

CONTRIBUTION DE LA VILLE DE NICE

AU PROJET DE POSITION

RELATIVE AUX CONDITIONS DE DEPLOIEMENT DES CAMERAS DITES « INTELLIGENTES » OU « AUGMENTEES » DANS LES ESPACES PUBLICS

Remarques générales

1. Pour une meilleure lisibilité et une meilleure appréhension du sujet, nous pensons :

- soit que tout au long de sa rédaction, ce projet de position devrait respecter un découpage strict entre le secteur privé (avec les exemples associés) et le secteur public (avec les exemples associés) ;
- soit qu'il devrait y avoir deux projets de position bien distincts : un consacré au seul secteur privé (avec les exemples associés), et un consacré au seul secteur public (avec les exemples associés).

En effet, le recours aux caméras « intelligentes » poursuit des objectifs diamétralement opposés selon qu'il s'agit d'un acteur public ou privé.

L'objectif de l'acteur public est notamment d'accroître la réactivité dans l'analyse des situations remontées.

2. S'agissant du secteur public, pour une meilleure lisibilité et une meilleure appréhension du sujet, nous pensons que ce projet de position devrait respecter un découpage clair entre ce qui est « intrusif » et ce qui n'est pas « intrusif » (en fonction de l'analyse d'image effectuée par le biais de la vidéo « augmentée » et la finalité poursuivie).

En effet, l'analyse des images effectuée par le biais de la vidéo « augmentée » ne permet pas forcément d'identifier des personnes (*ex : détection d'un objet abandonné sur la voie publique ; franchissement d'une zone réglementée : c'est la catégorie de l'objet, en l'occurrence une personne, qui franchit qui est détectée, pas les caractéristiques personnelles de la personne*) ; l'analyse des images effectuée par le biais de la vidéo « augmentée » permet simplement de faire remonter une alerte au Centre de Supervision Urbain (CSU) ; après, c'est une image de vidéoprotection « classique » visualisée par un opérateur dans le cadre de sa mission.

Nous pensons donc que devrait être opéré un découpage (entre ce qui est « intrusif » / « non intrusif ») selon des cas d'usage concrets et précis et que la question d'une analyse des images en temps réel et sur les enregistrements devrait également être abordée.

L'un des principaux cas d'usage opérationnels attendus des caméras « intelligentes » est le classificateur/discriminateur d'objet. Le classificateur d'objet permet d'aider l'opérateur dans ses missions. Appliqué sur l'ensemble du système de vidéoprotection ou sur une zone prédéfinie, le classificateur d'objet permet à l'opérateur d'être plus réactif et efficace en bénéficiant très rapidement, en direct ou de manière différée, d'éléments d'information sans avoir à chercher de manière manuelle.

Exemples de cas d'usage concrets (non intrusifs a priori) :

- Comptage de véhicules (dans le cadre de la régulation des flux de transport par exemple),
- Comptage de personnes (dans le cadre de la gestion des zones d'accès règlementées par exemple),
- Classification anonymisée d'objet par catégorie (voiture, vélo, camion, trottinette, personne) dans le cadre de la gestion des zones d'accès règlementées par exemple,
- Recherche de personne par attribut non permanent (couleur de pantalon par exemple)
- Recherche de véhicule par attribut (couleur)
- Recherche d'objet (sélectionné dans l'image)
- Dépôts sauvages

3. Pour une meilleure lisibilité et une meilleure appréhension du sujet, nous pensons que ce projet de position devrait également respecter un découpage clair entre ce qui est aujourd'hui permis par les textes en termes de vidéo « augmentée », et ce qui n'est pas aujourd'hui permis par les textes.

4. S'agissant du cadre juridique, nous pensons qu'il faudrait privilégier au niveau national des textes qui fixent clairement ce qui peut être mis en place en termes de vidéo « augmentée » et dans quelles conditions (avec les AIPD déjà réalisées le cas échéant). A l'instar de ce qui a été fait au niveau des « caméras-piétons » de la Police Municipale.

(A propos des « caméras-piétons » de la police municipale :

en cas de danger, est-il possible pour le policier de faire remonter l'image en temps réel à la police municipale ?)

1. Observations préalables

1. Cf nos remarques générales.

2. La sémantique ayant son importance, « Safe Cities » (employé dans le 1.10) signifie littéralement « villes sûres » et non « villes surveillées » (le terme « villes surveillées » a une connotation négative).

2. La vidéo « augmentée » : **portrait d'une technologie aux multiples usages**

1. Cf nos remarques générales.

2. L'Intelligence Artificielle (IA) intégrée aux caméras de vidéoprotection ne « change » pas la nature et la portée de la vidéo, mais améliore son efficacité permise par les progrès technologiques.

Lorsque de l'IA est mise en place dans le cadre du franchissement de zones réglementées ou d'objets abandonnés par exemple, cela fonctionne parfaitement et l'efficacité est réelle.

L'IA ne « valorise » pas le parc de vidéoprotection ; elle permet d'améliorer techniquement la détection de certaines situations et d'apporter une plus grande réactivité aux opérateurs par rapports aux évènements remontés.

3. L'IA ne doit pas être uniquement étudiée sous le prisme de la sécurité, en occultant son apport dans la recherche de solutions pour l'amélioration du cadre de vie des personnes, de la modification de l'aménagement urbain, de la gestion des mobilités et de leur impact sur l'écologie.

4. Les dispositifs d'IA utilisés actuellement font le même travail qu'un opérateur, hormis le fait qu'ils le font plus rapidement.

