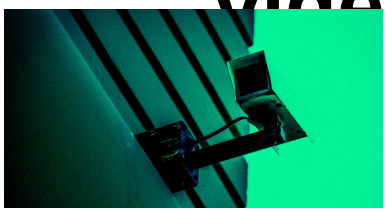
https://ricochets.cc/Algorithmes-d-analyse-automatisee-et-autres-traitements-des-images-de-la-videosurveillance-augmentee.html

Algorithmes d'analyse automatisée et autres traitements des images de la vidéosurveillance



- Les Articles -
Date de mise en ligne : vendredi 21 janvier 2022

La vidéosurveillance est déjà une belle saloperie, et la reconnaissance faciale qu'elle permet également.
En ce moment, on assiste au développement des algorithmes d'analyse automatisé et autres traitements logiciels des images de la vidéosurveillance.
Des dispositifs qui permettent de multiples analyses approfondies et automatiques des corps humains en mouvement dans l'espace public ou privé au profit d'usages très variés. Le tout à moindre coût et avec une précision toujours plus grande.

La technopolice des Etats et du business de « la-sécurité » rejoint la marchandisation et les innovations commerciales

La technopolice, portée par les Etats, le business de « la-sécurité », rejoint ici la marchandisation et les innovations commerciales. Leurs outils sont les mêmes, les données peuvent servir à l'un ou à l'autre, et il suffit d'ajouts de fonctions logicielles pour modifier et augmenter les usages de surveillance.

Algorithmes d'analyse automatisé et autres traitements des images de la vidéosurveillance Usages multiples de la vidéosurveillance et ajustables à la demande

- **Caméras dites «** intelligentes » ou « augmentées » dans les espaces publics : la CNIL lance une consultation publique

La CNIL a constaté ces dernières années une augmentation significative des dispositifs de vidéo dite « intelligente » ou « augmentée » dans les lieux ouverts au public. Afin d'accompagner leur déploiement dans le respect des droits des personnes, elle soumet un projet de position à consultation publique jusqu'au 11 mars 2022.

Les dispositifs de vidéo dite « intelligente » ou « augmentée » sont constitués de logiciels de traitements automatisés d'images couplés à des caméras. Ils permettent d'extraire diverses informations à partir des flux vidéo qui en sont issus.

Ces dispositifs sont susceptibles d'être utilisés par tout type d'acteurs, publics comme privés, en particulier dans la rue ou des lieux ouverts au public pour satisfaire des objectifs divers tels que l'amélioration de la sécurité des personnes ou des biens, l'analyse de la fréquentation d'un lieu ou encore des opérations de publicité.

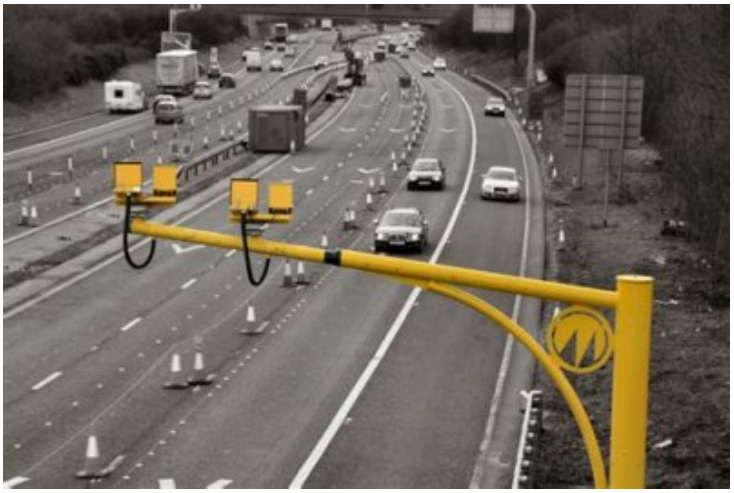
Après avoir reçu de nombreuses demandes de conseil et mené différents travaux sur le sujet, **la** CNIL publie aujourd'hui un projet de position concernant le déploiement de ces dispositifs dans les espaces publics et soumet ce document à consultation publique jusqu'au 11 mars 2022 inclus. Ce projet de position ne concerne pas les dispositifs de reconnaissance biométrique, dont la reconnaissance faciale.
(...)

- Formulaire de **Consultation publique : Position de la** CNIL relative aux conditions de déploiement des caméras dites « intelligentes » ou « augmentées » dans les espaces publics

La CNIL ne fait qu'accompagner et enrober le phénomène, le rendre légal et acceptable

La CNIL, instance consultative, ne fait qu'accompagner le phénomène, le rendre légal et acceptable, l'enrober d'une couche de recommandations, de droits et de possibilité de suivi des données. Eventuellement elle recadre ou ralentit temporairement certains dispositifs, mais elle n'arrêtera pas l'invasion de nos vies par les dispositifs techno-numériques de surveillance qui s'incrustent partout.
On observe partout les mêmes tendances, avec des variations selon les cultures locales, les rapports de force du moment et le degré d'industrialisation des régions.

