion à l'expérimentation lors des visites du comité. Celle-ci est corroborée par les réponses à un questionnaire d'évaluation diffusé en interne à l'issue des Jeux olympiques, dont les résultats montrent un fort intérêt pour le système mis en place ainsi que pour l'organisation opérationnelle retenue.

Quelques regrets ont toutefois été exprimés lors des visites, en particulier la limite du périmètre géographique (pas de possibilité de mise en œuvre, notamment aux abords extérieurs de la station) et surtout le caractère jugé excessivement restreint des cas d'usage. Un agent interrogé aurait ainsi, par exemple, souhaité que le dispositif puisse être utilisé pour identifier les vendeurs à la sauvette.

Les pistes « d'amélioration » souhaitées sont les suivantes :
- Étendre les cas d'usage : détection de rixes, suivi d'individus sans analyse biométrique (…) ;
- Permettre à l'opérateur de recourir à l'IA sur des périmètres élargis des évènements et ne pas se limiter aux simples manifestations culturelles, sportives et récréatives ;
- Pouvoir disposer de plages d'autorisations du recours à l'IA permanentes sur certains périmètres et certains cas d'usage ;

[91] Compte rendu n°4 de la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République, séance du mercredi 25 septembre 2024.

- Disposer d'une latitude sur le choix des solutions technologiques mises en œuvre, en permettant à la RATP de disposer de la relation contractuelle avec le fournisseur de la solution pour simplifier les échanges et de faciliter une fluidité des nécessaires interactions ;
- Disposer d'une capacité à réaliser les actions de préparation à l'utilisation de l'IA en autonomie pour disposer d'une latitude d'ajustements des traitements d'IA sur les caméras ;
- Maintenir les besoins de formation, de préparation et d'habilitation des opérateurs en charge de l'utilisation de l'IA pour affirmer que ces usages ne sont pas ouverts à tous ;
- Renforcer la sensibilisation des personnels sur le volet éthique, avec des mises à jour régulières sur le volet juridique ;
- Constituer un atelier de travail post-expérimentation avec le prestataire et le ministère de l'intérieur pour analyser en détail les conditions de déclenchement des alarmes et optimiser le fonctionnement des algorithmes.

▪ Cette forte adhésion se retrouve en ce qui concerne les agents de la SNCF.

Interrogé lors d'un premier déplacement, le 21 avril, un patrouilleur vidéo estime ainsi que cet outil est « toujours bon à prendre ». Le nombre de fausses alertes ne lui semblait « pas dérangeant », d'autant qu'il en « [comprenait] toujours le pourquoi ». Les opinions sont, en revanche, plus mitigées pour la détection d'objets abandonnés.

D'après un sondage réalisé en interne, cinq des six patrouilleurs vidéo souhaitent la poursuite des expérimentations.

Sur le plan pratique, une difficulté déjà évoquée tient cependant à la contrainte pour l'opérateur d'analyser l'image et les autres vidéos disponibles pour retrouver le motif de l'alerte, ce qui n'est pas toujours aisé.

Plusieurs souhaits ont, par ailleurs, été émis :
- Permettre aux opérateurs vidéo de désactiver les caméras, notamment dans le cas de fausses alertes intempestives, ce qui n'est aujourd'hui pas possible en dehors de la présence d′un représentant du ministère de l′intérieur (cf. supra) ;
- Pouvoir modifier les zones d'analyse en dehors de la présence d′un représentant du ministère de l′intérieur ;
- Utiliser le traitement pour identifier d'autres cas d'usage. Outre les cas d'usage autorisés par le décret du 28 août 2023 que la SNCF a choisi de ne pas expérimenter - armes, présence d'une personne au sol à la suite d'une chute -, les opérateurs vidéo rencontrés verraient un intérêt à ajouter les cas d'usage suivants : dégradation de biens, actes violents, recherche automatique de personnes en temps réel, aide à l'investigation a posteriori.

▪ En ce qui concerne les agents de la commune de Cannes, ceux-ci étaient très réservés sur la plus-value opérationnelle du traitement à l'issue du premier test réalisé lors du Festival.

Ils ont, en revanche, exprimé leur satisfaction à l'issue de la seconde salve d'expérimentation.

Les conditions opérationnelles de la première ayant été améliorées, le système offre, selon eux, des perspectives intéressantes pour la sécurisation future des événements. Les responsables subordonnent toutefois le déploiement de ces usages à une bonne préparation technique et un paramétrage efficient du système en amont, couplés à une bonne formation des agents et à la

maîtrise de la compétence policière (notamment dans la levée de doute et le contrôle des systèmes).

Il est à noter que les opérateurs vidéo du centre de vidéoprotection et leur encadrement ont regretté qu'ils ne puissent être impliqués dans ce projet en raison de leur statut administratif (cette question est évoquée au point *3.1.6* du rapport).

3.4. Libres propos des différents intervenants

Le comité a souhaité retranscrire ci-dessous le regard porté par différents membres du collège des utilisateurs sur le dispositif expérimenté (le regard des associations de défense des libertés publiques est mentionné au point *4.2.1*). Il n'entend pas s'approprier ces développements, qui n'ont d'autre objet que de permettre de mieux appréhender la position des opérateurs et administrations concernées sur l'intérêt opérationnel du traitement algorithmique en matière de vidéoprotection.

L'Association des maires de France a également communiqué au comité une contribution reproduite en annexe n° 14.

Préfecture de police

En dépit des difficultés de démarrage, la possibilité d'utiliser l'IA constitue à l'unanimité une grande avancée pour la préfecture de police. En effet, avec le fort développement de la vidéoprotection, l'IA vient comme une aide à la décision, en pointant aux policiers les caméras qui nécessitent d'être regardées.

Dans le cadre de l'expérimentation, la préfecture de police a pu prendre en main cette technologie et en tirer des enseignements / bonnes pratiques pour tirer le meilleur bénéfice du dispositif :
- Des caméras fixes doivent être dédiées à l'IA : en effet, une interaction d'un agent avec une caméra (changement de direction, zoom) dérègle le dispositif ;
- L'utilisation de l'IA sur une caméra demande un travail fin de paramétrage préalable pour obtenir un résultat optimal. Par exemple, une caméra trop éloignée d'une zone pour un traitement « mouvement de foule » pourra ne pas être en mesure d'assurer une détection si la foule est trop dense ;
- Le rôle du policier est déterminant pour déterminer les seuils à paramétrer après avoir observé le terrain et en fonction de son expérience ;
- Le temps administratif pour dérouler les processus prévus par la loi du 19 mai 2023 est très long et doit être intégré dans les rétro-calendriers de déploiement.

Une fois ces bonnes pratiques appropriées, les performances des algorithmes ont été satisfaisantes pour les cas d'usage suivants :
- Franchissement ou présence d'une personne ou d'un véhicule dans une zone sensible ou interdite ;
- Densité trop importante de personnes ;
- Détection des véhicules ou piétons en contre-sens ;
- Mouvements de foule.

La performance technique est bien au rendez-vous pour ces cas d'usage si le logiciel est utilisé dans les bonnes conditions. En revanche, les autres cas d'usage prévus par la loi ont amené trop

de faux positifs pour pouvoir être exploités opérationnellement. Cette observation est à nuancer car les autres cas n'étaient pas les plus attendus par les services opérationnels.

L'appropriation opérationnelle demande une formation adéquate des policiers et une bonne intégration dans les processus métiers. Le temps nécessaire à cette appropriation ne doit pas être négligé.

L'IA n'était pas complètement ni appropriée ni utilisée par les forces de l'ordre pendant les JO.

Cela s'explique de la manière suivante :

- La forte présence policière sur Paris pendant les JO a diminué l'intérêt de l'IA qui, a contrario, aurait eu davantage de sens en cas d'insuffisance d'effectifs policiers pour mailler le terrain, d'où un intérêt potentiel post JOP, quand la préfecture de police ne disposera plus de renforts extérieurs ;
- En amont des JO, il a été difficile d'obtenir des forces de l'ordre l'organisation de la formation d'opérateurs IA. Il y avait, en effet, un conflit de priorité légitime avec la finalisation de la préparation des JO ;
- Pour porter ses fruits, l'IA doit être pleinement intégrée dans les dispositifs métiers, ce qui demande du temps et de la conduite du changement ;
- Le traitement des alarmes IA nécessite de dégager un opérateur à temps plein sur la mission, ce qui suppose de bien dimensionner le nombre d'agents formés et d'avoir la ressource humaine suffisante ;
- Enfin, le déploiement de l'IA s'accompagne de contraintes juridiques fortes, qui font que l'IA doit être planifiée et ne peut pas être mise en œuvre à la volée.

Les JO, du fait de leur caractère totalement inédit, ont constitué un défi totalement hors norme pour lesquels les directions opérationnelles n'ont pu faire autrement que de s'appuyer sur des processus métiers parfaitement rodés. Face à un tel enjeu, on ne change pas les processus métiers dont on sait qu'ils fonctionnent, et il était utopique, pour un tel exercice, d'envisager de modifier profondément les processus.

La loi circonscrit l'utilisation de l'IA à la tenue d'événements, il n'est donc pas possible d'être en phase d'exploitation en dehors, ce qui limite le temps d'appropriation et de conduite du changement, alors même que le temps nécessaire pour rendre réellement opérationnel le dispositif en phase d'exploitation est non négligeable. Le « Retex » de la phase d'exploitation de Roland Garros montre par exemple que l'opérateur vidéo en charge du traitement des alarmes a eu besoin de plusieurs itérations afin de régler les seuils de déclenchement pertinents en termes métiers, qui avaient un sens opérationnel. L'enseignement à en tirer est qu'il faut pouvoir dégager une ressource concentrée sur ces opérations de réglage pendant l'évènement (ces réglages ne peuvent être faits en amont, tout dépend de ce qui se passe sur le terrain à l'instant t) ; en creux, l'évènement doit durer suffisamment longtemps ou il faut être sur un site donné avec des récurrences d'évènements ayant les mêmes caractéristiques (typologie du public, foule attendue, etc).

Enfin, dans les salles de commandement CIC, les forces de l'ordre disposent déjà de multiples outils informatiques avec lesquels l'IA gagnerait à être intégrée pour être mieux adoptée. Par exemple, la loi demande la tenue d'un journal des alarmes et de leur traitement. Le produit fourni par le marché national ne permet pas de générer automatiquement ce journal, l'opérateur en salle CIC doit donc tenir en parallèle un fichier excel, ce qui est très contraignant. Il serait

plus efficace de pouvoir intégrer ce journal à la main-courante informatique, avec une alimentation automatique du type d'alarme avec l'horodatage associé.

Concernant la tenue d'un évènement, les besoins exprimés par les directions opérationnelles montrent qu'on aurait plus besoin de pouvoir utiliser de l'IA au quotidien en la déployant à la volée en réaction à un incident, sans la relier directement à une compétition sportive par exemple.

A titre d'illustration, pendant les JO, suite à des dégradations répétitives (3 nuits de suite sur de la fibre optique, près du château de Vincennes, il a été envisagé de déployer le cas d'usage « franchissement de ligne » pour détecter à quelle heure, la nuit, un éventuel individu s'approchait de l'endroit. On était donc davantage dans un usage sur la réponse à un incident, lié indirectement à l'évènement sportif.

Si cela aurait été techniquement tout à fait possible, d'une part, le cas n'entrait pas stricto sensu dans ce que la loi permet (même si la sécurisation des câbles optiques peut contribuer fortement à la sécurisation globale d'un évènement), d'autre part, le temps administratif de production de l'arrêté et de diffusion de l'information du public (avec notamment la pose d'affichettes in situ, portant sur l'information du cas d'usage déployé) n'était pas compatible avec l'urgence de la situation. C'est finalement l'intelligence humaine, qui, en visionnant les images des caméras, a identifié la source du problème (qui était en fait une fouine).

RATP

La RATP voit très positivement l'expérimentation relative au traitement algorithmique des images de vidéoprotection conduite sous l'égide du Ministère de l'Intérieur durant la période d'autorisation prévue par la loi et dans les conditions fixées par celle-ci.

Le dispositif proposé aux transporteurs a permis à la RATP de tirer des enseignements précieux sur les cas d'usage suivants :

- Détection de mouvements de foules
- Détection de surdensités
- Détection de objets délaissés
- Détection d'intrusions en zone interdite.

S'agissant de la détection des objets délaissés par un traitement algorithmique d'images, elle représente un apport extrêmement précieux pour l'opérateur de transport qu'est la RATP. Dans le contexte de forte augmentation du nombre d'objets délaissés sur le réseau de métro et de RER exploité par la RATP (+ 263% entre 2019 et 2023), elle ouvre des perspectives qui pourraient même rapidement devenir fondamentales. En effet, la détection d'objets délaissés effectuée sous cette forme permet à la RATP de réaliser beaucoup plus rapidement la levée de doute, donc de qualifier l'objet, d'en retrouver éventuellement le propriétaire et, le cas, échéant d'éviter la mise en place de périmètres de sécurité ou le déploiement de maîtres-chiens détecteurs d'explosifs, avec toutes les conséquences négatives que cela emporte sur le fonctionnement du service aux usagers.

Parce qu'il rend possible une levée de doute immédiate, le traitement algorithmique des images en vue de la détection d'objets délaissés permet de limiter au maximum l'impact sur l'exploitation des lignes concernées. Pour tirer tout le bénéfice possible de ce type de traitement, il est toutefois nécessaire que les algorithmes soient dûment entraînés sur nos réseaux. A cet

égard, il existe à notre avis une marge de progression sur ce cas d'usage qui doit permettre d'aller à l'avenir encore plus loin dans le sens d'une optimisation de notre offre de transport.

S'agissant de la détection des intrusions mais également des zones de surdensité, les apports du traitement algorithmique des images sont également fondamentaux pour renforcer la sécurité de nos réseaux en ce sens que :

- Ils permettent de limiter les intrusions non souhaitées sur nos réseaux : de nombreux cas d'intrusions sur voies ont ainsi été détectés grâce à la solution utilisée dans le cadre de l'expérimentation, attestant de comportements dangereux de la part de nos usagers dont les équipes de la RATP n'ont pas connaissance de manière systématique en dehors du cadre expérimental. Par conséquent, des dispositifs de sûreté ont été mis en place pour corriger ces comportements durant les périodes de détections. L'expérimentation a du reste permis une réactivité renforcée de nos équipes sur le terrain (exploitant et sûreté) qui ont été mises au courant de situation dont elles n'auraient pas eu connaissance en temps normal et à raison desquelles elles ont pu intervenir lorsque cela était nécessaire. Cet apport est particulièrement important dans un contexte où les dégradations de nos matériels roulants et de nos infrastructures se multiplient et perturbent l'exploitation de certaines lignes ;

- Le traitement algorithmique des images de vidéoprotection permet de mieux gérer les situations dangereuses observées lors des sorties de manifestations du fait de la présence de foules importantes. L'expérimentation nous a ainsi aidés dans certains cas, au moyen d'échanges avec l'exploitant, à optimiser les dispositifs humains mis en place dans les stations concernées. Là encore, le recours au traitement algorithmique des images apporte le complément de réactivité nécessaire aux dispositifs humains pour optimiser la mise en œuvre des ressources sur le terrain.

S'agissant, enfin, du dernier cas d'usage, relatif à la détection de mouvement de foules, il est lui aussi susceptible de constituer un moyen d'alerte efficace pour identifier des comportements à risques et agir plus vite, donc plus efficacement. Le recours au traitement algorithmique permet ainsi d'informer l'opérateur de la situation détectée, dont il n'aurait pas connaissance autrement, et, partant, de réaliser une levée de doute rapide et efficace qui va ou non conduire à la mise en place de dispositifs dédiés. Les mouvements de foules sont particulièrement difficiles à anticiper pour un exploitant. L'apport des traitements algorithmiques d'images est important sur ce cas métier pour tout opérateur de sûreté dans les transports, même si la solution utilisée dans le cadre de l'expérimentation n'a permis d'identifier qu'un nombre limité de cas.

En conclusion, le recours au traitement algorithmique des images de vidéoprotection, tel que mis en place dans le cadre de l'expérimentation sur le réseau exploité par la RATP, a permis les bénéfices suivants :
- Donner les moyens d'une meilleure réactivité des équipes de sûreté (PC sûreté et terrain) en complément des dispositifs humains existants, avec 62 interventions opérationnelles qui ont été directement fondées sur une alerte issue de la solution utilisée ;
- Apporter une aide technologique essentielle à la gestion et au traitement d'installations vidéo toujours plus importantes (14 000 caméras fixes sur le terrain aujourd'hui) et rendre possible un gain de temps essentiel dans les situations à risques, qui sont le quotidien de nos opérateurs ;
- Maintenir un niveau de protection de la vie privée analogue à celui garanti en dehors du cadre expérimental du fait de l'absence de technologies de reconnaissances de données biométriques.

SNCF

- Pour le cas d'usage de la détection d'intrusion, l'évitement d'accidents ferroviaires dus à la présence de personnes sur les voies permet d'abord de sauver des vies et aussi d'éviter des perturbations de circulation très coûteuses pour SNCF tant sur le plan financier que sur le plan réputationnel. À titre d'illustration, la personne repérée sur les voies Eurostar en Gare du Nord présentait un comportement à risque, n'hésitant pas à s'introduire sous la motrice d'un train, et si un accident était survenu, les circulations Eurostar entre Paris et Londres auraient pu être lourdement impactées pendant plusieurs heures, et cela pendant la période de Jeux olympiques.