L'IA ne remplace pas l'homme, mais lui transmet une alerte.

La levée de doute est toujours humaine (l'opérateur a un rôle essentiel dans l'analyse final des images).

L'IA est un outil permettant d'aider l'opérateur dans sa tâche.

L'IA est complémentaire à l'humain, et non indépendante.

L'intégration de l'IA n'a pas fait varier à la baisse le nombre des opérateurs, bien au contraire, elle a favorisé le recrutement d'ingénieurs spécialisés et favorisera le recrutement d'autres opérateurs dans le cadre de la création d'une salle de gestion des alarmes.

5. Le vocable utilisé ayant son importance (cf 2.2.3), on ne « présume » pas de la réalité d'un stationnement interdit ou d'une circulation dans un couloir de bus ou du franchissement d'un feu rouge par exemple, on la « constate ».

L'IA permet justement une levée de doute humaine immédiate permettant de caractériser une infraction et non pas seulement de la présumer.

3. Une technologie porteuse de risques gradués pour les droits et libertés des personnes

1. Cf nos remarques générales.

2. Le système de caméra vidéo avec IA fonctionne comme un système de caméra vidéo « classique » (cf 3.1.1) : l'image des personnes est visionnée (ou enregistrée) par un nombre limité de personnes habilitées situées derrière un écran de contrôle ; captation et enregistrement des images, etc ...

L'IA ne dit rien d'autre qu'une alerte à l'opérateur.

3. Pour limiter les risques pour les droits et libertés des personnes, l'utilisation des algorithmes intégrés dans les systèmes vidéo doit être encadrée strictement par les textes.

4. On ne peut pas considérer par défaut que ces dispositifs sont inefficaces et ne permettraient pas de résoudre des problèmes d'ordre sécuritaire notamment.

L'IA ne constitue pas une solution miracle, mais peut contribuer à une meilleure réponse opérationnelle pour les collectivités et dans un spectre large de compétences (apport de l'IA dans divers domaines comme l'aménagement urbain ou la gestion des différents flux).

5. Un dispositif de vidéo « augmenté » qui aurait pour objectif de détecter des infractions et de faciliter l'appréhension de son auteur n'engendre pas un risque nécessairement plus élevé pour la personne concernée par rapport à un dispositif de vidéo « classique ».

6. Quelles sont les données sensibles qui pourraient être recueillies par l'IA à proximité d'un hôpital ou d'un lieu de culte par exemple en comparaison avec de la vidéo « classique » ?

Un cadre d'utilisation stricte de l'algorithme utilisé constitue la clé contre toute forme de dérive.

4. Des conditions de légalité différenciées en fonction des objectifs, des conditions de mise en œuvre et des risques des dispositifs de vidéo « augmentée »

1. Cf nos remarques générales.

2. Nous pensons nécessaire de préciser votre développement concernant les finalités pour lesquelles un dispositif vidéo « classique » peut être mis en place sur la voie publique. En effet il nous semblait qu'un tel dispositif devait répondre à au moins une des finalités permises par le CSI (*exemple des dépôts sauvages : c'est parce que cette finalité est permise par le CSI que la question de la pertinence d'une caméra vidéo avec IA peut se poser pour prévenir et détecter les dépôts sauvages*) et respecter les règles de protection des données.

3. L'IA ne vient pas se substituer aux outils qui existent déjà, mais vient en complément.

Dès lors, il nous semblerait plus simple et plus sûr que le cadre d'utilisation de l'IA intégrée aux caméras (cas d'usage précis) soit clairement défini sur le plan législatif.

4. La plus-value de la vidéoprotection réside notamment dans la qualité de l'image. Evoquer une diminution de qualité soit visuelle soit technique (dans le cadre du privacy by design) apparaît contreproductif en matière notamment de prévention et de sécurité, mais également en termes financier au regard du coût de ces dispositifs.

5. S'agissant de l'information des personnes concernées, afin de ne pas encombrer la voie publique d'informations peu lisibles, un panneau classique de vidéoprotection avec ajout d'un pictogramme d'IA pourrait-il suffire ? Bien entendu, cette information serait doublée d'une information plus complète sur le site internet de la collectivité.

6. Nous pensons nécessaire de préciser votre développement concernant la consultation obligatoire de la CNIL.

Même si l'AIPD réalisée (dans le cadre envisagé) indique que le traitement ne présente pas un risque élevé pour les personnes concernées (caractère non intrusif du dispositif), cette AIPD devrait être soumise obligatoirement à la CNIL pour consultation ?

Exemple de la détection des dépôts sauvages (finalité permise par le CSI) par exemple : dès lors que de l'IA serait intégrée aux caméras pour faciliter cette détection, l'AIPD réalisée devrait être soumise obligatoirement à la CNIL pour consultation ?

7. S'agissant du droit d'opposition, celui-ci peut effectivement difficilement être exercé en pratique.

L'extension de l'exception prévue par le RGPD nous semble aller dans le bon sens.

8. L'action des services de police ne pourra influencer sur l'exercice par les citoyens de leurs libertés et droits fondamentaux qu'en cas de commission d'une infraction seulement.

La commission d'une infraction (notamment crime ou délit) entraîne inévitablement des atteintes à certaines libertés pour son auteur.

L'IA n'apporte rien de nouveau sur ce point par rapport à la vidéo « classique » puisque les opérateurs peuvent déjà constater des infractions à partir de la vidéo « classique ».