Ces développements sont le déroulé logique de la civilisation industrielle et de ses besoins de puissance, de contrôle, d'optimisation, de prévision, ces technologies ne peuvent pas être arrêtées ou rendus inoffensives. Elles font partie du paquet cadeau global, soit on accepte la civilisation industrielle, et donc tout ce qui va invariablement avec (surveillance totale avec IA et algorithme, pass, brutalités policières, pollutions, destrution du vivant, précarité, etc.) , soit on la refuse en bloc parce que l'ensemble ou certains de ses aspects/conséquences nous rebutent.
Il est impossible de faire de tri, de réformer de manière conséquente des parties, de choisir un truc et d'en refuser un autre. Tout le paquet cadeau fait système, et ce système ne nous demande jamais notre avis.



Algorithmes d'analyse automatisé et autres traitements des images de la vidéosurveillance Lecture automatique de plaques minéralogiques de voitures

On le sait moins, mais la technopolice est très utilisée pour le contrôle des frontières : La surveillance algorithmique des frontières : robots partout, vie privée nulle part.

La Drôme, Rhône-Alpes, se trouve à la pointe des technologie de surveillance avec Wauquiez : **Rhône-alpes : Wauquiez veut imposer la reconnaissance faciale et les logiciels d'analyse comportementale prédictive dans les gares, cars scolaires et trains**.
A Crest, **la mairie en place veut continuer dans la vidéosurveillance**.
Des études ont montré l'inutilité de la vidéosurveillance, ce sera sans doute pareil pour la « vidéosurveillance augmentée », qui servira surtout le business de « la-sécurité », le business commercial et électoral.

La vidéosurveillance augmentée avec algorithmes et IA, ce sont les fabriquants et leurs représentants commerciaux qui en parlent le mieux :

- **VIDEOSURVEILLANCE** INTELLIGENTE
- **Luttez contre le vol à l'étalage avec l'**IA et la vidéosurveillance
- **A Suresnes, la mairie veut utiliser l'**IA pour repérer les Â« événements anormaux Â» avec ses caméras
- **Machine Learning dans la vidéosurveillance**
- **Top 5 des tendances de vidéosurveillance de Hanwha Techwin pour 2022**

- Vidéosurveillance intelligente : l'ère des algorithmes a démarré

Post-scriptum :

Extrait du projet de position de la CNIL :

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

Les notions de vidéo ou caméra dite « intelligente » ou « augmentée » sont des concepts protéiformes renvoyant à des technologies d' « intelligence artificielle » dans le domaine de l'analyse d'images ou « vision par ordinateur » pouvant couvrir des usages très variés. Il est donc nécessaire de poser précisément les termes de ces notions et des usages potentiels, afin d'être en mesure d'appréhender les risques induits et de fixer le cadre légal qui leur est applicable.

2.1. Une technologie consistant en une analyse automatisée d'images à partir de caméras vidéo

2.1.1. Le terme retenu par la CNIL de vidéo « augmentée » désigne ici des dispositifs vidéo auxquels sont associés des traitements algorithmiques mis en oeuvre par des logiciels, permettant une analyse automatique, en temps réel et en continu, des images captées par la caméra. Il s'agit de technologie dite de « vision par ordinateur » (« computer vision »), qui est une des branches de l' « intelligenceartificielle », consistant à munir les systèmes de capacités d'analyse des images numériques, par l'extraction d'informations comme la reconnaissance de formes, l'analyse des mouvements, la détection des objets...

2.1.2. La surcouche logicielle permet de « reconnaître », de façon probabiliste, des objets ou des silhouettes, des attributs, des caractéristiques (typologie d'un véhicule, sexe ou tranche d'âge d'un individu...), ou encore des comportements, des évènements particuliers (regroupement de personnes sur la voie publique, mouvement de foule, déplacement, stationnement d'un véhicule ou d'un individu dans un endroit précis...) déterminées en amont par les concepteurs et utilisateurs.

2.1.3. En pratique, les algorithmes d'analyse automatisée des images sont soit couplés à des caméras préexistantes de « vidéoprotection » (celles installées dans les espaces publics qui sont autorisées par arrêté préfectoral pour des finalités prévues par le code de la sécurité intérieure), soit spécifiquement déployés avec des dispositifs ad hoc.

2.1.4. Même si ces algorithmes s'intègrent à des caméras vidéo traditionnelles, le traitement de données qu'ils opèrent change la nature et la portée de la vidéo que nous connaissons depuis plusieurs dizaines d'années et qui ne cessent de se développer en dépit de l'absence d'études fiables quant à leur efficacité.

2.1.5. En effet, en permettant à leurs utilisateurs d'obtenir instantanément et de manière automatisée un grand nombre d'informations qui, pour certaines d'entre elles, ne pourraient être détectées par la seule analyse humaine des images, de tels algorithmes multiplient les capacités des dispositifs vidéo classiques.

2.2. Des cas d'usages multiples

2.2.1. Le recours à la vidéo « augmentée » peut s'inscrire dans des contextes extrêmement divers, au service d'intérêts aussi bien publics que privés.

