

ASSEMBLÉE NATIONALE

3 mars 2023

RELATIF AUX JEUX OLYMPIQUES ET PARALYMPIQUES DE 2024 - (N° 809)

Rejeté

AMENDEMENT

N ° CL290

présenté par

Mme Élisabeth Martin, M. Vannier, Mme Abomangoli, M. Alexandre, M. Amard, Mme Amiot, Mme Amrani, M. Arenas, Mme Autain, M. Bernalicis, M. Bex, M. Bilongo, M. Bompard, M. Boumertit, M. Boyard, M. Caron, M. Carrière, M. Chauche, Mme Chikirou, M. Clouet, M. Coquerel, M. Corbière, M. Coulomme, Mme Couturier, M. Davi, M. Delogu, Mme Dufour, Mme Erodi, Mme Etienne, M. Fernandes, Mme Ferrer, Mme Fiat, M. Gaillard, Mme Garrido, Mme Guetté, M. Guiraud, Mme Hignet, Mme Keke, M. Kerbrat, M. Lachaud, M. Laisney, M. Le Gall, Mme Leboucher, Mme Leduc, M. Legavre, Mme Legrain, Mme Lepvraud, M. Léaument, Mme Pascale Martin, M. Martinet, M. Mathieu, M. Maudet, Mme Maximi, Mme Manon Meunier, M. Nilot, Mme Obono, Mme Oziol, Mme Panot, M. Pilato, M. Piquemal, M. Portes, M. Prud'homme, M. Ratenon, M. Rome, M. Ruffin, M. Saintoul, M. Sala, Mme Simonnet, Mme Soudais, Mme Stambach-Terreiro, Mme Taurinya, M. Tavel, Mme Trouvé et M. Walter

ARTICLE ADDITIONNEL**APRÈS L'ARTICLE 7, insérer l'article suivant:**

Est passible de 3 ans de prison et 45.000 euros d'amende, le fait pour une personne physique ou morale de mettre en œuvre dans l'espace public un traitement automatique des images au moyen d'un algorithme permettant l'identification d'un individu au moyen de ses caractéristiques biométriques.

Est interdit d'effectuer sur des images tirées de la vidéosurveillance un traitement similaire à posteriori visant la réidentification des individus par le même moyen.

EXPOSÉ SOMMAIRE

La surenchère technologique va de paire avec le capitalisme de surveillance qui entraîne notamment la généralisation progressive de l'usage des technologies de reconnaissance faciale. Le projet « Safe City » vise à implanter la reconnaissance faciale automatique dans le quartier de La Défense. En région Provence-Alpes-Côte-d'Azur, deux lycées publics ont failli accueillir cette technologie à l'entrée de l'établissement afin de permettre l'accès aux élèves. A Valenciennes, Huawei offre son système de vidéosurveillance pour mieux implanter et tester son système sur les Français.

Pourtant, les débats suscités par cette technologie ne font que grandir : en janvier 2020, la pré-publication du livre blanc sur l'intelligence artificielle de la Commission européenne envisageait la mise en place d'une interdiction temporaire des technologies de reconnaissance faciale dans divers secteurs. La Datainspektionen, autorité de contrôle et de protection de l'informatique et des libertés de la Suède, a infligé une amende de 18 500 euros (200 000 SEK) à un établissement scolaire qui a tenté d'utiliser cette technologie en remplacement du système d'appel des élèves. Au premier semestre 2020, on apprenait que l'entreprise américaine ClearView avait directement collecté sur internet les photos laissées par les internautes pour entraîner ses algorithmes de reconnaissance faciale et fournir son service aux services de police ou directement aux policiers quand les services refusaient de souscrire à leur offre.

C'est pourquoi la reconnaissance faciale ne doit pas être considérée comme une technologie d'identification biométrique comme les autres. Dans notre vie sociale, nous ne cachons pas notre visage qui est un signal permanent envoyé lors d'événements, sur les réseaux sociaux, les médias en ligne, et à l'occasion d'événements divers de notre vie sociale. Le RGPD garantit aux citoyen.ne.s européen.ne.s « le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage » (Art. 22), selon la définition du profilage inscrite dans l'article 4. L'usage de la reconnaissance faciale, notamment de façon automatisée, entre en contradiction avec l'article 5 du RGPD (principes de licéité, loyauté, transparence). Parce que la reconnaissance faciale appartient à la catégorie plus large des techniques biométriques, elle entre également en contradiction avec l'article 9 interdisant « le traitement des données biométriques aux fins d'identifier une personne physique de manière unique ».

En outre, et parce que la reconnaissance faciale repose sur des estimations statistiques de correspondance entre les éléments comparés, cette technologie est de facto faillible et renferme des biais importants. La question du coût pour les acteurs publics et privés, de l'implémentation des technologies de reconnaissance (de l'installation des équipements/infrastructures aux serveurs, stockage et puissances de calcul, en passant par les coûts logiciels, de maintenance et d'évolutivité) est encore mal connue et demande des rapports d'évaluation précis dans un marché mondial de la biométrie qui pourrait avoir un poids de plus de 24,8 milliards de dollars en 2021 (agence Markets & Markets, 2016).

En tout état de cause, l'implémentation de plus en plus massive des technologies de reconnaissance faciale dans les espaces et établissements publics génère des risques pour la sécurité personnelle, la vie privée, les libertés individuelles et collectives et la protection des données personnelles majeures. Sous motifs impérieux de « sécurité », la stratégie du choc continue.