- Pour le cas d'usage de détection d'objets délaissés, le fait de repérer au plus tôt ces situations peut permettre d'accélérer l'enquête environnementale que doit conduire SNCF dans un délai de 20 minutes après détection, en retrouvant notamment plus facilement le propriétaire, ce dernier étant probablement encore dans les emprises de la gare concernée. Cela peut donc permettre d'éviter la mise en place de périmètres de sécurité et donc éviter, là encore, des perturbations de circulation des trains, ou au contraire, si la dangerosité de l'objet est avérée, la mise en place plus rapide d'un périmètre de sécurité afin d'éviter une catastrophe.

- Pour le cas d'usage de détection de surdensité de personnes, il a été observé lors des expérimentations que le bénéfice sûreté semble mineur. Pour autant, il représente un potentiel de bénéfices très intéressant pour le gestionnaire de gares (SNCF Gares & Connexions) ou pour les opérateurs de transports (SNCF Transilien ou TGV par exemple) qui pourraient l'exploiter pour optimiser les flux de voyageurs et anticiper des situations potentielles de perturbation ou à risques pour les personnes à quais.

- Pour le cas d'usage de la détection de mouvement de foule, celui-ci n'ayant fait l'objet que de très peu de signalements, il est difficile d'en appréhender des bénéfices autres que théoriques sur la détection éventuelle d'un fait de sûreté grave associé au mouvement de foule.

- Enfin, si le nombre de situations détectées ayant induit une intervention des forces de sécurité présentes en gare lors des expérimentations peut sembler faible (seulement 7 interventions : 6 pour des détections d'intrusion et 1 pour un objet abandonné), il est important de le relativiser en tenant compte de la mobilisation exceptionnelle des forces de sécurité dans les gares à l'occasion des évènements ayant fait l'objet d'une expérimentation. Une exploitation de ces cas d'usage dans une période normale permettrait très certainement la gestion d'un nombre de situations beaucoup plus important.

Ile de France Mobilité

Concernant le champ des transports, le dispositif d'intelligence artificielle utilisé a montré son intérêt opérationnel pour renforcer l'efficacité de la présence humaine et sa complémentarité avec les autres outils disponibles.

Aujourd'hui, les transports publics en Île-de-France disposent d'un réseau de vidéoprotection très maillé, avec plus de 80 000 caméras. Ce maillage permet une analyse fine en temps réel d'un événement signalé par ailleurs mais ne permet pas, au vu du très grand nombre de caméras à surveiller, une détection en temps réel de tous les éventuels événements de sûreté ou de sécurité.

L’expérimentation réalisée sur quelques centaines de caméras, à la fois pour la SNCF et la RATP, montre que l’association réseau de caméras, utilisation de vidéo équipée d’IA, analyse par des opérateurs formés et présence humaine sur le terrain permet de renforcer la sûreté des transports pour les usagers, avec une réelle complémentarité.

Tout d’abord, l’usage de l’intelligence artificielle facilite l’orientation des équipes sur le terrain en permettant une priorisation plus rapide des interventions, grâce à un réseau complémentaire de capteurs.

De plus, l’utilisation de l’intelligence artificielle pour la vidéoprotection permet aussi de détecter des événements qui pourraient ou auraient autrement échappé à la vigilance humaine au vu de l’étendue du réseau ou qui auraient été décelés plus tard avec un impact alors supérieur.

Dans le cas de la SNCF, la vidéoprotection intelligente a été intégrée à la chaine opérationnelle.

L’ensemble des opérateurs concernés dans le cadre de l’expérimentation a été formé, avec une forte adhésion des équipes devant la complémentarité du dispositif et la simplicité d’usage. La vidéoprotection augmentée constitue un outil d’aide à la décision : un opérateur valide ou non l’alerte, avant d’engager ou non une équipe sur le terrain.

L’IA a permis de détecter des événements de sûreté, notamment pour les intrusions et constitue un nouveau canal d’alerte, alors qu’aujourd’hui la vidéoprotection « simple » ne permet pas de détecter d’événements, mais simplement de vérifier a posteriori une alarme reçue par ailleurs.

Elle permet aux opérateurs vidéo d’appuyer encore davantage les équipes déployées sur le terrain en les alertant sur des événements détectés par la vidéoprotection augmentée. Le rôle des opérateurs vidéo se trouve ainsi renforcé.

En complément, elle permet aussi d’avoir une réponse opérationnelle adaptée à l’événement et de ne pas arrêter inutilement le fonctionnement du réseau, grâce à une levée de doute plus ciblée et plus rapide.

Concernant le déploiement, une période de calibrage est nécessaire pour chaque caméra ou groupe de caméras. Cette initialisation reste beaucoup plus simple dans les transports car il s’agit d’un réseau de caméras fixes et dont le positionnement est stable.

Enfin, une information complète des usagers a été réalisée en lien avec les opérateurs et la CNIL, notamment au moyen d’affichages notamment dans les gares et stations concernées, mais n’a appelé très peu de questions.

En conclusion, la vidéoprotection avec IA permet une détection plus rapide et plus fine des événements de sûreté mais aussi, indirectement de sécurité dans les transports. Elle s’inscrit pleinement en complémentarité des dispositifs humains déjà déployés sur les réseaux franciliens.
Elle renforce la sûreté des transports, tout en préservant les libertés individuelles avec une information adaptée des usagers.

Commune de Cannes[92]

Les conclusions de la commune de Cannes dans son « Retex » faisant suite à l'expérimentation conduite au cours du Festival étaient très négatives : d'un point de vue opérationnel, il n'avait pas été observé de réelle plus-value tout au long de la période concernée car la gestion de ce dispositif avait mobilisé des ressources qui auraient pu être employées de façon plus efficiente.

L'absence de paramétrage adapté, le manque de coordination des services ont conduit à la mise en place d'un système que les agents jugeaient insoutenable voire « décourageant ». Les centaines d'alertes remontées, ajoutée à un contexte opérationnel très contraignant (tenue d'un registre manuel, mobilisation exclusive et au détriment du terrain d'un agent de police dédié, absence de poste opératoire multiple) et à l'appréhension d'une nouvelle technologie, expliquaient ces conclusions.

Ainsi qu'il a été dit, les expérimentations qui ont suivi ont conduit à un bilan d'ensemble nettement plus positif, en raison de la mise en place d'une concertation approfondie entre les équipes opérationnelles, mais également avec le prestataire.

1°) Enseignements

a. Intégration de l'humain au cœur du dispositif

Si la police municipale cannoise dresse un bilan positif de l'expérimentation, elle insiste à son issue, sur l'importance d'accompagner la montée en équipement technique d'une montée en compétence des agents. Il est nécessaire de former les agents habilités sur le plan technique, mais aussi d'un point de vue éthique et juridique. En outre, pour conserver la compétence humaine, et maintenir les compétences opérationnelles, les responsables soulignent la nécessité de « ne pas tout automatiser » et de contraindre les agents à des vérifications fréquentes (notamment sur les dysfonctionnements du logiciel).

b. Utilisation stratégique du système

- Nécessité d'un travail d'équipe en amont pour identifier les zones où la vidéosurveillance algorithmique est pertinente ;
- Les caméras et les fonctionnalités doivent être sélectionnées de manière stratégique en fonction de la nature de l'événement ; tous les usages et toutes les caméras ne sont pas adaptés.

c. Collaboration renforcée

- Importance d'une bonne collaboration entre les opérateurs vidéo, la police municipale et les services opérationnels. Le choix de l'agent de police nationale est à cet égard, dans le contexte réglementaire présent, stratégique ;
- Le renforcement de l'astreinte et du service d'accompagnement de la société technique a participé au succès des dernières expérimentations ;
- De la nécessité de permettre aux agents vidéo habilités (hors personnel de la police stricto sensu) de recourir au système. Cette condition, exclue à ce jour par les textes, apparaît

[92] Les développements qui suivent retranscrivent la position de la commune, tels qu'elle ressort des échanges de ses responsables avec une membre du comité à l'occasion de ses deux déplacements dans le cadre de l'expérimentation.

indispensable à une pérennisation des outils pour le bon fonctionnement des services. Il s'agit de la principale revendication formulée.

Les deux salves d'expérimentations successives ont également permis de mettre en évidence les exigences stratégiques et opérationnelle requises pour assurer la fonctionnalité du système.

La commune de Cannes insiste sur l'importance d'un travail d'équipe en amont, impliquant l'ensemble des parties prenantes (dont le prestataire technique et les responsables de l'événement le cas échéant) pour identifier les zones où la vidéosurveillance algorithmique. Les caméras et les fonctionnalités doivent être sélectionnées de manière stratégique en fonction de la nature de l'événement : tous les usages et toutes les caméras ne sont pas adaptés, et ce d'autant que les systèmes dotés d'IA requièrent la priorité de CSU.

En termes organisationnels, la collaboration entre les opérateurs vidéo, la police municipale et les services opérationnels est primordiale. Le choix de l'agent de police nationale est à cet égard, dans le contexte réglementaire présent, stratégique. Il est également apparu indispensable que le prestataire accompagne les équipes à l'aune de la spécificité du terrain policier. En l'espèce, le renforcement de l'astreinte et du service d'accompagnement de la société technique a participé au succès des dernières expérimentations.

Pour des motifs opérationnels, la commune de Cannes plaide enfin pour un élargissement de l'habilitation aux agents vidéo habilités (hors personnel de la police municipale stricto sensu). Cette condition, exclue à ce jour par les textes, entrave la bonne marche du système et l'intégration métier de la vidéoprotection algorithmique au CSU.

2°) Perspectives

- La police cannoise plaide en faveur de la pérennisation du système et surtout de l'expérimentation pour affiner le fonctionnement algorithmique dans le temps.

En dehors des grands événements, le système pourrait servir à l'urbanisme et à la surveillance des zones sensibles. Ils seraient très utilement élargis, selon ces mêmes services, au suivi des plaques d'immatriculation (sans nécessaire rattachement à un fichier) et à la recherche avec filtre (ex : recherche d'un camion blanc, une voiture rouge dans tel zone, etc).

- Réglementation et supervision : les services plaident en faveur d'un élargissement des outils à la police municipale dans le cadre étroit des centres de supervision urbains, et à l'habilitation des agents dédiés à la vidéosurveillance qui seraient, selon eux et de surcroit, « mieux formés ».

Délégation interministérielle au Jeux olympiques et paralympiques

Par leur ampleur et leur durée, les Jeux olympiques et paralympiques de 2024 constituaient pour l'Etat et pour les organisateurs un défi logistique et sécuritaire inédit.

La préparation et l'accompagnement des Jeux par les services de l'Etat ont constitué une réussite, sans aucun incident notable de sécurité, de sûreté et de cybersécurité ni sans aucun surcroît d'activité judiciaire liée aux JOP, aux cérémonies, aux relais de la Flamme ou encore aux sites de célébrations.

L'événement a été un succès international reconnu, sportif, festif et populaire, au cours duquel il a été peu fait mention de problématiques de sécurité, hormis pour souligner une atmosphère paisible et sûre, concrétisée par une forte visibilité des forces de sécurité.

Ces Jeux resteront une référence, notamment parce que l'acceptabilité sociale et l'expérience spectateur avaient été mises au centre de l'organisation et de la stratégie de sécurité.

Au même titre que les performances sportives ou le succès de l'organisation, l'un des facteurs de réussite de ces Jeux a été la volonté, apparue dès la candidature, de léguer au pays-hôte un héritage utile et durable, matériel et immatériel, dans de nombreux domaines.

Ainsi, la DIJOP est attachée à ce que les dispositions législatives de la loi du 19 mai 2023 constituent également un héritage des Jeux olympiques et paralympiques de 2024, en se donnant du temps et des perspectives de développement, à l'instar d'autres legs matériels et immatériels de ces Jeux, pour que le traitement algorithmique des images de vidéoprotection atteigne sa pleine maturité dans les prochaines années, tant du point de vue des performances techniques que de la prise en main par les opérateurs.

Le constat que fait la DIJOP sur le déroulement de cette expérimentation, que le Délégué et ses collaborateurs ont suivie avec assiduité et intérêt dans les conditions décrites par le rapport, est que les performances techniques sont démontrées pour certains cas d'usage tels que la détection de l'intrusion d'individus ou de véhicules dans une zone non autorisée, la circulation dans un sens non autorisé, la densité de personnes et les mouvements de foule. A l'évidence, la vidéoprotection équipée d'IA permet une détection plus rapide et plus fine des événements de sûreté et de sécurité. Elle s'inscrit pleinement en complémentarité des dispositifs humains présents dans l'espace public.

L'expérimentation a également démontré la compatibilité de ces technologies avec la protection des libertés publiques, condition essentielle de l'acceptabilité sociale, au sujet de laquelle la DIJOP a toujours été très vigilante dans la préparation des JOP 2024, en particulier en matière de gestion de la sécurité et des déplacements dans l'agglomération parisienne.

En conséquence, la DIJOP demeure favorable à la primauté du contrôle humain et à une application de ces traitements algorithmiques en tant qu'aide à la décision, ainsi que le non-recours à la reconnaissance faciale pour ce domaine d'application.

Plusieurs facteurs et circonstances conduisent à ce stade à modérer l'intérêt opérationnel de l'outil, qui n'en demeure pas moins réel pour renforcer l'efficacité de la présence humaine et sa complémentarité avec d'autres outils disponibles, sous réserve d'une part d'étendre son périmètre d'emploi, par la loi, de manière pérenne, à la sécurité du quotidien, au-delà du seul cadre des manifestations qui présentent un caractère exceptionnel par leur densité et leur complexité, ainsi qu'à d'autres cas d'usage utiles aux opérationnels et d'autre part de simplifier les modalités administratives de déploiement.

Il ressort cependant que, dans le cadre des Jeux, c'est plutôt dans les secteurs de grande superficie en pleine nature, comme la base nautique de Vaires-sur-Marne, davantage qu'aux abords des établissements recevant du public dans les zones urbanisées, où les forces de sécurité étaient nécessairement concentrées sur les points névralgiques à défaut de pouvoir surveiller l'intégralité de la zone, que le traitement algorithmique s'est avéré le plus utile.

Or, dans la perspective des Jeux olympiques et paralympiques d'Hiver 2030, le contrôle des accès à de très vastes espaces naturels en montagne, par principe non clôturés pour respecter l'ambition environnementale, constituera à l'évidence un enjeu stratégique et l'une des missions prioritaires confiées aux forces de sécurité publiques et privées, afin de garantir la qualité de l'expérience spectateur et l'acceptabilité sociale de ces Jeux, dans les mêmes conditions qu'en 2024.

4. Un public insuffisamment informé mais intéressé

Comme le prévoit le décret du 11 octobre 2023 (cf. supra), seul le collège des personnalités qualifiées s'est prononcé sur la présente partie du rapport.

4.1. L'information du public

4.1.1. Le dispositif général mis en place

▪ L'article 10 de la loi du 19 mai 2023 prévoit que le public doit être préalablement informé « par tout moyen approprié » de l'emploi de traitements algorithmiques. Il confie en particulier au ministre de l'intérieur le soin d'organiser son information générale sur l'emploi de tels traitements.

Dans son avis sur le projet de décret relatif aux modalités de pilotage et d'évaluation de l'expérimentation, la CNIL a recommandé fortement que l'information générale relative à la tenue d'une expérimentation soit délivrée également sur les lieux où les traitements algorithmiques seront déployés ainsi que dans ceux où une captation d'image ultérieurement utilisées pour l'apprentissage est prévue (par exemple, par l'affichage de codes QR renvoyant vers le site web du ministère).

▪ Les utilisateurs se sont conformés aux prescriptions légales ainsi qu'à cette recommandation. Dès la phase de paramétrage et jusqu'à la fin de l'exploitation opérationnelle, le public a ainsi reçu une information sur les évènements et les lieux où le dispositif IA était déployé :

- Des affiches relayant cette information, dont le visuel et le texte ont été élaborés en concertation avec la CNIL, ont été posées aux abords de chaque site d'expérimentation. Ces affiches faisaient notamment apparaître les cas d'usage testés et renvoyaient à un lien permettant l'exercice des droits garantis par le RGPD (cf. *infra*) ;
- L'information était explicitée sur les sites internet de chaque responsable de traitement. Son contenu a, lui aussi, été concerté avec la CNIL. Le QR-code figurant sur chaque affiche permettait au public d'y accéder aisément. Une information générale du public a également été diffusée sur le site internet du ministère de l'intérieur[93].

- Le ministre de l'intérieur a réalisé deux points presse, les 16 février et 14 mai 2024, pour fournir des précisions sur les avancées de la mise en œuvre de l'expérimentation.

4.1.2. Les modalités d'information spécifiques à chaque opérateur

▪ La préfecture de police a réalisé systématiquement une information de premier niveau via des affichettes au format A3 posées sur la voie publique (dont le contenu avait été validé au préalable par la CNIL)[94], ainsi qu'une information de deuxième niveau via le site internet de la préfecture.