2.2.2. Ces dispositifs peuvent, du fait de leurs capacités, s'intégrer dans des lieux de natures très différentes (voie publique, transports publics, centres commerciaux, culturels et sportifs...), avec une couverture géographique, des exigences de densité (quelques caméras ou un réseau très maillé) et des infrastructures très variées (mobile, fixe, embarquée, drone, portable...) pour poursuivre des objectifs divers.

2.2.3. Les questionnements ou initiatives en la matière portés ces derniers mois à la connaissance de la CNIL, notamment par des développeurs d'outils et initiateurs de projets, témoignent de la multitude des cas d'usage envisageables. Parmi ceux-ci, on peut par exemple relever :
(...)
L'intégration d'algorithmes dans ces systèmes vidéo, analysant de manière systématique et automatisée les images issues des caméras, a pour conséquence d'élargir considérablement la quantité d'images traitées et des informations qui peuvent en être inférées. Ces nouveaux outils vidéo peuvent ainsi conduire à un traitement massif de données personnelles, parfois même de données sensibles.

3.1.4. Les personnes ne sont donc plus seulement filmées par des caméras mais analysées de manière automatisée, en ce qu'elles sont ou ce qu'elles font, afin d'en déduire, de façon probabiliste, un grand nombre d'informations permettant, le cas échéant, une prise de décisions ou de mesures concrètes les concernant.

3.1.5. Un tel changement ne constitue pas une simple évolution technologique ou un approfondissement des dispositifs de vidéoprotection, mais une modification de leur nature. La CNIL rappelle à cet égard qu'une vigilance particulière doit être accordée vis-à-vis de la tentation du « solutionnisme technologique » qui consisterait ici à considérer que les dispositifs de vidéo « augmentée » sont nécessairement efficaces et permettraient de résoudre par eux-mêmes de nombreux problèmes d'ordre économique ou social.

3.1.6. Pour réguler l'essor de la vidéoprotection, la CNIL a depuis longtemps pointé le risque d'une surveillance généralisée des individus, induit par ces dispositifs. Cette surveillance était cependant, en partie, limitée matériellement par les capacités humaines de visionnage des images. Or, ce risque prend une nouvelle ampleur du fait qu'il se double désormais d'un risque d'analyse généralisée des personnes : les dispositifs automatisés offrant un champ, une systématisation et une précision d'analyse impossible jusque-là pour un humain. Au-delà de créer un phénomène d'accoutumance et de banalisation de technologies de plus en plus intrusives, ces dispositifs, du fait de leur importante capacité d'analyse, offrent à leurs utilisateurs la faculté de connaître des éléments nouveaux sur les personnes filmées pour prendre des décisions et des mesures les concernant (analyser le parcours d'achat d'une personne dans un magasin et en déduire ses goûts et ses habitudes, analyser le visage d'une personne pour en déduire son humeur et afficher une publicité ou des promotions en conséquence...).

3.1.7. Ce risque d'analyse généralisée prend une dimension particulière lorsque ces dispositifs sont déployés dans des espaces publics, où s'exercent par nature de nombreuses libertés individuelles (droit à la vie privée, liberté d'aller et venir, d'expression et de réunion, droit de manifester, liberté de conscience et d'exercice des cultes...). La préservation de l'anonymat dans l'espace public est une dimension
essentielle pour l'exercice de ces libertés ; la captation et, maintenant l'analyse, de l'image des personnes dans ces espaces sont incontestablement porteuses de risques pour les droits et libertés fondamentaux de celles-ci.

3.1.8. Au-delà des risques que présente chaque traitement de données, induit par le déploiement de dispositifs de vidéo « augmentée » pris isolément, des risques importants pour les libertés individuelles existent du simple fait de leur généralisation (actuelle et anticipée) qui pourrait aboutir à un sentiment de surveillance généralisée.

3.1.9. Par ailleurs, la vidéo « augmentée » peut constituer une technologie invisible et « sans contact » pour les personnes. Si les citoyens peuvent constater et, d'une certaine manière, appréhender l'installation de différentes caméras vidéo dans leur quotidien, ils n'ont pas de moyen d'avoir conscience que celles-ci peuvent, non pas seulement les filmer, mais également les analyser.

3.1.10. En outre, les technologies de vidéo « augmentée », comme tout traitement algorithmique, présentent un potentiel de versatilité qui doit être pris en compte dans leur perception globale. Ces technologies sont en effet techniquement capables, parfois par de simples réglages, de changer de fonctions : un dispositif de vidéo « augmentée » initialement installé pour réaliser une analyse de la fréquentation d'un lieu (comptage des personnes et segmentation par genre et tranches d'âge) pourrait, assez simplement, permettre également le suivi du parcours des personnes au sein de ce lieu.
Ou encore, un dispositif de vidéo « augmentée » dans un panneau publicitaire qui adresse de la publicité sur la base

de l'âge ou du genre de la personne pourrait techniquement également le faire sur la base de l'analyse de son visage et de ses émotions.