Réponse à la consultation publique relative aux conditions de déploiement des caméras dites intelligentes ou augmentées dans les espaces publics.

Présentation de l'association :

810 est une association dédiée au développement d'une culture informatique française reposant sur des valeurs d'intérêt générale. Au cœur de ses manifestations, 810 promeut des enjeux de protection des données personnelles, d'accessibilité et d'écoconception des services informatiques.

Auteurs du document :

Commentaires relatifs au chapitre 1.

Le paragraphe 1.3 exclut les dispositifs de reconnaissance biométrique, notamment faciale, qui relèveraient d'un cadre réglementaire distinct. Or, la capacité d'identification d'un individu est un usage souhaité par le secteur de la vidéoprotection pour la vidéo augmentée. Cela permettrait, par exemple, de repérer une personne qui revient régulièrement aux abords d'un lieu dans le cadre de maraudages ou de repérages.

Ces dispositifs reposent sur la définition de gabarits, c'est-à-dire d'une représentation chiffrée d'un individu, que ce soit sur la base de critères faciaux, d'un morphotype ou même d'une démarche[1].

Certains algorithmes permettent de générer des gabarits propres à chaque individu, sans que ce gabarit permette d'authentifier directement l'individu. Le lien entre le gabarit anonymisé et la personne concernée doit être réalisé par une personne habilitée qui pourra croiser la chronologie de l'analyse comportementale aux enregistrements vidéo, pour authentifier la personne concernée.

Il faut considérer que les algorithmes permettant d'identifier un individu sur la base son morphotype ou de sa démarche sont aussi dangereux, en terme de risques pesant sur les données personnelles, qu'un algorithme de reconnaissance faciale : sur la base d'un enregistrement vidéo, il permettront d'authentifier la personne responsable de certaines actions.

Nous qualifieront de « reconnaissance biométrique » l'ensemble de ces processus, même si la reconnaissance des comportements pourrait dépasser le simple cadre des attributs biométriques.
La « reconnaissance biométrique » ne doit pas être considérée comme un seul processus de *« collecte du visage [morphotype/démarche] et sa transformation en un gabarit, puis la reconnaissance de ce visage [morphotype/démarche] par comparaison du gabarit correspondant avec un ou plusieurs autres gabarits »*[2].
La définition d'un gabarit permettant l'identification d'un individu, puis la reconnaissance de l'individu concerné par ce gabarit, sont deux actions distinctes.

1 https://apnews.com/article/china-technology-beijing-business-international-news-bf75dd1c26c947b7826d270a16e2658a
2 https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux

Seule la première est nécessaire à l'historisation des comportements d'une personne, mais c'est la seconde qui permet d'authentifier la personne.
La transformation en un gabarit doit être intégrée à l'étude des dispositifs de vidéos augmentée car l'historisation des actions est déterminante dans la prédiction des risques que les personnes peuvent encourir dans les lieux publics. Il est donc nécessaire que la CNIL définisse « la ligne rouge » à ne pas franchir dans ce domaine.

Nous pensons que le lien entre gabarit et personne physique doit être une action humaine soumise à une grande traçabilité, à l'instar de la consultation des enregistrements vidéo, tel que définis dans le code de la sécurité intérieure (CSI). Le logiciel permettant l'augmentation du traitement vidéo ne devrait pas stocker d'attribut personnel de l'individu (tranche d'age, couleur de peau, sexe, etc.) qui permettrait d'authentifier la personne concernée sans consulter la vidéo enregistrée.

Commentaires relatifs au chapitre 2.

Fort des remarques réalisées pour le précédent chapitre, il nous paraît important que la CNIL recommande des architectures d'information pour les dispositifs de vidéos augmentées.

En effet, dans le cas où une historisation des comportements d'individus anonymisés peut être croisée aux données vidéos, pour authentifier les personnes concernées, il serait préférable de séparer physiquement et/ou logiquement le stockage des données comportementales anonymisées et le stockage des vidéos. L'augmentation de la vidéo devrait être considérée comme un traitement distinct de la captation de la vidéo, notamment parce que les compétences nécessaires sont différentes.

Quel que soit le système informatique considéré, plus la connaissance informatique de l'utilisateur est grande, plus il y a de chance qu'il soit en capacité de bien réagir fasse à un bug ou un problème de traitement de l'information. L'augmentation d'un système de vidéo nécessite des opérateurs spécifiquement formés qui puissent être en mesure de comprendre assez précisément le fonctionnement des systèmes de reconnaissance d'image. Sans cela, l'utilisateur opérationnel risquerait de s'en remettre aux décisions issues du traitement automatisé, ce qui changerait la nature du traitement.