[93] https://www.interieur.gouv.fr/actualites/actualites-du-ministere/securite-des-jeux-olympiques-des-operateurs-de-cameras-augmentes

[94] L'affichette a été réalisée selon le modèle de la SNCF, qui avait de l'avance dans le cadre du projet PREVENT.

40 affichettes ont ainsi été déployées (le nombre par site est fonction du nombre de caméras installées et du nombre d'accès aux sites).

PRÉFECTURE DE POLICE
Liberté
Égalité
Fraternité

EXPÉRIMENTATION VIDÉOPROTECTION AUGMENTÉE

VIDEOSURVEILLANCE ANALYSIS EXPERIMENT
EXPERIMENTACIÓN DE VIDEO ANÁLISIS

Afin de renforcer la sécurité de cet espace, la préfecture de Police est susceptible de mettre ponctuellement en œuvre, à titre expérimental, une analyse automatisée en temps réel des images de vidéoprotection sur lesquelles vous pouvez figurer.

Autorisée jusqu'au 31 mars 2025 par la loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques 2024, cette expérimentation alterne des phases d'étalonnage et de mise en œuvre des solutions logicielles d'analyse automatisée, à l'occasion de manifestations d'ampleur (concerts, manifestations sportives, etc.).

Elle vise à aider la Direction de l'ordre public et de la circulation et la Direction de la sécurité de proximité de l'agglomération parisienne à détecter :

- la présence d'objets abandonnés ;
- le non-respect par une personne ou un véhicule du sens de circulation commun ;
- le franchissement ou la présence d'une personne ou d'un véhicule dans une zone interdite ou sensible ;
- la présence d'une personne au sol à la suite d'une chute ;
- le mouvement de foule ;
- la densité trop importante de personnes ;
- les départs de feux.

Pour plus d'information concernant cette expérimentation :
For more information about this experiment:
Para más información sobre esta experimentación :

https://www.prefecturedepolice.interieur.gouv.fr/demarches/plan-de-videoprotection

Vous pouvez exercer vos droits auprès de donnees-personnelles-prefecturedepolice@interieur.gouv.fr

Par ailleurs, si vous considérez que le traitement vous concernant constitue une violation de la réglementation, vous disposez du droit d'introduire une réclamation auprès de la CNIL (commission nationale de l'informatique et des libertés), 3 place de Fontenoy – TSA 80715 – 75334 Paris Cedex 07 ; https://www.cnil.fr/fr/plaintes.

Réalisation : Direction de l'innovation, de la logistique et des technologies, préfecture de Police - février 2024

▪ La RATP a fait le choix de mettre en place des affiches pérennes dans chacune des principales stations de métro, avec un affichage à chaque entrée des gares et stations concernées, ainsi que sur les quais des stations desservies.

Expérimentation vidéoprotection augmentée

Videosurveillance analysis experiment
Experimentación de video análisis

Afin de renforcer la sécurité dans cette [station/gare], la RATP est susceptible de mettre ponctuellement en œuvre, à titre expérimental, une analyse automatisée en temps réel des images de vidéoprotection sur lesquelles vous pouvez figurer.

Autorisée jusqu'au 31 mars 2025 par la loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques 2024, cette expérimentation alterne des phases de paramétrage et de mise en œuvre des solutions logicielles d'analyse automatisée, à l'occasion de manifestations d'ampleur (concerts, manifestations sportives, etc.).
Elle vise à aider les agents du service interne de sécurité de la RATP à détecter des événements prédéterminés parmi les cas d'usage suivants : présence d'objets abandonnés, franchissement ou présence d'une personne ou d'un véhicule dans une zone interdite ou sensible, mouvement de foule, densité trop importante de personnes.

Cette aide automatisée à la détection est ensuite analysée par l'opérateur vidéo qui seul valide si le signalement est pertinent et s'il y a lieu de le transmettre aux services opérationnels.

Pour plus d'information concernant cette expérimentation ou pour l'exercice de vos droits auprès du Délégué à la protection des données de la RATP :

For more information about this experiment:
Para más información sobre esta experimentación:

https://www.ratp.fr/politique-generale-de-confidentialite

Par ailleurs, si vous considérez que le traitement vous concernant constitue une violation de la réglementation, vous disposez du droit d'introduire une réclamation auprès de la CNIL (commission nationale de l'informatique et des libertés) : 3 place de Fontenoy – TSA 80715 – 75334 Paris Cedex 07
https://www.cnil.fr/fr/plaintes.

Cet affichage précise les finalités du dispositif, les modalités de l'exercice des droits RGPD, et renvoie vers le site https://www.ratp.fr/politique-generale-de-confidentialite pour plus d'information.

Une information plus dynamique et plus explicative est détaillée sur ce site internet, avec le détail explicatif du fonctionnement du traitement algorithmique, les expérimentations en cours, leurs dates, ainsi que les gares et stations concernées.

▪ La SNCF a déployé 150 affiches de format A3 ou A4 dans les différentes gares concernées par l'expérimentation. Celles-ci ont été apposées aux entrées et sorties de ces gares et sur les quais.

Afin de renforcer la sécurité dans cette gare, la Direction de la Sûreté SNCF est susceptible de mettre ponctuellement en œuvre, à titre expérimental, une analyse automatisée en temps réel des images de vidéoprotection sur lesquelles vous pouvez figurer.

Autorisée jusqu'au 31 mars 2025 par la loi n°2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques 2024, cette expérimentation alterne des phases de paramétrage et de mise en œuvre des solutions logicielles d'analyse automatisée, à l'occasion de manifestations d'ampleur (concerts, manifestations sportives, etc.). Elle vise à aider les agents du service interne de sécurité de la SNCF à détecter des événements prédéterminés parmi les cas d'usage suivants :

- présence d'objets abandonnés,
- franchissement ou présence d'une personne ou d'un véhicule dans une zone interdite ou sensible,
- mouvement de foule,
- densité trop importante de personnes.

Le signalement est ensuite analysé par l'opérateur vidéo qui décide, seul, s'il est pertinent et s'il est nécessaire d'intervenir.

Pour plus d'information concernant cette expérimentation :
For more information about this experiment:
Para más información sobre esta experimentación:
http://sncf.com/fr/video-appels-surete

Vous pouvez exercer vos droits à l'adresse : sf.experimentations-video@sncf.fr

Par ailleurs, si vous considérez que le traitement vous concernant constitue une violation de la réglementation, vous disposez du droit d'introduire une réclamation auprès de la CNIL (commission nationale de l'informatique et des libertés), 3 place de Fontenoy – TSA 80715 – 75334 Paris Cedex 07 ; https://www.cnil.fr/fr/plaintes

▪ La commune de Cannes s'est dotée de panneaux de signalisation « en dur » sur le modèle des panneaux autoroutiers ; ils ont été déployés sur et autour des zones concernées. Ces panneaux comportaient les mentions légales et les dates de mise en œuvre des expérimentations.

Selon les responsables, le format offre de la visibilité mais présente aussi des inconvénients. Le premier d'entre eux est le coût de fabrication qui se surajoute au coût technique. L'obligation d'inscrire à chaque fois les dates imposait de les reproduire au gré des expérimentations.

Pour la seconde salve d'expérimentations (NRJ Music Awards, Marathon et marché de Noël), l'ensemble des dates ont pu être inscrites sur un même panneau. Cela a impliqué une organisation importante en amont, pour établir les dates de manière ferme (délibération en conseil municipal), mais a permis des économies substantielles pour la collectivité.

Une publication détaillée a également été faite sur le site internet de la commune[95].

4.1.3. Une information à améliorer

- Le choix d'une information spécifique, distincte de l'information prévue en ce qui concerne le recours à la vidéoprotection, doit être approuvé au regard des exigences légales ainsi que des spécificités du dispositif d'IA.

- L'absence d'apposition des affiches à l'emplacement précis des caméras équipées d'IA se justifie pour des considérations opérationnelles, en particulier le souci de prévenir d'éventuelles dégradations et le risque de remettre en cause l'efficacité de la détection automatique. Elle n'appelle pas de critique.

- En revanche, l'information fournie au public paraît, de façon générale, trop discrète pour garantir sa bonne compréhension.

Ainsi, le format des affiches, en particulier celles de format A4, était souvent trop petit pour les passants, de sorte qu'elles passaient souvent inaperçues, même pour les personnes informées

[95] https://www.cannes.com/fr/index/mentions-legales/experimentation-videoprotection-augmentee.html

de l'expérimentation. Les membres du comité l'ont constaté à de nombreuses reprises lors de leurs visites.

▪ En outre, la notion de « vidéoprotection augmentée » et le logo qui l'accompagnait étaient peu évocateurs et pas assez pédagogiques.

▪ Enfin, si l'expérimentation venait à être prolongée ou pérennisée, il pourrait être utile que les différents opérateurs organisent des réunions publiques de compte-rendu annuel sur la mise en œuvre du traitement.

4.1.4. De très faibles remontées du public qui interrogent

Les différents opérateurs ont tous constaté qu'en dépit de l'information ainsi organisée et de nombreux articles sur le sujet dans les médias nationaux, les remontées du public avaient été particulièrement faibles tout au long de l'expérimentation. Cette constatation se fonde sur le différentiel entre le nombre de demandes, bien plus important, lorsqu'il s'agit de vidéoprotection classique et leur faible taux lors de l'expérimentation.

Ainsi, par exemple, dans le cadre des Jeux olympiques, la SNCF n'a été saisie d'aucune demande d'exercice du droit d'accès ou même de demande d'information et seules 32 personnes ont vu la page internet consacrée à l'expérimentation.

Cela peut s'expliquer de deux façons :
- Soit les affiches d'information n'ont pas été vues, en raison de leur taille modeste et de leur manque de lisibilité (cf. supra) ;
- Soit, se sentant faiblement concerné ou par compréhension insuffisante quant à l'objet précis de l'expérimentation, le public n'a pas estimé nécessaire d'aller voir plus en détail la page d'information ou de formuler une demande d'exercice de droits.

4.2. L'association à l'expérimentation

4.2.1. Les réactions des associations, de la Défenseure des droits et du Conseil national des barreaux

▪ Plusieurs membres du comité se sont entretenus avec des représentants de l'association La Quadrature du Net le 3 juin 2024. Il en ressort une inquiétude particulière quant au cadre de l'analyse.

L'association insiste particulièrement sur la « logique de bac à sable » mise en œuvre, conduisant, selon elle, à « sortir le cadre de l'évaluation du protocole des libertés fondamentales ». Les Jeux olympiques constitueraient, selon elle, un « prétexte », fournissant l'occasion d'introduire en droit positif une telle technologie attentatoire aux libertés individuelles et dont l'efficacité serait dérisoire. La présente expérimentation révèlerait une forme d'hypocrisie en ce que la pérennisation du dispositif serait d'ores et déjà envisagée.

L'association s'inquiète, en particulier, de la possible collecte de données qui seraient, selon elle, susceptibles d'être qualifiées de biométriques, notamment la silhouette des individus.

Elle interpelle le comité quant au souci de ne pas restreindre l'analyse à une appréciation purement technique des systèmes, et la nécessité de prendre en compte des enjeux de société

(utilité et coût des systèmes, traitement de données « corporelles », mise en jeu des responsabilités)[96].

L'effet cliquet de l'adoption technologique est particulièrement redouté : il amorcerait le déploiement de systèmes hautement plus attentatoires à la vie privée à l'instar de la reconnaissance faciale et émotionnelle.

▪ Certains membres du comité se sont également entretenus, le 10 janvier 2025, avec une représentante de l'association Ligue des droits de l'Homme (LDH). Celle-ci a également déploré le fait que la présente expérimentation, dans le contexte des Jeux olympiques, contribuerait à renforcer l'acceptabilité de telles technologies auprès de la population, en dépit de leur caractère très intrusif et attentatoire aux libertés individuelles.

Selon l'association, le dispositif impliquerait bien le traitement de données biométriques, en ce qu'il permet d'identifier la démarche d'un individu (le rapport évoque cette question au point *5.2.2.*) et il constituerait une menace pour la liberté d'aller et venir et la liberté d'expression.

Sur le plan opérationnel, il existerait encore, selon elle, un risque que l'opérateur vidéo ne réponde aux injonctions de la machine, au lieu de chercher par lui-même à détecter les situations à risque. En outre, l'introduction de tels dispositifs pourrait conduire à réduire la présence humaine sur le terrain, ce qui irait, selon l'association, à l'encontre de l'objectif d'amélioration de la sécurité du public.

L'association s'interroge enfin sur la délégation de fonctions régaliennes à des entreprises ayant une activité de sécurité privée et sur l'existence de biais éventuels dans les applications fournies.

L'ensemble des critiques des associations La Quadrature du Net et LDH à l'encontre du dispositif se retrouvent dans leurs deux notes d'analyse reproduites en annexe n° 12.

▪ Ces vives réserves et inquiétudes rejoignent celles exprimées par la Défenseure des droits dans sa contribution reproduite en annexe n° 11.

▪ De même, le Conseil national des barreaux a également exprimé sa préoccupation quant aux possibles atteintes à la vie privée et au manque de garanties suffisantes, notamment en termes de transparence et de formation des agents impliqués[97].

▪ Enfin, des chercheurs français ont également analysé cette question (V. en particulier R. Chatellier[98] et G. Gormand[99]).

---

[96] Voir plus largement sa communication sur la question : LQDN, Jeux Olympiques : fichage de Masse et discrimination politique, 30 juillet 2024.

[97] Résolution du 21 mai 2024 sur la proposition de loi relative au renforcement de la sûreté dans les transports https://www.cnb.avocat.fr/fr/actualites/le-cnb-conteste-plusieurs-mesures-envisagees-dans-la-proposition-de-loi-visant-renforcer-la-surete

Résolution du 3 février 2023 : « Opposition au traitement algorithmique des images de vidéosurveillance, à l'extension de la procédure de criblage et aux dispositions pénales prévues par le projet de loi relatif aux Jeux olympiques et paralympiques de Paris 2024 ».

La vidéosurveillance automatisée aux JO et Jeux Paralympiques de 2024 inquiète la profession | Conseil national des barreaux

[98] Des premières caméras à l'expérimentation des algorithmes : un panorama du développement territorial, technologique et de l'encadrement juridique de la vidéosurveillance | Cairn.info

[99] Jeux olympiques de Paris : attention, on vous surveille | Radio-Canada

4.2.2. Les précédentes études visant à évaluer le degré de confiance du public dans le recours à l'intelligence artificielle en matière de vidéoprotection

▪ A l'étranger, plusieurs travaux réalisés par des universitaires ont cherché à évaluer la confiance du public à l'égard des dispositifs de vidéoprotection recourant à l'IA. Ils sont cependant, le plus souvent, tournés vers les technologies de reconnaissance faciale :

- Les travaux d'un institut britannique, l'Ada Lovelace Institute, qui évaluent la réception du public et les effets de bords de l'usage des technologies de reconnaissance faciale dans l'espace public (« chilling effect », opportunité en fonction des cas d'usages, confiance dans la technologie, évaluation du sentiment de sécurité)[100] ;
- Ceux de Ben Bradford, concernant la manière dont la confiance du public et la légitimité perçue influencent l'acceptation de la technologie de reconnaissance faciale par les forces de police[101] ;
- L'étude conduite par Pete Fussey et Dr Daragh Murray visant à mesurer la confiance du public lors des essais de reconnaissance faciale en temps réel réalisés par la London Metropolitan Police[102].

▪ En France, plusieurs études réalisées par des instituts de sondage ont cherché à évaluer le niveau général d'acceptabilité du recours à de tels traitements.

Tel est le cas, en particulier, des deux études suivantes :

- Étude sociétale Opinionway réalisée du 18 au 26 juillet 2022, à la demande de la SNCF ;
- Étude du Continuum Lab de septembre 2024, effectuée avec OpinionWay[103].

Ces différentes études font apparaître qu'une nette majorité de la population approuve le recours aux traitements algorithmiques aux fins d'assurer la sécurité publique, sans être pour autant insensible aux risques pour les libertés publiques.

Il ressort ainsi de l'étude de septembre 2024 que 65 % des personnes sondées se disent favorable à l'utilisation de l'IA par les forces de sécurité intérieure et 63 % souhaitaient la généralisation de l'expérimentation actuellement en cours[104].

▪ Doit enfin être signalée, dans le cadre de la présente expérimentation, la très intéressante étude réalisée par des étudiants de l'Incubateur de politiques publiques de Sciences Po en lien avec la CNIL (cf. annexe n° 13). Ceux-ci ont se sont entretenus, lors des premiers tests, avec 40 usagers de la SNCF.

Il en ressort un manque général de connaissance des droits en matière de protection de données personnelles, une difficulté à comprendre le fonctionnement des caméras de surveillance algorithmique et leur différence avec les dispositifs de reconnaissance biométrique et de reconnaissance faciale et une inefficacité des dispositifs d'information actuels dans l'espace public.

