

Le Monde

© 2025 Le Monde. Tous droits réservés.
Le présent document est protégé par les lois
et conventions internationales sur le droit
d'auteur et son utilisation est régie par ces
lois et conventions.
0WWJZ0UEX2bY5MpyZUpE_GdvIz1q_QlJgFbABvW6mU
EbZ-h-robzQmxbIKKi43YueMWY4

news-20250818-LMF-eddxcmofrxc20250818xc66316473234

Nom de la source	Lundi 18 août 2025
Le Monde (site web)	
Type de source	Le Monde (site web) • 778 mots
Presse • Presse Web	
Périodicité	
En continu	
Couverture géographique	
Internationale	
Provenance	
France	

« Il y a une petite musique qui monte et qui dit que si vous voulez être en sécurité, il faut de la reconnaissance faciale »

Mâître de conférences en droit public, **Caroline Lequesne a fait partie du comité d'évaluation qui a suivi l'expérimentation de la vidéosurveillance algorithmique dans le cadre des Jeux olympiques et paralympiques de Paris 2024.**

Caroline Lequesne est responsable du master 2 « droit algorithmique et gouvernance des données », à l'université Côte d'Azur. Elle prévient : la reconnaissance faciale engendre de nouveaux risques pour les libertés fondamentales ainsi que des coûts.

Comment se manifeste l'attention croissante à la reconnaissance faciale en France ?

Au cours des cinq dernières années, nous avons assisté à une intensification du lobbying de la part des industriels et des politiques pour mener plus d'expérimentations. Tandis qu'au niveau juridique, les lignes sont interprétées de manière discutable.

Il n'y a, en revanche, pas de grand débat citoyen et lorsqu'il y en a un, il est en général dévoyé par ceux qui font de la

politique politicienne. Il y a une petite musique qui monte et qui dit que si vous voulez être en sécurité, il faut de la reconnaissance faciale. L'idée gagne du terrain auprès du public. Sensibiliser sur le seul terrain des libertés fondamentales ne suffit plus.

Que faire alors ?

Informers et dire que non seulement la reconnaissance faciale n'apporte pas plus de sécurité mais que, en plus, elle coûte cher et engendre de nouveaux risques. Nombre de personnes se retranchent derrière l'idée qu'elles n'ont rien à cacher. Or, l'intelligence artificielle [IA] fonctionne par déductions. Elle crée des profils qui peuvent vous catégoriser d'une manière que vous n'auriez sans doute pas imaginée. Peut-être que, sans le savoir, vous ressemblez à une personne recherchée ou que votre démarche, vos expressions ne correspondent pas à la « norme » de l'algorithme. Le public ne mesure pas l'impact des erreurs qui peuvent être commises par l'IA. Aux Etats-Unis, où ces outils sont très développés, les arrestations par erreur demeurent nombreuses et éprouvantes pour ceux qui les subissent.

Que vous inspire le fait que ce mouvement semble inéluctable ?

Il y a une forme de fatalisme dans le débat public que je trouve dangereux. En novembre 2024, lorsque le ministre de l'intérieur, Bruno Retailleau, a dit qu'il ne pourrait pas mettre un policier derrière chaque citoyen et qu'il nous faudrait de la vidéosurveillance algorithmique [VSA], beaucoup en ont conclu au chemin inéluctable de la pérennisation de ces technologies. Si la volonté politique est forte, la loi VSA n'a, à ce jour, pas été prorogée.

L'évaluation indépendante conduite par le comité d'évaluation de l'expérimentation de VSA a rendu des conclusions mitigées. Le législateur et le Conseil d'Etat s'en font l'écho en amont de l'adoption de la loi JO 2030 : les outils sont en phase expérimentale et leur plus-value devra être démontrée. Cet épisode témoigne de dynamiques démocratiques à l'œuvre. Il faut les soutenir : elles rappellent qu'un autre chemin reste possible et qu'il n'y a pas de « sens de l'histoire » technologique.

En quoi les publics plus vulnérables sont-ils plus exposés à ce genre de technologie ?

Documents sauvegardés

Cette vulnérabilité se manifeste par des dysfonctionnements plus nombreux en raison de votre couleur de peau, de vos troubles, et les ciblage plus fréquents résultant de votre position dans l'espace public et la société. C'est ce mendiant dont le comportement est suspect en raison de son immobilisme ; c'est ce jeune qui passe ses fins de journée en bas de son immeuble. Les études montrent que les plus précaires sont souvent les plus exposés aux errances algorithmiques. Il y a aussi le coût qu'exige la protection des données personnelles. Mentionnons également les traitements de données biométriques des migrants et le fait que la frontière soit devenue le lieu d'expérimentation par excellence.

e-qui-monte-et-qui-dit-que-si-vous-voul
ez-etre-en-securite-il-faut-de-la-reconn
aissance-faciale_6631647_3234.html

Que dire de l'évolution de cette technologie dans la sphère privée ?

Récemment, j'ai été troublée par l'évolution de certaines pratiques dans des espaces publics comme les supermarchés et les stades. Certains cherchent à s'inspirer de ce qu'a fait le Brésil pour proposer une expérience à 360 degrés avec de la reconnaissance faciale.

Demain, nous accéderions au stade et consommerions une bière à la pause grâce à nos visages. Jusqu'à présent, son recours était légitimé sur un plan sécuritaire. Sa généralisation pour des motifs commerciaux conduirait à sa banalisation. Ce ne serait pas sans conséquence sur notre vivre-ensemble : la fin de l'anonymat, c'est aussi la fin des conditions de la démocratie.

Cet article est paru dans Le Monde (site web)

[https://www.lemonde.fr/economie/article/2025/08/18/il-y-a-une-petite-musique](https://www.lemonde.fr/economie/article/2025/08/18/il-y-a-une-petite-musique/2025/08/18/il-y-a-une-petite-musique)