Par ailleurs, l'historisation des comportements d'un individu, même anonymisée, doit avoir une durée de rétention seuil, au-delà de laquelle, le profil doit être supprimé. Les *cookies*, qui sont le pendant web d'une telle traçabilité, ont bien une durée limitée par la réglementation. *« La durée de conservation des images issues d'une caméra filmant la voie publique ou un lieu ouvert au public doit être proportionnée et correspondre à l'objectif pour lequel le système de vidéoprotection est installé. Cette durée ne doit pas dépasser 1 mois. »* Ce pourrait être une base pour la durée de rétention maximale des gabarits.

Commentaires relatifs au chapitre 3.

La vidéo augmentée, une aide au pilotage

Dans le cadre de la vidéoprotection, et en cohérence avec l'article 22 du Rgpd relatif au droit d'opposition de l'individu à une prise de décision automatisée, il nous paraît important de rappeler qu'un dispositif de vidéo augmentée, évaluant des comportements individuels, ne doit être qu'un outil d'aide au pilotage et à la décision. Il doit permettre à un opérateur humain de porter attention à des situations spécifiques, mais ne doit en aucun cas déclencher seuls les mesures éventuelles que peuvent entraîner ces situations.

Par exemple, lorsqu'un comportement à risque est détecté, il doit être porté à l'attention des responsables opérationnels de la sécurité, mais ne doit pas déclencher directement une alerte auprès des équipes d'intervention. La demande d'intervention doit rester de la responsabilité des équipes de pilotage.

La vidéo augmentée, digne de confiance.

En tant que dispositif d'intelligence artificielle, nous pensons qu'il est important d'intégrer aux logiciels de vidéo augmentée certaines préconisations issues des réflexions européennes pour concevoir des intelligences artificielles dignes de confiance[3].

La traçabilité et la transparence des algorithmes concernés par toute décision automatisée est déterminante pour que l'humain puisse faire confiance à la machine.

Cette transparence concerne tant la conception humaine des algorithmes, que leur amélioration automatique via l'apprentissage machine.

Transparence humaine.

Tout éditeur d'une solution de vidéo augmentée doit s'engager à la plus grande transparence auprès de la CNIL concernant la conception de l'intelligence artificielle concernée. La CNIL, engagée à la confidentialité, pourra ainsi vérifier la conformité vis-à-vis des principes de la réglementation.

Une labellisation devrait être envisagée pour renforcer la confiance des clients potentiels.

3 https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html

Il nous semble important de rappeler les nombreux biais qui peuvent exister, notamment les biais de confirmation[4] ou biais statistiques[5]. Une attention particulière devrait être portée à la diversité des équipes en charge du développement des logiciels de vidéo augmentée. Des modalités d'audit de cette diversité seraient à prévoir.

Transparence de l'apprentissage.

Les dispositifs d'intelligence artificielle les plus avancés sont en mesure d'apprendre eux-mêmes de leurs expériences. Par exemple, si une situation jugée comme non problématique par les concepteurs provoquait à plusieurs reprises des incidents, un dispositif apprenant serait en mesure de modifier ses critères d'attention pour reconsidérer ladite situation comme dangereuse.

Si de telles fonctionnalités étaient implémentées dans des logiciels de vidéo augmentée, il faudrait assurer une grande traçabilité de ces évolutions. Le système pourrait produire régulièrement des recommandations d'évolutions, qu'il proposerait aux personnels de sécurité qui auraient la responsabilité de les accepter ou non.

On pourrait ainsi imaginer que la configuration d'une même IA varie en fonction du client chez qui elle est implantée, puisqu'elle apprendrait de situations différentes.

Responsabilité.

L'intelligence artificielle responsable du traitement de vidéo augmentée doit être considérée comme une personne morale additionnelle ayant accès aux données personnelles potentiellement sensibles, issues de la vidéoprotection. Si elle venait à mettre en péril des données à caractère personnelle, un cadre juridique doit assurer qu'on pourrait imputer la responsabilité à une personne physique qui serait, soit l'éditeur qui aurait implémenté les fonctions concernées, soit l'installateur, soit le mainteneur du système, soit l'exploitant qui aurait accepté des évolutions risquées (cf. le chapitre précédent).

On pourrait imaginer une formation certifiante pour ce type de dispositif, assurant que l'installateur/mainteneur/exploitant du système connaît et comprend les problématiques associées, et est en capacité de réagir en cas d'imprévu. Cette problématique pourrait par exemple être intégrée à termes au « Référentiel APSAD R82 Vidéosurveillance ».

4 https://ec.europa.eu/futurium/en/system/files/ged/ai_now_2018_report.pdf
5 https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G?utm_source=Twitter&utm_medium=Social

Enfin, les plages d'ouvertures du service, et le lancement de chacun des traitements servant l'augmentation de la vidéo doivent être loggés pour assurer que l'on puisse déterminer avec précision les accès du logiciel de vidéo augmentée aux images même la vidéo. De la même manière qu'aujourd'hui, lorsqu'une personne accède à un enregistrement de vidéo-surveillance, son nom doit être inscrit dans un carnet dédié.