---

[100] Ada Lovelace Institute, Beyond Face Value: Public Attitudes to Facial Recognition Technology, 2019.
[101] BRADFORD et al., "Live Facial Recognition: Trust and Legitimacy as Predictors of Public Support for Police Use of New Technology", *British Journal of Criminology*, 2020.
102 FUSSEY, P. and MURRAY, D. (2019), Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology. 16 Sep 2019.
[103] https://www.continuumlab.fr/wp-content/uploads/2024/09/ENQUETE-TECHNO_4PAGES.pdf
[104] Contre 21 % d'un avis contraire et 16 % qui ne se prononcent pas.

4.2.3. L'étude quantitative et qualitative réalisée par le comité d'évaluation

▪ Dans le cadre de la présente évaluation de l'expérimentation, et comme le prévoyait le décret, le comité a fait le choix, avec le soutien du ministère de l'intérieur, d'organiser une étude spécifique, confiée à un cabinet indépendant, la société Verian (ex TNS Sofres), centrée sur les caractéristiques particulières du traitement qu'il appartient au comité d'évaluer. A savoir un traitement ne recourant pas à la reconnaissance faciale, portant exclusivement sur des cas d'usage précisément définis et qui ne peut être mis en œuvre que par des personnes publiques.

Cette étude (en annexe n° 9 du présent rapport) comportait deux volets :
- Un volet quantitatif, portant sur un échantillon de 1 005 personnes représentatif de l'ensemble de la population (enquête réalisée sur internet du 3 au 5 décembre 2024) ;
- Un volet qualitatif, réalisé à partir d'entretiens de 2h30 dans le cadre, chacun, de trois « focus-groupes », en présentiel, la semaine du 2 décembre 2024, à Paris et à Marseille[105].

Il est à noter que les entretiens ont été animés par un représentant du cabinet indépendant et que plusieurs membres du comité d'évaluation ont assisté à celui qui a été organisé à Paris.

▪ Les résultats du volet quantitatif font apparaître les éléments suivants.

90 % des personnes interrogées adhèrent très largement à l'usage de la vidéoprotection dans l'espace public pour lutter contre la délinquance et une sur deux y est même « tout à fait » favorable (en particulier les plus âgés).

Les personnes interrogées se montrent très largement ouvertes au recours à l'utilisation de caméras de surveillance s'appuyant sur l'intelligence artificielle, que ce soit pour repérer une situation à risque, sans pouvoir reconnaître une personne déterminée ni identifier ses caractéristiques physiques (81 % y sont favorables) ou pour reconnaître une personne déterminée ou identifier certaines de ses caractéristiques physiques sur les images analysées (76 % de favorables). Dans les deux cas, environ 40 % de la population testée s'y dit même tout à fait favorables.

Une grande majorité des personnes interrogées se sentirait également « beaucoup plus en sécurité » et « parfaitement à l'aise et libre » en présence d'un tel dispositif et ce quel que soit le contexte d'usage (par la police, les réseaux de transports ou les compagnies privées).

En dépit de cette approbation générale, la population testée identifie toutefois des dérives potentielles : une majorité pense ainsi que cela va banaliser la surveillance générale via le recours à l'IA (à 62 %), mais aussi que cela risque d'être mal utilisé (59 %), ou encore que cela pourrait entraîner des discriminations (54 %).

Les réticences sont ainsi un peu plus marquées pour un usage éventuel, non retenu dans le cadre de l'expérimentation actuelle, dans les écoles, sur les lieux de travail, et plus globalement par des acteurs privés.

Par ailleurs, interrogée sur les priorités pour garantir la sécurité publique, la population testée cite en premier l'augmentation du nombre de policiers/gendarmes sur la voie publique (38 %)

[105] Groupe 1 (CSP+, à Paris ; Groupe 2 (CSP-, à Marseille) ; Groupe 3 (Jeunes, à Marseille)

et le recrutement de personnes spécialisées dans les nouveaux types de risques (28 %), bien devant l'investissement dans la vidéo équipée d'IA (18 %).

Enfin, 61 % de la population testée dit avoir entendu parler de l'expérimentation de la vidéosurveillance assistée par IA mise en place dans le cadre des Jeux olympiques, mais seulement une personne interrogée sur cinq déclare savoir précisément de quoi il s'agit. D'où l'importance qui s'attache à mieux communiquer sur ce que la loi autorise et sur l'objet du traitement.

- Le volet qualitatif de l'étude permet de corroborer et d'affiner ces différents constats. Malgré certaines réserves exprimées (crainte d'une surveillance généralisée, d'une diminution des libertés ou de détournements à des fins économiques…), la plupart des personnes ayant participé aux « focus-groupes » acceptent facilement d'être surveillés dans l'espace public, dans la mesure « où l'on n'a rien à se reprocher ».

Les dispositifs de traitements algorithmiques, de même que la présente expérimentation, sont fréquemment associés à la reconnaissance faciale ainsi qu'aux analyses liées aux densités de personnes et de mouvements de foule.

Concernant les traitements ne recourant ni à la reconnaissance faciale ni à l'usage de données biométriques, les participants voient assez peu d'impacts négatifs à ces dispositifs pour eux-mêmes : la vidéosurveillance étant déjà une réalité quotidienne et « entrée dans les mœurs », le recours à l'IA ne leur semble pas constituer un changement majeur mais éventuellement la promesse d'une efficacité accrue des dispositifs de surveillance (qui est aujourd'hui souvent questionnée).

Les principales inquiétudes qui s'expriment néanmoins portent sur les risques de détournement de ces dispositifs à des fins commerciales ou de suivi de productivité et de contrôle des salariés. Ces dispositifs, s'ils venaient dans le futur à être introduits dans ces secteurs, seraient avant tout perçus comme des outils de surveillance et non de protection, en ce que la caméra n'empêche pas, par elle-même, la survenue des risques, contrairement à une présence humaine sur le terrain.

Au-delà de l'expérimentation, et selon la question posée d'initiative par le sondeur, si l'usage de la reconnaissance faciale suscite certes certaines craintes (liées notamment à son usage en Chine pour contrôler la population), beaucoup y voient également un outil utile pour faciliter la recherche, l'identification et l'arrestation de personnes recherchées ou criminelles, sous réserve qu'il soit limité aux questions essentielles de sécurité et encadré pour éviter toute dérive.

5. Un dispositif expérimental qui, en l'état, ne heurte les libertés publiques ni dans sa conception ni dans sa mise en œuvre

Le comité, et tout particulièrement le collège des personnalités qualifiées, s'est montré particulièrement attentif, dans le cadre de ses investigations et de ses réflexions, au respect par le traitement algorithmique expérimenté des libertés publiques. Il n'a pas relevé d'atteinte aux exigences posées par la Constitution, le droit de l'Union européenne ou le cadre légal et règlementaire mais souligne néanmoins les enjeux qui s'attachent à un contrôle très attentif de la mise en œuvre d'un tel outil, afin notamment de prévenir toute éventualité de détournement de ses finalités légales ou de biais discriminatoires dans son utilisation.

5.1. Conformité aux prescriptions légales et réglementaires

5.1.1. Un respect des différentes exigences procédurales globalement satisfaisant

Comme le prévoyaient la loi du 19 mai 2023 et le décret du 28 août 2023, la mise en œuvre du traitement a fait l'objet d'autorisations préalables du préfet de police, d'AIPD et d'engagements de conformité.

En revanche, en une occasion, il est arrivé que les autorisations requises ne soient délivrées que très tardivement et qu'elles ne soient publiées au recueil des actes administratifs qu'après le début de la mise en œuvre des traitements. En effet, comme le relève la Défenseure des droits dans ses observations transmises au comité, l'arrêté du préfet de police autorisant le traitement pour le début des épreuves olympiques a été pris la veille de la cérémonie d'ouverture, le 25 juillet, mais il n'a été publié que cinq jours plus tard.

La préfecture de police, tout en regrettant ce retard, a précisé qu'il s'agissait d'un dysfonctionnement interne dans une période de très forte activité, alors même que l'arrêté préfectoral avait bien été signé dans les temps, et qu'elle a ensuite veillé à ce que cette situation ne se reproduise pas. L'effectivité du recours au juge ne s'en est pas moins trouvée affectée.

5.1.2. Le respect des conditions de fond posées par la loi

Le comité n'a constaté aucune mise en œuvre des traitements au-delà du cadre défini par la loi, tant en ce qui concerne les évènements et sites concernés que les différents cas d'usage.

Dans le doute, l'opérateur s'abstenait. Ainsi la RATP s'est refusée à tester le dispositif dans une station fermée, avec du personnel de l'établissement pour observer la capacité du logiciel sur les mouvements de foules, dans l'incertitude de la légalité d'une telle opération.

De même, comme il a été dit, la préfecture de police n'a pas recouru à l'IA pour identifier les possibles auteurs d'actes de malveillance sur des câbles optiques, lors des épreuves olympiques à Versailles, dans le doute sur une telle possibilité dans le cadre légal actuel. C'est finalement l'intelligence humaine, qui, en visionnant les images des caméras, a identifié la source du problème (qui était en fait une fouine).

5.1.3. Le respect des exigences de confidentialité des données conservées

▪ Le comité n'a constaté aucune méconnaissance de l'exigence légale portant sur la durée de conservation, qui doit être limitée à ce qui est strictement nécessaire et, dans tous les cas, à moins de douze mois.

En ce qui concerne la préfecture de police, la durée maximale de conservation des images est, conformément aux dispositions de l'article L. 252-5 du code de la sécurité intérieure relatives à la vidéoprotection, de 30 jours, un délai supérieur n'étant, au demeurant, pas compatible avec la capacité de stockage[106].

En ce qui concerne la RATP, les enregistrements ne sont conservés que 24 heures. Les métadonnées sont, quant à elles, pendant 72 heures, durée susceptible d'être portée à huit jours (cette limite étant posée pour des raisons techniques, en lien avec la capacité du serveur).

En ce qui concerne la SNCF, l'interconnexion des traitements au système vidéo d'Ile de France permet d'éviter l'enregistrement d'images supplémentaires en dehors de ce système. Les opérateurs utilisent ainsi uniquement leur système vidéo utilisé quotidiennement et peuvent accéder à l'ensemble des 11 000 caméras et des quatorze jours d'enregistrements du système vidéo de production.

En ce qui concerne la commune de Cannes, les images du centre de vidéoprotection sont conservées trente jours sur les serveurs, conformément à l'autorisation préfectorale délivrée.

▪ L'article 16 du décret du 28 août 2023 prévoit, par ailleurs, que : « *Les opérations de collecte, de consultation, de communication, de modification et d'effacement des données à caractère personnel et informations traitées, ainsi que les signalements générés par les traitements font l'objet d'un enregistrement. Les journaux des opérations de consultation et de communication permettent d'établir le motif, la date et l'heure de ces opérations et les personnes en étant à l'origine. Ces journaux sont conservés douze mois. Le responsable du traitement tient un registre des suites apportées aux signalements effectués par le traitement ainsi que le nom et le prénom des personnes ayant accès aux signalements* ».

La tenue de tels documents a bien été constatée en ce qui concerne la préfecture de police[107], la RATP, la SNCF et la commune de Cannes.

▪ Au-delà du respect de la réglementation, certaines bonnes pratiques en matière de confidentialité et de cybersécurité méritent d'être soulignées.

Citons en particulier la mise en place de :
- Processus spécifiques de gestion des salariés et des agents du prestataire habilités à accéder aux données ;
- Mécanismes de sauvegarde des données ;

[106] La préfecture a fait le choix d'une infrastructure de stockage dédiée à l'IA, qu'il a fallu réévaluer en cours d'expérimentation car une saturation a été observée.
[107] Concernant la préfecture de police, le service réalisant l'expérimentation a été doté d'un registre à tenir. Afin de rendre la tenue de ce registre compatible avec les exigences opérationnelles, une déclinaison sous forme d'un fichier Excel par expérimentation a été réalisée. C'est notamment sur cette base que les statistiques ont pu être réalisées pendant les Jeux paralympiques.

- Règles d'authentification fortes pour l'accès aux traitements et des profils spécifiques à chaque type d'utilisateurs (opérateur vidéo, administrateur SNCF, fournisseur) ;
- Dispositifs de protection des réseaux et des matériels (firewall, antivirus) ;
- Mesures de traçabilité des accès logiciel ;
- Mesure de contrôle d'accès aux locaux ;
- Mesures destinées à prévenir tout transfert de données en externe.

▪ Dans le cas de l'expérimentation à Cannes, certaines difficultés ont été observées lors de la première expérimentation en ce qui concerne le respect des exigences de confidentialité. Ainsi, par exemple, les agents ne disposaient pas de « logs personnels », leur attribution n'ayant pas été prévue par le prestataire. Ces éléments ont été ajustés par la suite.

Ce constat appelle à une vigilance particulière de la part des acteurs publics, qui doivent s'assurer que les prestataires répondent bien aux exigences qui leur sont imposées par les textes en matière de traçabilité des données, de protection des données individuelles et de cybersécurité.

5.2. Un dispositif soumis aux exigences du RGPD et de la législation CNIL

5.2.1. L'applicabilité du RGPD et de la loi CNIL au dispositif IA

▪ Le RGPD et la loi CNIL s'appliquent aux traitements de données à caractère personnel.

Le 1 de l'article 4 du RGPD qualifie ainsi « *toute information se rapportant à une personne physique identifiée ou identifiable* ». Une personne est réputée identifiable lorsqu'elle « *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* ».

La jurisprudence du Conseil d'Etat, rendue au sujet de l'utilisation de drones dans l'espace public, qualifie de traitement de données à caractère personnel, au sens du RGPD et de la loi CNIL, la collecte d'images susceptibles de comporter des données identifiantes aux fins de les transmettre à des opérateurs vidéo pour leur visionnage en temps réel et leur utilisation en vue de la réalisation de missions de police administrative[108]

La Cour de justice de l'Union retient, de même, que l'image d'une personne enregistrée par une caméra constitue une donnée à caractère personnel dans la mesure où elle permet d'identifier la personne concernée[109]. Les données sont considérées comme étant à caractère personnel dès lors que le responsable de traitement dispose de moyens raisonnables pour identifier les personnes concernées par celles-ci[110], que les informations permettant d'identifier la personne soient détenues par le responsable du traitement ou par une autre personne[111]. L'analyse des moyens doit se faire au regard des « *facteurs objectifs, tels que le coût de l'identification et le*

[108] JRCE, 18 mai 2020, Association La quadrature du net, n°440442, 440445, C ; CE, 10/9 CHR, 22 décembre 2020, Association La quadrature du net, n°446155, B.
[109] CJUE, 11 décembre 2014, Ryneš, C- 212/13, point 224 ; 14 février 2019, Buivids, C-345/17, point 315.
[110] Considérant 26 du RGPD.
[111] CJUE, 19 octobre 2016, Breyer, C 582/14, para. 43.

temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci »[112].

▪ Dans son avis de juillet 2022 précité, la CNIL en a déduit que « *même dans le cas où les images recueillies au moyen de l'IA sont anonymisées, voire détruites, très rapidement après leur captation et analyse, ces opérations constituent un traitement de données à caractère personnel si les images contiennent des personnes* ». Les dispositions du règlement et de la loi applicables en matière de protection des données personnelles leur sont bien applicables.

Les métadonnées conservées par le traitement IA (date de la détection, le numéro de la caméra et le type d'évènement identifié) constituent ainsi des données à caractère personnel tant que les images correspondantes sont conservées.

En revanche, elles ne le sont plus, en principe, à partir du moment où ces images ont été supprimées.

Seul devrait, peut-être, être réservé le cas particulier où un individu serait interpellé dans un lieu donné grâce à une alerte par les traitements algorithmiques – l'alerte peut alors être reliée à une personne déterminée, ce qui pourrait justifier que cette dernière ait accès à ces données[113].

5.2.2. Une question de principe : les données peuvent-elles être qualifiées de biométriques ?

▪ La diversité des données biométriques est soulignée par les commentateurs. Dans son *Cyberdroit*, Me Christiane Feral-Schuhl écrit que « *les dispositifs biométriques regroupent l'ensemble des techniques qui permettent d'identifier une personne à partir d'une caractéristique physique ou biologique : l'ADN, la rétine, l'iris, l'empreinte digitale, la reconnaissance faciale, la géométrie du contour de la main, la voix…). Elle permet également de mesurer les caractéristiques comportementales, par exemple la vitesse de frappe du clavier ou encore le timbre de la voix* ».

▪ En vertu du 14 de l'article 4 du RGPD, les données biométriques sont « *les données à caractère personnel (…), relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques* ».

La CNIL définit, quant à elle, les données biométriques comme toutes données « *regroupant des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques voire comportementales. Elles sont des données à caractère personnel car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN, empreintes digitales, etc)* ».

Dans sa décision sur la loi du 19 mai 2023, le Conseil constitutionnel définit les données biométriques comme celles « *relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique qui permettent ou confirment son identification unique* ».

[112] Considérant 26 du RGPD.

[113] V. CJUE, 20 septembre 2022, C-793/19 : rappel de l'interdiction de conservation et indifférenciée des métadonnées.

L'article 9 du RGPD pose le principe de l'interdiction du traitement de telles données, dont en posant, en son paragraphe 2, différentes exceptions, en particulier (g) si « *le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée* ».

Cette interdiction de recueil des données biométriques est reprise à l'article 10 de la loi du 19 mai 2023.

