



16ème législature

Question N° : 13918	De M. Aurélien Saintoul (La France insoumise - Nouvelle Union Populaire écologique et sociale - Hauts-de-Seine)	Question écrite
Ministère interrogé > Intérieur et outre-mer		Ministère attributaire > Intérieur et outre-mer
Rubrique > police	Tête d'analyse >Logiciel Briefcam - Utilisation illégale, hébergement des données et sécurité	Analyse > Logiciel Briefcam - Utilisation illégale, hébergement des données et sécurité.
Question publiée au JO le : 19/12/2023 Date de changement d'attribution : 12/01/2024 Question retirée le : 11/06/2024 (fin de mandat)		

Texte de la question

M. Aurélien Saintoul interroge M. le ministre de l'intérieur et des outre-mer sur l'utilisation illégale du logiciel Briefcam par la police nationale, l'hébergement des données et leur sécurité. Briefcam est une entreprise israélienne détenue par Canon qui développe un logiciel d'analyse algorithmique pour images de vidéosurveillance. Cette société propose également des dispositifs de reconnaissance faciale qui s'ajoutent au système de vidéosurveillance en place. Celle-ci permet « de détecter, de suivre, d'extraire, de classer, de cataloguer » une personne en fonction de son visage, d'après le site internet de l'entreprise. Légalement, la police nationale ne peut utiliser la vidéosurveillance algorithmique que dans de très rares cas, tels que les enquêtes judiciaires ou administratives « sanctionnant un trouble à l'ordre public ou une atteinte aux biens, aux personnes ou à l'autorité de l'État », comme le souligne le rapport d'information de 2023 « sur les enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité ». La loi relative aux jeux Olympiques et Paralympiques de 2024, adoptée au Parlement en avril 2023, autorise son expérimentation par la police nationale à une large échelle jusqu'au 31 mars 2025. La représentation nationale a néanmoins interdit le recours à la reconnaissance faciale qui permet d'identifier une personne sur des images à partir de traits du visage en raison des risques élevés d'atteinte à la vie privée. Pourtant, d'après les révélations récentes du média en ligne *Disclose*, les forces de l'ordre utiliseraient les systèmes Briefcam, notamment ses fonctionnalités de reconnaissance faciale, depuis 2015 en toute illégalité, c'est-à-dire en dehors du cadre légal prévu par la directive européenne « police-justice » de 2016 et la loi française « informatique et libertés » de 2015. L'utilisation du logiciel n'a pas été déclarée à la Commission nationale de l'informatique et des libertés (CNIL) et les travaux d'évaluation de son impact sur la protection des données, normalement obligatoires, n'ont pas été réalisés. La CNIL a annoncé le mercredi 15 novembre 2023 le lancement d'un contrôle du ministère de l'intérieur portant sur son utilisation du logiciel Briefcam. Le 20 novembre, M. le ministre a demandé quant à lui une enquête administrative sur l'utilisation par ses services de la reconnaissance faciale *via* un logiciel de vidéosurveillance. Par la suite, le tribunal administratif de Caen a ordonné le mercredi 22 novembre 2023 à une communauté de communes de Normandie d'effacer les données personnelles acquises *via* le logiciel de vidéosurveillance Briefcam. Plus d'une centaine de villes seraient équipées de l'application Briefcam selon Florian Leibovici, représentant du logiciel en Europe. C'est aussi le cas de l'Assemblée nationale. Compte tenu de cette actualité et des conséquences pour le respect de la vie privée des Français, il est indispensable de s'interroger sur la localisation des données recueillies et la sûreté de leur hébergement. Il souhaite ainsi savoir où sont stockées les données utilisées par les services du ministère de l'intérieur ainsi que certaines collectivités locales en lien avec le logiciel de vidéosurveillance Briefcam et quel protocole garantit leur protection.