- Ainsi que l'exigent la loi et le décret, aucune donnée biométrique, ni même d'ailleurs de données identifiantes (par ex., couleur d'un vêtement), ne sont utilisées dans l'algorithme de détection.

Peut-on y assimiler le repérage d'une silhouette ? Le simple fait que l'outil permette ensuite aux opérateurs humains de signaler son comportement et que ceux-ci soient ensuite en mesure de la retrouver par l'examen des autres caméras est-il licite ? Ce point est contesté mais le comité a retenu à ce stade une réponse affirmative.

Dans son avis sur le projet de loi, le Conseil d'Etat notait[114] que « *les traitements ne collectent ni n'utilisent aucune donnée biométrique et ne peuvent, en particulier, recourir à la reconnaissance faciale* ». Le Sénat va dans le même sens[115].

De même, les systèmes ne permettent en aucun cas une identification comportementale ou émotionnelle. Les cas d'usage retenus par le décret, et tels que déployés sur le terrain, excluaient tout recueil de données portant sur la démarche, les émotions, ou encore la température corporelle.

5.2.3. Le respect du principe de minimisation

En application du principe de minimisation des données posé au c) de l'article 5.1. du RGPD, les données personnelles doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* ».

En l'espèce, il apparaît que les diligences mises en œuvre par les différents opérateurs dans le cadre de l'expérimentation permettent d'assurer le respect de ces exigences.

D'une part, le périmètre de l'expérimentation est encadré tant par son objet que par sa durée. Les différents opérateurs ont, comme il a été dit, mis en œuvre le traitement sur un nombre limité de caméras et sur des sites qui étaient au nombre de ceux où la mise en place du traitement était autorisée par le décret.

D'autre part, la durée de conservation des données est limitée à ce qui est nécessaire pour exploiter le dispositif (cf. *supra*). Aucune métadonnée relative aux éléments automatiquement détectés dans les images n'est conservée par les algorithmes ou n'est transmise aux utilisateurs. Les seules métadonnées conservées sur les serveurs d'analyse sont les informations relatives aux signalements générés (date, heure, caméra concernée et évènement détecté) ainsi que les données relatives au paramétrage des analyses (zones et seuils de détection).

[114] Au point 24.
[115] Cf. le rapport n°248 de Mme Canayer sur le projet de loi (art 7).

5.2.4. Droit d'accès aux données personnelles

▪ Les opérateurs ont mis en œuvre le droit d'accès aux données personnelles garanti par le RGPD, auquel renvoie l'article 17 du décret du 28 août 2023. La mise en œuvre de ce droit s'avère cependant délicate.

Saisi d'une demande, le responsable du traitement doit d'abord identifier le demandeur dans les enregistrements vidéo disponibles, au vu des informations que ce dernier lui transmet (date, heure, localisation, tenue vestimentaire, photo, pièce d'identité). Cette recherche doit être effectuée manuellement par un agent habilité et être réalisée pendant la durée de conservation des images de vidéoprotection (qui est celle habituellement prévue, indépendamment de tout recours à l'IA).

S'il parvient à procéder à cette identification, il doit ensuite extraire la séquence vidéo correspondante et l'anonymiser afin de supprimer toutes les données personnelles des tiers présents sur les images. Cela peut être très complexe, en particulier en cas de forte affluence.

La SNCF fait état de 11 demandes d'exercice de droits, notamment à l'occasion des premières expérimentations (cf. *supra*) : 24 séquences ont dû être anonymisées pour un total de trois demandes auxquelles il a été répondu positivement. Les autres demandes n'ont pu être satisfaites, soit parce que les gares n'étaient pas concernées par l'expérimentation, soit parce que les éléments transmis n'étaient pas suffisants pour permettre d'identifier le demandeur.

La RATP n'a reçu, quant à elle, que trois demandes d'accès. Il s'est cependant avéré qu'aucun des demandeurs n'avait fait l'objet d'une détection par le traitement.

Enfin, aucune demande d'accès n'a été effectuée auprès de la commune de Cannes, et ce pour l'ensemble des manifestations concernées.

▪ Des améliorations seraient possibles. Le comité observe, à cet égard, que certains opérateurs (la RATP, en particulier) ont fait le choix de ne visualiser que la seule personne (seule donnée personnelle) en occultant, alors même que ce n'était pas légalement requis, tout l'environnement, même lorsqu'il ne faisait pas apparaître de tiers.

La préfecture de police a, quant à elle, l'expérience du traitement des demandes d'accès via le PVPP.

5.2.5. Droit d'opposition, de modification et d'effacement

En vertu du IV de l'article 17 du décret du 28 août 2023 (base légale nécessaire en vertu de l'article 23 du RGPD), le droit d'opposition ne s'applique pas aux traitements algorithmiques faisant l'objet de la présente expérimentation.

Le droit à la modification équivaut en pratique à un droit à l'effacement.

En ce qui concerne le droit d'effacement, celui-ci est difficile à mettre en œuvre. Il ne ressort pas des éléments recueillis qu'un dispositif vidéo d'anonymisation n'est aujourd'hui certifié ou labellisé afin de garantir l'irréversibilité du traitement d'anonymisation. Les opérateurs observent ainsi que les opérations d'anonymisation peuvent ainsi être très chronophages.

5.3. La question de la conformité du dispositif au règlement européen sur l'IA

▪ La conformité du dispositif règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (« règlement IA ») paraît pouvoir être admise.

▪ Pour toutes les IA, le règlement IA pose, à l'article 4, un principe de maîtrise de l'IA : les fournisseurs et les déployeurs de systèmes d'IA sont tenus de prendre « *des mesures pour garantir, dans toute la mesure du possible, un niveau suffisant de maîtrise de l'IA pour leur personnel et les autres personnes s'occupant du fonctionnement et de l'utilisation des systèmes d'IA pour leur compte, en prenant en considération leurs connaissances techniques, leur expérience, leur éducation et leur formation, ainsi que le contexte dans lequel les systèmes d'IA sont destinés à être utilisés, et en tenant compte des personnes ou des groupes de personnes à l'égard desquels les systèmes d'IA sont destinés à être utilisés* ».

Le règlement définit la « *maîtrise de l'IA* » comme les « *compétences, les connaissances et la compréhension qui permettent aux fournisseurs, aux déployeurs et aux personnes concernées, compte tenu de leurs droits et obligations respectifs dans le contexte du présent règlement, de procéder à un déploiement des systèmes d'IA en toute connaissance de cause, ainsi que de prendre conscience des possibilités et des risques que comporte l'IA, ainsi que des préjudices potentiels qu'elle peut causer* » (article 3, pt 56).

En l'espèce, le droit national reprend ces exigences. L'article 10 de la loi pose ainsi un « *principe de primauté humaine, assurant qu'à tout instant le traitement ne fonctionne que sous la supervision des personnes qui le mettent en œuvre* ».

▪ L'article 6 du règlement IA encadre par ailleurs, de façon spécifique, les traitements considérés comme étant « à haut risque ».

Il pourrait être considéré que le présent traitement répond bien à cette qualification, en ce qu'il pourrait relever du point 6 de l'annexe III, auquel renvoie le paragraphe 2 de l'article 6 :
« *Répression, dans la mesure où leur utilisation est autorisée par le droit de l'Union ou le droit national applicable*
a) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives ou en leur nom <u>pour évaluer le risque qu'une personne physique devienne la victime d'infractions pénales</u> ;
d) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives pour évaluer le risque qu'une personne physique <u>commette une infraction</u> ou récidive, sans se fonder uniquement sur le profilage des personnes physiques visé à l'article 3, paragraphe 4, de la directive (UE) 2016/680, ou pour évaluer les traits de personnalité, les caractéristiques ou les antécédents judiciaires de personnes physiques ou de groupes »[116].

[116] Il est plus douteux qu'il entre dans le champ du point 2 de l'Annexe III sur les infrastructures critiques en ce sens qu'il serait un « *système d'IA destiné à être utilisé en tant que composants de sécurité dans la gestion et l'exploitation d'infrastructures numériques critiques, du trafic routier ou de la fourniture d'eau, de gaz, de chauffage ou d'électricité* ».

Toutefois, il résulte de l'article 6.3 que la qualification de traitement à haut risque ne peut être retenue que si le traitement présente un « *risque important de préjudice pour la santé, la sécurité ou les droits fondamentaux des personnes physiques* ».

Un tel risque devra être exclu, en vertu de ces mêmes dispositions, s'il n'a pas « *d'incidence significative sur le résultat de la prise de décision* », et en particulier s'il est destiné à accomplir une tâche procédurale étroite, à améliorer le résultat d'une activité humaine préalablement réalisée ou à détecter les constantes en matière de prise de décision ou les écarts par rapport aux constantes habituelles antérieures et n'est pas destiné à se substituer à l'évaluation humaine préalablement réalisée, ni à influencer celle-ci, sans examen humain approprié.

En l'espèce, le traitement mis en œuvre, qui n'autorise pas la reconnaissance faciale, paraît devoir être regardé comme destiné à « *améliorer le résultat d'une activité humaine préalablement réalisée* ». Il ne relèverait donc pas de la qualification d'IA à haut risque.

A noter que si une telle qualification devait néanmoins être retenue, cela impliquerait de respecter des exigences de système de gestion des risques, de gouvernance des données, de documentation technique, d'enregistrement, de transparence et fourniture d'informations aux déployeurs, de contrôle humain, d'exactitude, robustesse et cybersécurité, ainsi que de formation. On relèvera que la loi reprend déjà assez largement ces exigences.

5.4. Enjeux plus généraux sur les libertés publiques

5.4.1. Le principe de liberté d'aller et venir

Le recours à l'intelligence artificielle en matière de vidéoprotection soulève la question de l'éventuelle atteinte au principe de liberté d'aller et venir, en lien avec l'effet dissuasif qui en résulterait pour l'accès aux lieux et évènements concernés.

De nombreuses études, notamment des rapports des Nations Unies, évoquent ainsi le « chilling effect », défini comme le fait dissuader l'exercice légitime de certains droits par la menace d'une sanction légale.

La Défenseure des droits s'est, entre autres, interrogée sur un tel risque en lien avec la mise en œuvre de dispositifs de surveillance très étendue.

Les traitements algorithmiques faisant l'objet de la présente expérimentation ne permettent certes pas d'identifier une personne, mais une fois le fait à risque détecté (pénétration dans une zone non autorisée, port d'arme à feu…), les opérateurs qui disposent d'un maillage de caméras suffisants pourraient suivre à l'œil humain l'individu qui en est à l'origine en basculant sur le dispositif de vidéoprotection classique en jonglant de caméra en caméra. Il en est ainsi, en particulier, dans les transports en commun.

La réalité d'un tel effet dissuasif est contestée par les utilisateurs. Ainsi, selon la SNCF, le traitement algorithmique n'aurait aucun impact spécifique sur la liberté d'aller et venir. Au contraire, il faciliterait la gestion des flux de voyageurs ou sur l'évitement de situations perturbées et aurait un effet positif sur le sentiment de sécurité.

Le comité n'a pas été en mesure de mettre en évidence que la présente expérimentation, dans le contexte dans lequel elle a été réalisée, aurait eu des effets dissuasifs sur la liberté de circulation. Rien n'indique non plus, à l'inverse, qu'elle aurait eu un impact positif à cet égard.

Les résultats de l'enquête précitée réalisée par la société Verian suggèrent que la grande majorité des usagers n'a pas été affectée dans ses déplacements par l'information de la mise en œuvre d'un tel traitement (cf. *supra*).

5.4.2. Le respect des finalités légales

Ainsi qu'il a été dit, la mise en place des caméras équipées de traitements algorithmiques ne se justifie qu'à des fins de lutte contre le terrorisme et de protection de la sécurité physique des personnes.

S'il existe une possibilité d'utiliser le traitement algorithmique à d'autres fins que celles légalement prévues (exploitation du service, surveillance de certains agents, etc.), le comité n'a constaté aucun manquement sur ce point et aucun ne lui a été remonté par des tiers (association, syndicat, etc).

Les différents utilisateurs soulignent tous que leur politique est très stricte à ce sujet. La RATP, par exemple, s'est engagée à ne pas faire usage des images ainsi recueillies à des fins disciplinaires.

Dans certains cas, il est vrai que le recours au traitement IA conformément à ces finalités légales peuvent conduire les opérateurs à repérer des comportements qui justifient une intervention, même en l'absence de risque terroriste ou d'atteinte à la sécurité des personnes.

Ainsi, la détection de la pénétration dans une zone non autorisée de la RATP ou de la SNCF pourrait conduire à interpeller les auteurs de tags. De même, la mise en évidence d'une densité anormale d'individus pourrait être utile aux fins de fluidifier la circulation des usagers, même en l'absence de risque sécuritaire identifié.

De tels usages du traitement algorithmique ne sont pas proscrits, sous réserve que la mise en place d'une caméra équipée d'IA à cet endroit se justifie bien par les enjeux en matière de terrorisme et de sécurité des personnes. Dans l'exemple précité, cette caméra ne doit pas avoir été mise en place dans le but d'identifier les auteurs de tags – il s'agirait alors d'un détournement des finalités du dispositif.

Cependant, si, à l'occasion de la recherche des pénétrations en zone proscrite, un intrus venait pour taguer, la caméra avec traitement algorithmique signalerait l'entrée dans la zone proscrite (par exemple, une zone de garage des voitures de métro). En même temps, la caméra algorithmique reste une caméra et elle peut entraîner une intervention anti-tag.
En revanche, la caméra algorithmique ne saurait permettre, incidemment, de contrôler les allers et venues et les temps de repos des agents d'une entreprise de transport.

5.4.3. Le principe de non-discrimination

- Les systèmes algorithmiques sont tributaires des données envoyées par les caméras et de la décision d'un opérateur de placer une zone de détection sur telle ou telle partie d'une image. Une observation spécifique de certaines caméras ou de certaines zones de certaines

caméras pourrait mener à une observation excessive de certaines catégories de personnes. Tel serait le cas, par exemple, si la détection par IA n'était placée que sur une seule tribune d'un stade, par exemple afin de cibler un public plus jeune ou plus populaire.

Un tel biais pourrait également se retrouver, pour les transporteurs, dans le choix des stations de métro ou des gares choisies, ou encore dans le choix du type d'objet abandonné qu'il serait demandé de détecter. Il a notamment été constaté que dans les gares, le traitement était susceptible d'assimiler les personnes assises à côté de bagages à des objets, ce qui pourrait conduire à cibler davantage les sans domicile fixe, si le traitement venait à être détourné de ses finalités légales.

La Défenseure des droits évoque, à cet égard, dans sa contribution, le risque de biais discriminatoires involontairement intégrés aux systèmes et non détectés ou non suffisamment évités (par ex. systèmes qui assimileraient des équipements nécessaires à des personnes en situation de handicap à des objets non autorisés) ainsi que le risque de biais volontaires (par ex. utiliser l'IA pour localiser les groupements de personnes statiques dans les quartiers populaires).

Elle relève cependant que la limitation du nombre de cas d'usage permet de prévenir ce risque.

Evoquant les biais de confiance des utilisateurs de systèmes, elle s'interroge sur la marge de manœuvre réelle dont les agents disposent après avoir reçu les signalements d'attention et sur la formation reçue sur ces différents biais.

- Les différents utilisateurs contestent l'existence de tels biais dans leur mise en œuvre du traitement, que ce soit lors de la phase de calibrage ou pendant les phases opérationnelles. Ainsi par exemple, tous types d'individu sont détectés en cas d'intrusion, à commencer par les personnels de l'entreprise elle-même (par ex. dans les tunnels de la RATP).

La SNCF souligne que des mesures techniques permettent de limiter un tel risque ainsi que le détournement éventuel des finalités. Il en est ainsi de la limitation de l'administration des traitements aux seules équipes d'administrateurs (encadrement), sans que les patrouilleurs vidéo ne puisent modifier les paramétrages techniques. Un opérateur vidéo ne pourrait configurer la mise en œuvre d'un traitement dans une zone spécifique en en détournant la finalité. Elle rappelle également l'importance qui s'attache à la réalisation d'une sensibilisation éthique. Enfin, les mesures de traçabilité déployées doivent permettre la réalisation d'audits réguliers afin de vérifier la bonne utilisation des traitements.

La RATP souligne également qu'aucun biais n'a été constaté à ce stade et le comité n'en a pas davantage identifié dans le cadre des investigations réalisées. Le dispositif a été testé dans des lieux de nature différente en lien avec des manifestations sportives ou culturelles d'ampleur, nécessitant un déploiement opérationnel spécifique. Ainsi, aucune catégorie de population n'a été visée. Il en est de même en ce qui concerne le choix des caméras sélectionnées à cette fin.

Si, au regard des spécificités sociologiques du tissu urbain francilien, un choix discriminatoire de gares et stations est, en théorie, possible (les stations Bir Hakeim et Porte d'Aubervilliers ne sont pas fréquentées par les mêmes personnes), ce risque a été écarté en recherchant une diversité de manifestations et de sites, sélectionnés sur la base d'éléments objectifs non discriminatoires.

Ainsi que cela ressort de la carte communiquée, le choix des stations était toujours légitimé par l'existence d'un lieu de rassemblement ou de forte interconnexion de lignes (Châtelet ou République), sans lien avec la composition sociologique des usagers.

- En l'état de ses investigations, le comité n'a pas identifié de situations dans lesquelles le traitement aurait été mis en œuvre de façon discriminatoire. Il souligne néanmoins la réalité de tels risques et l'importance qui s'attache à ce que les opérateurs prennent les mesures adéquates pour les prévenir, tant en ce qui concerne l'expertise humaine requise avant tout déploiement du traitement que la formation à destination des agents (cf. *infra*).

5.4.4. Les conditions d'utilisation dans un cadre judiciaire

Aucun principe ni aucune exigence légale ne fait obstacle à ce que le recours au traitement en vue d'identifier une situation à risque aboutisse au final, à la suite de l'intervention des forces de sécurité, à l'interpellation de l'auteur des faits et à l'engagement de poursuites judiciaires à son encontre. Dans le cadre de l'expérimentation, il a été observé que de telles poursuites avaient été engagées dans ce contexte en de très rares occasions (cf. *supra 1.3.6.*).

Le comité souligne toutefois l'importance qui s'attache alors au respect des conditions liées à l'intégrité de la preuve (absence d'altérité…) et à la mise sous scellés numériques.

5.4.5. Les craintes d'un premier pas vers des dispositifs plus intrusifs

La crainte que le recours au présent traitement algorithmique pour la vidéoprotection constitue un premier pas vers des dispositifs plus intrusifs a été régulièrement mise en avant, notamment par la CNIL, qui appelle à se méfier des effets d'accoutumances suscité par les expérimentations[117].

Dans son avis du 17 juin 2020 sur l'utilisation des caméras dites « intelligentes » et des caméras thermiques, elle souligne ainsi que : « *Si les objectifs assignés à ces nouveaux dispositifs sont le plus souvent légitimes, la CNIL constate que leur déploiement impliquerait une collecte et une analyse systématiques de données d'individus circulant dans l'espace public ou dans des lieux ouverts au public. Leur développement incontrôlé présente le risque de généraliser un sentiment de surveillance chez les citoyens, de créer un phénomène d'accoutumance et de banalisation de technologies intrusives, et d'engendrer une surveillance accrue, susceptible de porter atteinte au bon fonctionnement de notre société démocratique*. » [118]

Ces inquiétudes ont été reprises par la Défenseure des droits dans les observations communiquées (cf. annexe n° 11) et elles sont également relayées par nombre d'associations de défense des libertés, comme La Quadrature du net et la Ligue des droits de l'Homme (cf. annexe n° 12), pour qui la présente expérimentation constituerait un précédent inquiétant pour

[117] « *Les expérimentations ne sauraient éthiquement avoir pour objet ou pour effet d'accoutumer les personnes à des techniques de surveillance intrusive, en ayant pour but plus ou moins explicite de préparer le terrain à un déploiement plus poussé. Il ne saurait s'agir, à ce stade, de rendre « acceptables » des dispositifs nuisant à l'autonomie des personnes ou portant atteinte à leurs droits fondamentaux. L'acceptabilité ne peut devenir un objectif qu'ultérieurement, pour des dispositifs reconnus comme parfaitement légitimes et licites* », CNIL, Reconnaissance faciale : pour un débat à la hauteur des enjeux, 14 novembre 2019, p.10.

[118] https://www.cnil.fr/fr/la-cnil-appelle-la-vigilance-sur-lutilisation-des-cameras-dites-intelligentes-et-des-cameras

les libertés fondamentales[119]. Plusieurs recherches universitaires ont approfondi cette thématique[120].

La menace pour les droits fondamentaux est un risque que l'on ne saurait taire, mais qui procédera d'un choix politique futur ne relevant pas des compétences du présent comité d'évaluation. Le comité invite toutefois à observer la prudence et la vigilance à l'occasion de ces expérimentations : il relève et relaie dans son rapport un certain nombre de bonnes pratiques opérationnelles et démocratiques mises en œuvre pour préserver le respect des droits fondamentaux. Celles-ci demeurent les fondements démocratiques de tous déploiements, indépendamment des choix futurs du législateur.

[119] EDRI, Global civil society and experts statement: Stop facial recognition surveillance now, 26 septembre 2023 ; Human Rights Watch, Time to Ban Facial Recognition from Public Spaces and Borders, 29 septembre 2023.
[120] Bennett C.J. and Haggerty K. D. (dir.), Security Games: Surveillance and Control at Mega-Events, Milton Park, UK / New York, USA: Routledge, 2011, 194 p. ISBN 978-0-415-60262-4.

Conclusion générale

Synthèse des observations du comité

Il ressort de l'ensemble des éléments recueillis dans le cadre de la présente évaluation, à la suite des documents collectés et investigations diligentées, que le recours aux traitements algorithmiques mis en place dans le cadre de l'expérimentation s'est traduit par des performances techniques inégales, très variables en fonction des opérateurs et des cas d'usages, des contextes d'utilisation, ainsi que des caractéristiques techniques et du positionnement des caméras. Dans tous les cas, une prise en compte suffisante de la diversité des situations lors des phases d'entraînement des modèles ainsi que la qualité du paramétrage précédemment réalisé sont essentielles. Dans tous les cas aussi, la prise en compte des libertés publiques très en amont est tout aussi nécessaire.

Ainsi, par exemple, le recours à une caméra positionnée à faible hauteur, dans des conditions d'éclairage satisfaisantes, aux fins de détecter la pénétration d'individus dans une zone donne lieu à des résultats excellents. A l'opposé, le nombre d'erreurs de détection sera particulièrement élevé en cas de recours à une caméra très en hauteur et destinée à détecter des objets abandonnés.

Ce bilan contrasté se retrouve sur le plan opérationnel.

En efficacité, le nombre d'alertes a permis de concentrer dans certains cas l'attention des personnels sur des faits suspects qui n'auraient pas été repérés sans l'IA.

L'intérêt du dispositif dans le cadre de l'expérimentation dépend largement du contexte d'utilisation et des cas d'usage. De façon générale, il est plus marqué lorsque la présence policière est insuffisante pour couvrir toute la zone considérée mais néanmoins suffisante pour permettre une intervention en temps utile. L'importance du nombre de « faux positifs »[121] altère en outre son intérêt pour certains cas d'usage, comme la détection d'objets abandonnés. Le nombre d'interventions réalisées du seul fait du traitement par les différents opérateurs, aux fins de constater ou empêcher un risque ou une infraction, est demeuré extrêmement résiduel.

Les agents concernés sont globalement satisfaits de la mise en œuvre du dispositif. L'intégration des écrans des caméras IA dans les salles de commandement, lorsqu'elle a été réalisée, a contribué à favoriser la complémentarité des caméras classiques et des caméras IA.

Les différents opérateurs se sont par ailleurs efforcés de répondre aux exigences légales en ce qui concerne l'information du public, même si, selon le comité, celle-ci aurait pu être rendue plus claire et plus lisible. L'enquête réalisée par le comité révèle que le public, dans sa grande majorité, est loin de se désintéresser des enjeux liés à la mise en place de ces dispositifs, qu'il s'y montre globalement favorable dans son principe, mais non sans exprimer certaines inquiétudes quant aux garanties qui s'y attachent, en particulier si de tels traitements venaient à être étendus à d'autres utilisateurs ou à d'autres contextes d'utilisation.

De façon générale, il est essentiel que l'information donnée soit suffisante pour garantir que le public soit éclairé et qu'il connaisse les droits qui lui sont reconnus par le droit européen et la législation nationale.

[121] C'est-à-dire, comme il a été dit *supra*, d'alertes remontées à tort par le traitement.

Enfin, le comité s'est montré particulièrement attentif, dans le cadre de ses investigations et de ses réflexions, au respect des libertés publiques par les traitements algorithmiques expérimentés et les opérateurs. Il n'a pas relevé d'atteinte aux exigences posées par la Constitution, le droit de l'Union européenne ou le cadre légal et règlementaire mais souligne néanmoins les enjeux qui s'attachent à un contrôle très attentif de la mise en œuvre d'un tel outil, afin notamment de prévenir tout risque de détournement des finalités légales ou, plus fondamentalement, d'accoutumance au recours à une telle technologie à des fins de surveillance.

Une vigilance particulière s'impose donc, ce qui implique que le recours à de tels dispositifs soit entouré de différentes garanties légales et que les différents utilisateurs mettent en place des diligences spécifiques (formation, confidentialité…).

Les perspectives et points d'attention

L'abandon, la prolongation ou la pérennisation : un choix politique qui ne relève pas de la mission du comité d'évaluation

Eu égard à son périmètre et à son champ d'application limité, restreint à certaines manifestations particulières et centré sur un évènement d'ampleur exceptionnelle, et ainsi qu'au nombre très réduit de logiciels effectivement testés, la présente expérimentation ne permet en aucun cas de se prononcer de façon générale sur la pertinence du recours à l'IA en matière de vidéoprotection.

Tout abandon, toute prolongation ou toute pérennisation de l'expérimentation devrait envisager les nouvelles évolutions technologiques, l'évolution des besoins et attentes des opérateurs et les enjeux du recours au dispositif dans des contextes moins exceptionnels.

Il n'appartient bien évidemment pas au comité d'évaluation de se prononcer sur l'opportunité politique d'un éventuel abandon ou d'une éventuelle prolongation ou pérennisation de l'expérimentation. Les utilisateurs ont émis des avis favorables, sans que leur position n'engage celle du comité. A l'extérieur du comité, les associations ont communiqué leurs mises en garde à ce sujet (cf. *supra*).

Au Parlement, le rapport d'information sur l'application de la loi du 19 mai 2023, remis par Agnès Canayer et Marie-Pierre de La Gontrie au nom de la commission des lois du Sénat, a mentionné la nécessité de procéder à un bilan exhaustif de l'expérimentation avant son éventuelle pérennisation tandis que certains parlementaires proposaient, avant même le début de l'expérimentation, la généralisation du recours aux traitements algorithmiques à des fins de vidéoprotection[122].

Les enseignements en ce qui concerne la méthodologie pour le suivi du dispositif

Le caractère pluridisciplinaire et indépendant du comité a été positif pour la mise en œuvre de l'évaluation à durée déterminée.

[122] Proposition de loi n° 128 relative à la reconnaissance biométrique dans l'espace public, adoptée par le Sénat le 12 juin 2023.

Pour l'avenir, une telle politique de vidéoprotection restera sous le contrôle de la CNIL, des juges judiciaires et administratifs et, bien sûr, du Parlement.

Il reviendra aux autorités de savoir si elles souhaitent créer, comme l'avaient décidé la ville de Paris et la préfecture de police pour le PVPP, un ou plusieurs comités informels de personnalités indépendantes chargés de suivre les développements éventuels de cette technique et de faire connaître leurs observations.

Points d'attention sur les plans juridique, administratif et technique

▪ Sur le plan juridique, le comité souligne, au préalable, l'importance de bien faire respecter le cadre légal, en mettant fin aux initiatives de certaines collectivités territoriales ou personnes privées qui continuent de recourir à des dispositifs d'IA en matière de vidéoprotection en dehors du champ de la présente expérimentation. Cette exigence est indispensable pour la confiance des citoyens dans la loi qui introduit et utilise l'IA dans le domaine de la sécurité car un tel respect s'impose avant tout en vue de la préservation des libertés publiques. Accessoirement, les prestataires qui respectent la loi ne doivent pas être exposés à la concurrence déloyale de la part de fournisseurs moins scrupuleux.

▪ Dans le cadre d'une éventuelle prolongation ou pérennisation de l'expérimentation, le comité considère d'abord qu'il appartiendrait au législateur de réaffirmer les principes généraux suivants :

- Le contrôle des parlementaires en amont et le renvoi à des projets de décrets soumis à la CNIL ;
- L'interdiction de la reconnaissance faciale en dehors du contexte judiciaire ;
- L'évaluation constante des enjeux pour les libertés publiques et les droits fondamentaux ;
- Le principe de primauté humaine, lequel implique la garantie que le traitement fonctionne à tout instant sous la supervision des personnes qui le mettent en œuvre ;
- Le recours exclusif à des technologies en adéquation avec l'état de l'art, à des données pertinentes pour l'entraînement des modèles et à des caméras dont les caractéristiques sont en adéquation avec le cas d'usage ;
- La mise en place d'un système robuste et permettant de conserver les informations pendant une durée limitée ;
- L'information claire du public quant à l'étendue exacte de l'utilisation des caméras équipées d'IA en ce qui concerne son droit d'accès.

▪ Dans le cadre de la mise en œuvre de ces principes, un abandon ou un prolongement de l'expérimentation (et a fortiori son élargissement ou sa pérennisation) soulèveraient nécessairement les questions sensibles suivantes :

<u>1°) En cas d'abandon</u> :

Quelles conséquences en matière de sécurité des personnes entraînerait l'abandon d'un tel traitement dans le cadre juridique prévu par l'expérimentation ?

D'un côté, cet abandon contribuerait-il à renforcer la confiance du public pour un usage prudent des nouvelles techniques de surveillance si elles ne sont pas absolument indispensables ?

D'un autre côté, entraînerait-il une « perte de chance » d'efficacité ? L'impact serait-il vraiment significatif alors que ce traitement est aujourd'hui réservé à certains évènements d'une ampleur particulière ?

2°) En cas de prolongation ou de pérennisation :

2-1°) Renforcer certaines garanties ?

a) Faudrait-il davantage expliciter les conditions d'exercice des droits garantis par le RGPD, la directive « police – justice » et la loi CNIL ?

b) Faudrait-il reprendre la proposition de la Défenseure des droits, qui soulignait l'intérêt de prévoir que les autorisations soient publiées 48 heures en amont de l'évènement afin de garantir l'effectivité du droit au recours ?

c) Faudrait-il rendre obligatoire, avant la délivrance des habilitations, une formation, attestée et contrôlée, de sensibilisation aux questions éthiques et juridiques (libertés fondamentales) et connaissance du droit soulevées par les traitements algorithmiques, à destination tant des opérateurs vidéo que de la hiérarchie ?

Le contenu de telles formations pourrait, en particulier, être homogénéisé et préciser notamment la façon dont les agents doivent se positionner par rapport aux signalements qui leur sont remontés via le traitement.

d) Faudrait-il homogénéiser et renforcer l'exigence, pour les agents habilités, d'une clause de confidentialité contraignante et courant sur plusieurs années ?

e) Faudrait-il prévoir (ainsi que cela a été évoqué au point *4.1.3*.) que les différents opérateurs organisent des réunions publiques de compte-rendu annuel sur la mise en œuvre du traitement ?

2-2°) Alléger certaines exigences ou garanties ?

a) Faudrait-il procéder à un renvoi plus large du législateur au pouvoir réglementaire, afin de ne pas rigidifier excessivement le cadre légal applicable ? Est-il notamment nécessaire de citer dans la loi les seuls opérateurs autorisés à mettre en œuvre les traitements ?

b) Faudrait-il, tout en maintenant le principe d'interdiction d'identification biométrique, autoriser la détection par l'IA sur la base de la similarité d'apparence (par exemple la couleur du vêtement d'un individu, ce qui permettrait d'associer le porteur d'un bagage abandonné à son propriétaire)[123] ?

Dans son avis de juin 2024, la CNCDH admet l'opportunité d'une exception à ce principe d'interdiction « *pour la prévention d'une menace grave et imminente pour la vie, ou la sécurité des personnes et celle des ouvrages, installations et établissements d'importance vitale* ».

c) Faudrait-il alléger les contraintes administratives procédurales préalables à la mise en œuvre du traitement, en vue d'une plus grande réactivité ?

[123] Il a été notamment observé que cette fonctionnalité était prévue dans le programme européen Prevent, auquel sont associées la SNCF et la RATP.

Il a été constaté que des délais administratifs trop resserrés ne permettaient pas de laisser un délai suffisant pour paramétrer le traitement afin d'anticiper les éventuels dysfonctionnements puis pour effectuer les tests.

d) Faudrait-il reconnaître à chaque utilisateur davantage d'autonomie dans la mise en œuvre du traitement ? La question se pose en particulier en ce qui concerne la procédure d'appel d'offres.

Il a été observé que dans le contexte particulier de cette première expérimentation, et en raison en outre des contraintes de calendrier, le choix a été fait d'une procédure centralisée. Sur la base de l'expérimentation et des leçons qu'on peut en tirer, la question d'une certaine décentralisation se poserait.

e) Faudrait-il élargir, en ce qui concerne la mise en œuvre du traitement IA par les collectivités territoriales, les catégories d'agents susceptibles d'être habilités à l'utiliser ?

Certaines collectivités peuvent préférer réserver les policiers à la présence sur le terrain pour habiliter des personnels administratifs en vue du suivi des caméras IA.

Inversement, le procédé en lui-même est susceptible de produire des conséquences pour les libertés. Et la loi a prévu des garanties particulières dans le statut des policiers, qu'ils relèvent de la police ou de la gendarmerie nationales ou des polices municipales, en application de l'article L. 252-2 du code de sécurité intérieure.

Quels que soient les choix futurs, la qualité administrative et technique des personnels devra être définie soigneusement.

f) Faudrait-il prévoir la possibilité de procéder à des itérations entre les prestataires et les opérateurs, aux fins de recueillir de nouvelles données d'entraînement dans le cadre de l'exploitation du traitement et d'améliorer en conséquence ses performances techniques ?

2-3°) Adapter certaines garanties ?

a) Faut-il supprimer certains cas d'usage ou, au contraire, en ajouter d'autres ?

La question d'une éventuelle suppression se pose en particulier pour ceux d'entre eux (départs de feu, personnes au sol à la suite d'une chute) dont l'intérêt opérationnel est le plus limité en l'état de la technologie utilisée. Elle se poserait bien sûr en des termes différents dans le cas du recours à des traitements plus performants de ce point de vue.

D'autres enjeux de sécurité pourraient également être mentionnés, comme la détection des rixes. Cette question est cependant délicate en ce qu'un tel cas d'usage impliquerait une analyse comportementale.

Ainsi la question pourrait se poser d'admettre le dispositif pour toute finalité en lien avec la sécurité des personnes, en laissant à chaque opérateur le soin, dans ce cadre, de préciser le cas d'usage. Dans ce changement majeur, les caméras avec IA deviendraient une technique de police banalisée. Elles s'étendraient à toutes les formes de police y compris le renseignement ou la police aux frontières. Elles soulèveraient néanmoins une question quant à la précision suffisante et aux effets du décret, sur laquelle il n'appartient pas au comité de se prononcer.

b) Se posera enfin la question plus générale de caméras IA non plus pour un but de sécurité mais plus simplement pour un but d'amélioration de l'exploitation d'un service public donné. Ainsi, dans le cas des services publics de transport en commun, environnement dans lequel l'expérimentation IA a pu être déployée conformément à la loi du 19 mai 2023, au vu des enjeux de sécurité induits, il pourrait également être envisagé le recours aux traitements algorithmiques pour la mesure des flux, la gestion de la cadence des trains et bus, ou l'estimation des vitesses de rotation. Déjà, dans l'expérimentation de 2024, le cas d'usage densité de population est en réalité à la fois utile à la sécurité et à l'exploitation.

Dans cette hypothèse, en lien avec l'exploitation du service, sans rapport direct avec des enjeux de sécurité, serait introduite une autre forme de vidéoprotection avec IA.

Le comité note ainsi la question évoquée par la RATP et la SNCF mais sans l'avoir explorée (il n'avait pas à le faire). Mais la question peut se poser, plus généralement, pour l'ensemble des opérateurs autorisés à recourir à l'IA en matière de vidéoprotection.

- Outre ces éventuelles évolutions du cadre législatif et réglementaire, d'autres questions se poseraient sur le plan pratique :

1°) Faudrait-il privilégier le recours à des caméras dédiées ou à des caméras utilisées dans le cadre du système de vidéoprotection traditionnelle[124] ?

2°) Faudrait-il rendre plus systématique le caractère collectif de la décision de levée de doutes en cas de remontée d'alertes ?

3°) Comment améliorer la coordination, pour un même évènement, entre les différents acteurs en présence (opérateur techniques, responsable de l'organisation, force de sécurité, etc.) et améliorer la gestion des dysfonctionnements ? Peut-on, par exemple, systématiser la mise en place d'une hotline ?

4°) Serait-il utile d'organiser une veille permanente sur la législation et les pratiques dans les autres Etat occidentaux (notamment dans le cadre du déploiement du règlement européen sur l'IA) ?

[124] Des réflexions sont en cours à la préfecture de police sur une éventuelle évolution de sa doctrine.

ANNEXES

1°) Composition du comité d'évaluation

Le président du comité d'évaluation, Christian VIGOUROUX, a été nommé par décret du 28 novembre 2023.

Florian ROUSSEL, maître des requêtes au Conseil d'Etat, a été désigné en qualité de rapporteur général du comité.

La composition du comité a été actualisée par un arrêté du 10 janvier 2025[125], publié au JORF du 12 janvier 2025 :

Membres du collège des personnalités indépendantes :

Sur désignation de la présidente de l'Assemblée nationale :
Mme Sandra REGOL
M. Stéphane MAZARS

Sur désignation du président du Sénat :
Mme Nadine BELLUROT
M. Jérôme DURAIN

Sur désignation de la présidente de la Commission nationale de l'informatique et des libertés :
Mme Caroline LEQUESNE, maître de conférences en droit public à l'Université Côte d'Azur.
M. Benjamin NGUYEN, professeur des universités en informatique à l'Institut national des sciences appliquées - Centre-Val de Loire

Sur désignation de l'Académie des technologies :
Mme Sophie PROUST, présidente du pôle numérique de l'académie des technologies
M. Nikos PARAGIOS, professeur des universités en mathématiques à l'Ecole centrale Supelec - Université Paris-Saclay

Sur proposition du président du comité d'évaluation :
Mme Brunessen BERTRAND, professeur de droit public, université de Rennes.
M. Jean-François BEYNEL, magistrat, premier président de la cour d'appel de Versailles.
M. Hubert du MESNIL, ingénieur général des ponts, des eaux et des forêts.
Me Corinne THIERACHE, avocate au barreau de Paris

Sur désignation du président de l'association des maires de France :
Mme Rafika REZGUI, maire de Chilly-Mazarin

Membres du collège des services utilisateurs :

M. Louis LAUGIER, directeur général de la police nationale, représenté en cas d'empêchement par Mme Adeline CHAMPAGNAT, conseillère technologies et numérique ou par M. Pierre-Alain DUPONT, conseiller adjoint technologies et numérique

[125] Arrêté portant nomination des membres du comité d'évaluation de l'expérimentation de traitements algorithmiques d'images légalement collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs.

M. le général d'armée Hubert BONNEAU, directeur général de la gendarmerie nationale, représenté en cas d'empêchement par le général de division Marc BOGET, directeur de la stratégie digitale et technologique

M. Julien MARION, directeur général de la sécurité civile et de la gestion des crises, représenté en cas d'empêchement par Mme Isabelle MERIGNANT, sous-directrice de la doctrine et des ressources humaines à la direction des sapeurs-pompiers ou par la lieutenante-colonelle Angélique LE BORGNE, adjointe au chef du bureau de la doctrine, de la formation et des équipements

M. Laurent NUNEZ, préfet de police, représenté en cas d'empêchement par Mme Magali CHARBONNEAU, directrice de cabinet du préfet de police ou par M. Philippe LE MOING SURZUR, secrétaire général de l'administration de la préfecture de police

Mme Julie MERCIER, directrice des entreprises et partenariats de sécurité et des armes, représentée en cas d'empêchement par le colonel Olivier BARTH, sous-directeur des acteurs de la sécurité du quotidien et de la stratégique territoriale

M. Jean CASTEX, président-directeur général de la Régie autonome des transports parisiens, représenté en cas d'empêchement par Mme Emmanuelle CORTOT-BOUCHER, secrétaire générale de la RATP ou par M. Guillaume RONDEAU, directeur juridique de la RATP

M. Jean-Pierre FARANDOU, président-directeur général de la SNCF, représenté en cas d'empêchement par M. Xavier ROCHE, directeur de la sûreté de la SNCF ou par M. Franck BERTIN, directeur de la prospective de la SNCF

Mme Valérie PECRESSE, présidente d'Ile-de-France Mobilités, représentée en cas d'empêchement par Mme Bénédicte GUITARD, déléguée régionale à la sûreté dans les transports d'Ile-de-France Mobilités ou par Mme Hélène BRISSET, directrice du numérique d'Ile-de-France Mobilités

M. Pierre-Antoine MOLINA, délégué interministériel aux jeux Olympiques et Paralympiques et délégué interministériel aux grands évènements sportifs, représenté en cas d'empêchement par M. Christophe DELAYE, conseiller en charge de la sécurité ou par Mme Sandrine PEREIRA-RODRIGUES, conseillère en charge de la sécurité

S*ur désignation du président de l'association des maires de France :*
M. Nicolas GORJUX, premier adjoint au maire de Cannes

2°) Liste des personnes auditionnées ou ayant remis une contribution écrite

Gérald DARMANIN, Ministre de l'intérieur

Claire HEDON, Défenseure des droits

Marie-Laure DENIS et Louis DUTHEILLET DE LAMOTHE, respectivement présidente et directeur général de la CNIL

Michel CADOT, Délégué interministériel aux Jeux olympiques et paralympiques, et Pierre-Antoine MOLINA, son successeur

Laurent NUNEZ, Préfet de police

Quentin BARENNE et Matthias HOUILLER, Société Wintics

Alan FERBACH, Société Vidétics

Bastien LE QUERREC, Félix TREGUERE, Mme Noémie LEVAIN, Association La Quadrature du Net

Maryse ARTIGUELONG, Association La Ligue des droits de l'homme

Sara BALDEN, Thomas FRACHON, Roméo BERNHART, Victor MAGAUD et Raja MADANI, étudiants à Sciences Po Paris

Les échanges avec les membres du collège des utilisateurs du comité d'évaluation et avec les agents rencontrés lors des déplacements lors des phases de test ne sont pas mentionnés ici.

Les fonctions mentionnées sont celles exercées à la date de l'entretien.

3°) Récapitulatif des déplacements des membres du comité dans le cadre des expérimentations

Jeux olympiques

Test Arena La Défense (28/7) : C. Vigouroux, F. Roussel
Test Porte de Versailles (29/7) : C. Vigouroux, F. Roussel, J-F. Beynel
Test SNCF (30/7) : C. Vigouroux, F. Roussel, B. Nguyen, B. Bertrand
Test Stade de France (30/7) : C. Vigouroux, B. Bertrand, B. Nguyen
Test Porte de Versailles (1/8) : C. Vigouroux, F. Roussel, B. Bertrand
Test RATP (1/8) : C. Vigouroux, F. Roussel, J-F. Beynel, B. Bertrand
Test Vaires-sur-Marne (2/8) : J-F. Beynel, B. Bertrand
Test SNCF (6/8) : H. du Mesnil
Test Bercy (9/8) : C. Thiérache, C. Lequesne, H. du Mesnil, C. Delaye, S. Pereira-Rodrigues
Test RATP (10/8) : C. Thiérache, C. Lequesne
Test Roland Garros (10/8) : C. Thiérache, C. Lequesne, C. Delaye, S. Pereira-Rodrigues

Jeux paralympiques

Test RATP (4/9) : C. Thiérache, B. Bertrand, N. Bellurot, C. Delaye, J. Durain
Test SNCF (5/9) : B. Bertrand, N. Bellurot, S. Pereira-Rodrigues
Test Préfecture de police (5/9) : C. Thiérache
Test Vaires-sur-Marne (6/9) : C. Vigouroux, F. Roussel

Déplacements à l'occasion des autres tests :

1° Préfecture de police

Bercy Arena – concert du groupe Dépêche Mode (3/3) : C. Vigouroux, F. Roussel, H. du Mesnil et C. Thiérache
Match PSG Atletico Madrid (6/11) : C. Vigouroux / N. Bellurot
Match PSG et match de rugby (22/11) : J-F. Beynel
Match PSG-Lyon (15/12) : C. Vigouroux
Nuit de la Saint-Sylvestre (31/12) : C. Vigouroux

2° RATP

Concert à l'Arena Défense (20/4) : C. Vigouroux, F. Roussel, B. Bertrand
Fête de la musique (21/6) : J-F. Beynel, C. Thiérache, B. Nguyen
Concert à l'Arena La Chapelle (14/12) : H. du Mesnil
Retour des fêtes (3/1/25) : C. Vigouroux, S. Regol

3° SNCF

Match PSG-Lyon (21/4) : C. Vigouroux, F. Roussel, C. Thiérache
Réunion de présentation SGDSN (11/7) : F. Roussel
Relais flamme olympique (15/7) : J-F. Beynel, C. Thiérache
Départs en vacances (19/12) : F. Roussel, S. Mazars

4° Ville de Cannes

Festival (23/05) : C. Lequesne
Marché de Noël (11/12) : C. Lequesne

4°) Comparaison européenne et internationale sur les traitements algorithmiques en matière de vidéoprotection

4-1) Source ministère de l'intérieur[126]

Dans le cadre de l'expérimentation de la vidéo « intelligente » prévue par la loi du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024, la DAEI et la DCIS ont réalisé une comparaison des dispositifs similaires existants en Allemagne, Belgique, Espagne, Irlande, Italie, Pays-Bas, Royaume-Uni et Slovénie.

En **Allemagne** la police fédérale a testé pendant 18 mois un logiciel d'analyse vidéo semi-automatique (Investigator) en matière de lutte contre la criminalité et le pérennisera probablement à partir de janvier 2024. Il a été constaté que la valeur ajoutée en matière de police pour lutter contre la criminalité était considérable. L'application dispose de la reconnaissance faciale. Comme le logiciel n'est utilisé qu'en matière de poursuite pénale et non de manière préventive, le ministère fédéral de l'Intérieur et du Territoire (BMI) s'attend à un éventuel débat public nettement plus modéré que les logiciels similaires en matière de prévention de la menace. Un projet pilote de « vidéosurveillance intelligente » a également été lancé à Mannheim fin 2018. Depuis juillet 2023, elle est également utilisée dans le quartier de St. Georg à Hambourg où la Hansaplatz est équipée à titre expérimental pendant trois mois. Il ne fonctionne toutefois pas avec une reconnaissance faciale mais enregistre certains modèles de comportement qui indiquent typiquement un comportement criminel.

En **Belgique** l'utilisation de caméras algorithmiques par les polices locales fait partie des usages de l'intelligence artificielle à des fins policières même si la législation ne permet que l'utilisation des caméras algorithmiques pour la reconnaissance automatique des plaques d'immatriculation.
Depuis 2019, la police locale des villes de Courtrai, Kuurne et Lendelde utilise un système de vidéosurveillance « intelligent » développé par l'entreprise BriefCam. Le premier objectif est de faciliter les enquêtes : par exemple si une personne portant un sac à dos et un manteau bleu s'est enfuie dans une certaine direction, l'algorithme permet de la retrouver facilement. La personne est ensuite suivie par d'autres caméras afin d'obtenir une image plus complète de l'itinéraire qu'elle a emprunté et de détecter les délits qui ont pu être commis. La génération d'alertes en direct est une autre fonctionnalité recherchée : par exemple au début et à la fin de la journée scolaire, les camions ne sont pas autorisés à circuler à proximité des écoles. Si un camion est repéré alors qu'il traverse une zone interdite, le système envoie une alerte à la police. Le système stocke tous les objets qui apparaissent dans les images vidéo. Un algorithme décide ensuite à quelle catégorie appartient chaque objet. Dans des circonstances exceptionnelles, à la demande d'un juge d'instruction, il est possible d'utiliser la reconnaissance faciale.

En **Espagne**, deux lois principales encadrent l'utilisation de la vidéosurveillance par les forces de l'ordre mais pas encore les systèmes intelligents (dont la reconnaissance faciale). Le système de reconnaissance faciale ABIS (*Automatic Biometric Identification System*), mis à la disposition de la police nationale, de la Guardia Civil et des forces de police autonomiques (sauf

[126] Note de la Direction des affaires européennes et internationales et de la Direction de la coopération internationale de sécurité (DCIS) de la Direction générale de la Police nationale du 1er mars 2024.

l'Ertzaintza, la police autonomique basque) pour n'être utilisé que dans le cadre d'enquêtes policières, a fait l'objet d'un premier essai pilote en 2019. En janvier 2023, la Renfe (équivalent SNCF) disposait déjà de systèmes de vidéosurveillance intelligents dans plus de 60 stations Cercanías (gares RER). Il s'agit de la première étape vers la numérisation complète des systèmes de sécurité de 483 gares, un projet appelé Renfe Smart Security Station (RS3) devrait être achevé en 2024 avec l'appui du plan de relance NextGenerationUE de l'UE. Des polices municipales ont mis en place également des systèmes de vidéosurveillance intelligente.

Au **Royaume-Uni**, la vidéoprotection continue à se développer à un rythme rapide du fait de l'innovation technologique, de la baisse des coûts unitaires et d'un cadre réglementaire très souple. Le couplage de caméras à des logiciels d'intelligence artificielle est une pratique fréquente. Les terminaux peuvent être fixes ou mobiles. Comme pour le reste, le cadre est en réalité très souple, avec quelques mécanismes de contrôle. Les 46 polices britanniques utilisent de nombreux logiciels dans des domaines très divers dont l'analyse comportementale à visée antiterroriste.
Le métro de Londres a testé pendant un an, entre octobre 2022 et septembre 2023, une combinaison entre l'intelligence artificielle et la surveillance vidéo en temps réel, dans une station du Nord-Ouest de la capitale britannique : Willesden Green. Si l'idée originelle était de lutter contre la fraude, il s'agissait aussi de détecter les mouvements de foule, ainsi que les comportements criminels et antisociaux. Les agressions étaient cependant difficiles à repérer: il est arrivé plusieurs fois qu'un usager lève simplement le bras et déclenche l'alerte. En réalité, le dispositif servait surtout à affiner les algorithmes, afin que ceux-ci enregistrent les différents cas à reconnaître. La police venait par exemple montrer certaines armes à la caméra, en dehors des heures ouvrées du métro, pour que les algorithmes soient capables les identifier ultérieurement. Transport of London, l'organisme public responsable des transports en commun de Londres, a annoncé que le dispositif était en train d'être développé dans d'autres stations du réseau.

En **Irlande**, il n'existe pas de vidéo-surveillance intelligente au sein de la police ou même publique.

Dans le domaine judiciaire, l'**Italie** utilise le système SARI (système automatique de reconnaissance faciale) basé sur une analyse morphologique globale et plus uniquement sur un système de superposition ou de comparaison de photos anthropométriques. Il est accessible et alimenté par les quatre forces de l'ordre étatiques : police d'État, carabiniers, garde des finances et police pénitentiaire. Les forces de l'ordre italiennes ont à leur disposition et utilisent ponctuellement le logiciel BriefCam.

Au **Pays-Bas**, il n'existe pas de cadre législatif pour le déploiement de la reconnaissance faciale, la GHT. Toutefois, fin 2020 des règles provisoires ont permis une expérimentation limitée de la GHT, sans déploiement opérationnel. Un cadre provisoire permettant des déploiements opérationnels a été adopté le 11 janvier 2023 et définit dix critères pertinents pour l'évaluation d'une demande d'approbation de déploiement (l'usage de la GHT est encore très limité et la police n'utilise pas la reconnaissance faciale en temps réel dans les espaces publics). Les déploiements de la GHT se feront pour les trois prochaines années conformément à ce cadre de déploiement, qui sera évalué et ajusté si nécessaire durant cette période.

En **Slovénie** la police n'utilise pas de système de reconnaissance faciale associé à la vidéo-surveillance. Mais elle a recours à la reconnaissance faciale depuis 2014, avec un cadre légal établi en 2019, pour trouver des suspects à l'aide de méthodes d'enquête ouvertes (telles que la recherche d'images sur les réseaux sociaux et d'autres sources en ligne).

4-2) Source : Mme Lequesne, membre du comité

Les outils d'intelligence artificielle au soutien de la détection automatique des armes : pratiques trompeuses sur le marché américain.

La détection d'armes dans les lieux accessibles au public fait l'objet d'une offre commerciale diversifiée. Aux Etats Unis, elle se traduit principalement par la mise en place de détecteurs ayant recours à des capteurs (scanners). Leader du marché, la société Evolv s'est distinguée par la promotion de technologies de sécurité recourant à l'intelligence artificielle, promettant des « zones sans arme » et une « expérience utilisateur fluide ». Entre 2022 et 2024, la société a multiplié les contrats visant à sécuriser les espaces accessibles au public. A la suite des attentats de 2017, la salle omnisports du Manchester Arena a été la première à s'équiper (2022)[127] ; ont suivi de nombreux établissements scolaires américains (2023) et un projet pilote conduit dans le métro de New-York (2024)[128].

Le bilan de ces déploiements a toutefois été sujet à controverses. Les résultats probants des évaluations officielles, réalisées par le NCS4 (*National Center for Spectator Sports Safety and Security*), ont ultérieurement été mis en cause : d'abord par des résultats officieux non contestés par la compagnie, puis par des incidents et une nouvelle série de tests révélant notamment l'incapacité du système à repérer les couteaux[129]. Dans le métro les faux négatifs, estimés à 85%, ont en outre grevé la fluidité du trafic et renforcé, in fine, des contrôles aléatoires discriminants[130]. Face aux risques soulevés pour les libertés et la sécurité publiques, la Fédéral Trade Commission (FTC) a ouvert une enquête, qui a abouti à la condamnation de la société pour pratiques trompeuses[131]. Cette dernière fait également l'objet d'investigation de la part de la Securities and Exchange Commission (SEC) concernant ses communications aux investisseurs.

La vidéosurveillance algorithmique en Belgique : une dynamique amorcée, retour d'expérience incertains et contrastés.

En Belgique, le recours à la vidéosurveillance algorithmique fait l'objet de multiples cas d'application pour lutter contre les dépôts clandestins de déchets reconnaître les plaques minéralogiques. La région bruxelloise en constitue une bonne illustration. Outre la

[127] J. Clayton, "Manchester Arena's weapon scanning tech questioned", BBC, 2 November 2022.

[128] Concernant la détection d'armes par vidéoprotection, il sera encore relevé le dispositif mis en œuvre par les autorités de Chicago, qui se rapproche beaucoup de la VSA mis en place pendant les JO : https://www.americancityandcounty.com/artificial-intelligence/chicago-s-transit-authority-looks-to-ai-powered-gun-detection-to-help-curb-violent-crime

[129] John Honovich et Nikita Ermolaev, *FTC: Evolv "Knowingly" And "Repeatedly" Engaged In "Unlawful Acts"; Prohibits 10 Categories of Misleading Claims*, IPVM, 26 novembre 2024

[130] Barry Friedman, Max Isaacs et Katie Kinsey, *Subway Gun Scanners: The Wrong Tech in the Wrong Place*, Vital City, 30 juillet 2024

[131] Federal Trade Commission v. Evolv Technologies Holdings, Inc., No. 1:24-cv-12345, United States District Court for the District of Massachusetts (Nov. 26, 2024

mutualisation des systèmes entre la police et la STIB (société de transport bruxelloise) par le CIRB (Centre d'Informatique pour la Région bruxelloise), la police utilise des logiciels d'analyse des images en direct (Briefcam et ACIC)[132]. Les retours d'expérience de ces déploiements sont peu connus et contrastés. Tandis que l'on peut lire que « la police est (…) submergée et dans l'impossibilité d'agir à chaque alarme, d'autant plus que les « faux positifs » sont nombreux »[133], des gains de productivité et l'efficacité des systèmes sont également rapportés dans la presse[134]. D'autres déploiements sont en outre annoncés pour 2025 et s'inscrivent dans la prévention des actes violents. La police d'Anvers a ainsi annoncé le déploiement de « caméras équipées d'intelligence artificielle capables de reconnaître automatiquement les comportements violents ». Il s'agirait en effet d'utiliser l'intelligence artificielle pour « interpréter certains comportements comme de l'agression, puis à en informer la police, leur permettant d'intervenir plus rapidement »[135]. Il s'agit d'un volet du projet AEGIS visant à l'amélioration de la protection de la communauté juive. Subventionné par l'union Européenne, le projet est construit en partenariat avec, notamment, la police espagnole, la gendarmerie roumaine, Oddity AI et deux organisations juives. Il constituerait, du moins dans sa promesse, une nouvelle étape de la surveillance algorithmique en introduisant des éléments d'analyse comportementale exclu dans le dispositif de la loi JO.

---

[132] https://lacible.be/wp-content/uploads/2023/03/Rapport-2021-EDH.pdf

[133] https://www.liguedh.be/wp-content/uploads/2023/07/3-Videosurveillance-a-Bruxelles.pdf

[134] « La Bruyère et Berchem-Sainte-Agathe [en Province de Namur] ont également mis en place des systèmes de surveillance, réduisant de moitié les vols dans l'une et luttant contre la délinquance dans l'autre » https://www.rtl.be/actu/decryptage-rtl-info/recours-croissant-la-videosurveillance-reconnaissance-faciale-legalisee-sous/2024-10-08/article/719643

« L'idée d'utiliser des caméras intelligentes pour détecter la violence peut sembler innovante, mais cette approche ne date pas d'hier. Ce système est déjà utilisé dans des quartiers « sensibles » à Merksem et Deurne pour lutter contre les dépôts sauvages. En trois semaines, il a permis d'infliger 87 amendes administratives et de réduire considérablement le temps de traitement des images de vidéosurveillance. Ce processus aurait pris 70 heures à un agent, tandis que l'IA l'a bouclé en 3,5 heures. » https://daardaar.be/rubriques/societe/des-cameras-intelligentes-pour-detecter-la-violence-depasse-t-on-les-bornes/

[135] https://www.vrt.be/vrtnws/en/2024/11/26/antwerp-police-investigate-whether-smart-cameras-equipped-with-a/

5°) Liste des principaux acronymes

ANSSI : Agence nationale de la sécurité des systèmes d'information

AIPD : analyse d'impact relative à la protection des données personnelles

CIC : centre d'information et de commandement

DIJOP : délégation interministérielle aux jeux Olympiques et Paralympiques

GPSR : groupe de protection et de sécurité des réseaux (groupe de sûreté de la RATP)

IA : intelligence artificielle

JOP : Jeux paralympiques

Lab-IA : structure administrative (plate-forme) mise en place au sein de la RATP aux fins d'assurer la mise en œuvre et le suivi de l'expérimentation

LRJ : logiciel de rapprochement judiciaire

PC : poste de commandement

PVPP : plan de vidéoprotection pour Paris

RGPD : Règlement général sur la protection des données

SSI : sécurité des systèmes d'information

SUGE : service de sûreté générale de la SNCF

VMS : Système de gestion vidéo (le terme désigne les serveurs qui permettent le stockage des images et hébergent la partie logicielle du système).

6°) Rappel des phases préalables au plan technique et réglementaire pour la mise en œuvre opérationnelle des solutions logicielles (note de la DEPSA)

L'exploitation de traitements algorithmiques appliqués à des dispositifs de videoprotection implique de respecter plusieurs phases préalables, tant au plan technique que réglementaire mais également en termes de respect des obligations portant sur la protection des données personnelles et l'information à destination du public.

1. Préalable technique

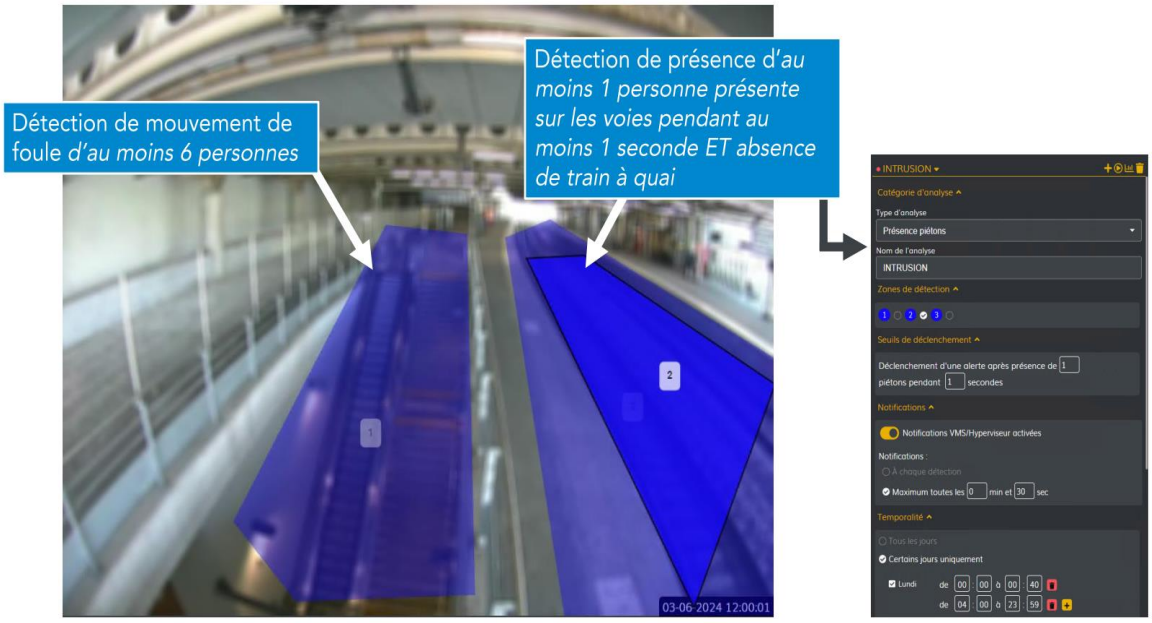
Au plan technique, l'exploitation opérationnelle des solutions logicielles est systématiquement précédée d'une phase de paramétrage, constituée de deux étapes :

1. **une étape de programmation ;**
2. **et une étape de calibration**.

L'étape de programmation consiste pour chaque caméra à :

- d'une part, déterminer ceux des huit événements pertinents parmi ceux autorisés par le décret n° 2023-828 du 28 août 2023 précité, compte-tenu de l'environnement opérationnel : tous les événements ne sont en effet pas pertinents en fonction de là où se situe la caméra ou des enjeux de sécurité propres à chaque site,
- d'autre part, définir les zones dans le champs de vision de la caméra – également appelés « polygones » - où l'on souhaite détecter l'un ou plusieurs des événements autorisés par l'expérimentation et, lorsque pertinent (densité importante de personnes notamment), les seuils de détection associés (nombre de personnes dans une zone ou par mètre carré).

Exemple de programmation :



L'étape de calibration consiste, ensuite, à vérifier, pour l'ensemble des caméras équipées et également caméra par caméra, la qualité de la programmation initiale. Il s'agit à ce stade d'une activation de la solution en conditions réelles, mais sans aucune exploitation opérationnelle.

Cette étape permet d'ajuster si nécessaire la programmation afin de limiter le nombre de fausses alarmes, ainsi que d'affiner les seuils de détection au regard des besoins opérationnels.

Conformément à l'article 7 du décret n° 2023-828 du 28 août 2023 précité, la programmation et la calibration qui constituent les deux étapes itératives du paramétrage des solutions logicielles visé au 3° de l'article 4 du décret précité, sont régies par les dispositions relatives à la phase de conception (cf. chapitre II du décret). Elles s'effectuent ainsi systématiquement sous la supervision d'un agent du ministère de l'intérieur qui est, pour cette phase, responsable de traitement. Contrairement aux phases d'exploitation opérationnelle (cf. chapitre IV du décret), elles ne sont pas soumises à autorisation préalable du préfet compétent.

2. Préalable réglementaire

Au plan réglementaire, l'exploitation opérationnelle des solutions logicielles nécessitent des autorisations préalables délivrées par les autorités préfectorales compétentes.

Pour la délivrance des autorisations, les autorités préfectorales compétentes, en concertation si nécessaire avec le comité de pilotage de l'expérimentation, s'assurent en particulier que :

- le service demandeur est éligible à l'utilisation du dispositif[136] ;
- la manifestation a bien un caractère culturel, récréatif ou sportif ;
- les circonstances de fait (ampleur et fréquentation de la manifestation, contexte sécuritaire) justifient le recours à ce dispositif ;
- le recours aux traitements algorithmique poursuit l'unique finalité d'assurer la sécurité de la manifestation concernée et les évènements dont il est envisagé la détection sont de nature à atteindre cet objectif ;
- le périmètre géographique concerné et la durée sollicités sont proportionnés au regard de la finalité poursuivie ;
- les modalités d'information du public de premier et second niveaux sont appropriées.

Partant, sur la base d'un modèle-type élaboré par le comité de pilotage, l'arrêté d'autorisation comprend systématiquement dans son dispositif les éléments suivants :

- le service responsable du traitement algorithmique et les services associés à sa mise en œuvre ;
- l'intitulé de la manifestation sportive, récréative ou culturelle concernée ;
- le périmètre géographique concerné par la mise en œuvre des traitements algorithmiques, précisé si possible dans un plan en annexe ;
- les évènements à détecter parmi ceux autorisés ;
- les modalités d'information du public ;
- la durée de l'autorisation.

3. Protection des données personnelles et information du public

Au regard de la sensibilité particulière de la thématique de l'intelligence artificielle et de la vidéoprotection, notamment du point de vue de la protection des données personnelles, et de la confusion persistante dans l'opinion publique entre « reconnaissance faciale », « intelligence

[136] Conformément au paragraphe I de l'article 10 de la loi du 19 mai 2023 et à l'article 13 du décret n° 2023-828 du 28 août 2023, seuls peuvent mettre en œuvre les traitements algorithmiques : les services de la police nationale et de la gendarmerie nationale, les services d'incendie et de secours, les services de police municipale et les services internes de sécurité de la SNCF et de la Régie autonome des transports parisiens dans le cadre de leurs missions respectives.

artificielle prédictive » et traitement de données en temps réel, une attention particulière est donnée à l'information du public.

En amont de chaque phase d'exploitation opérationnelle, le responsable de traitement transmet à la CNIL un engagement de conformité et une analyse de l'impact du traitement au regard de la protection des données (AIPD).

Dans la plupart des cas, lorsque des paramétrages ont été réalisés pendant une durée de plus d'une semaine, des AIPD ont également été rédigées. Conformément au chapitre II du décret n° 2023-828 du 28 août 2023, ces AIPD n'ont pas été transmises à la CNIL.

Parallèlement, dès la phase de paramétrage et jusqu'à la fin de l'exploitation opérationnelle, chaque déploiement a fait l'objet d'une information du public :

- **matérialisée par une information de premier niveau, *via* une signalétique** dédiée (déployée aux abords de chaque site d'expérimentation sous forme d'affiches). Le visuel et le texte des affiches ont été concertés avec les services de la CNIL ;
- **complétée par une information de second niveau disponible** sur les sites Internet de chaque responsable de traitement, par renvoi par QR Code depuis les affiches de premier niveau (à l'exception de Cannes). Le texte de cette information du public de second niveau a également été concerté avec les services de la CNIL.

Ces deux niveaux d'information, sont, par ailleurs, complétés par une information générale du public disponible sur le site Internet du ministère de l'intérieur et des outre-mer : https://www.interieur.gouv.fr/actualites/actualites-du-ministere/lancement-de-lexperimentation-video-intelligentes-en-vue-de