N° 1317

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

DIX-SEPTIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 17 avril 2025.

PROPOSITION DE LOI

*visant à l'***interdiction** *de la* **reconnaissance faciale***,*

(Renvoyée à la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, à défaut de constitution d'une commission spéciale dans les délais prévus par les articles 30 et 31 du Règlement.)

présentée par

Mme Élisa MARTIN, Mme Mathilde PANOT, Mme Nadège ABOMANGOLI, M. Laurent ALEXANDRE, M. Gabriel AMARD, Mme Ségolène AMIOT, Mme Farida AMRANI, M. Rodrigo ARENAS, M. Raphaël ARNAULT, Mme Anaïs BELOUASSA-CHERIFI, M. Ugo BERNALICIS, M. Christophe BEX, M. Carlos Martens BILONGO, M. Manuel BOMPARD, M. Idir BOUMERTIT, M. Louis BOYARD, M. Pierre-Yves CADALEN, M. Aymeric CARON, M. Sylvain CARRIÈRE, Mme Gabrielle CATHALA, M. Bérenger CERNON, Mme Sophia CHIKIROU, M. Hadrien CLOUET, M. Éric COQUEREL, M. Jean-François COULOMME, M. Sébastien DELOGU, M. Aly DIOUARA, Mme Alma DUFOUR, Mme Karen ERODI, Mme Mathilde FELD, M. Emmanuel FERNANDES, Mme Sylvie FERRER, M. Perceval GAILLARD, Mme Clémence GUETTÉ, M. David GUIRAUD, Mme Zahia HAMDANE, Mme Mathilde HIGNET, M. Andy KERBRAT, M. Bastien LACHAUD, M. Abdelkader LAHMAR, M. Maxime

LAISNEY, M. Arnaud LE GALL, M. Antoine LÉAUMENT, Mme Élise LEBOUCHER, M. Aurélien LE COQ, M. Jérôme LEGAVRE, Mme Sarah LEGRAIN, Mme Claire LEJEUNE, Mme Murielle LEPVRAUD, M. Damien MAUDET, Mme Marianne MAXIMI, Mme Marie MESMEUR, Mme Manon MEUNIER, M. Jean-Philippe NILOR, Mme Sandrine NOSBÉ, Mme Danièle OBONO, Mme Nathalie OZIOL, M. René PILATO, M. François PIQUEMAL, M. Thomas PORTES, M. Loïc PRUD'HOMME, M. Jean-Hugues RATENON, M. Arnaud SAINT-MARTIN, M. Aurélien SAINTOUL, Mme Ersilia SOUDAIS, Mme Anne STAMBACH-TERRENOIR, M. Aurélien TACHÉ, Mme Andrée TAURINYA, M. Matthias TAVEL, Mme Aurélie TROUVÉ, M. Paul VANNIER,

députées et députés.

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

En France, garantir la sécurité dans l'espace public est progressivement devenu synonyme de recours à des technologies de surveillance.

La vidéosurveillance a été largement étendue et normalisée depuis la fin des années 1990. Selon les dernières estimations de l'avis sur la surveillance dans l'espace public rendu par la commission nationale consultative des Droits de l'Homme en juin 2024, plus de 90 000 caméras dédiées à la vidéosurveillance seraient présentes sur le territoire français.

Ce phénomène s'inscrit dans l'expansion des politiques sécuritaires de l'État et révèle sa conversion progressive à la technopolice.

Le déploiement de la vidéosurveillance se fonde sur le postulat de son efficacité pour lutter ou prévenir la criminalité, ce qui n'a pourtant jamais été prouvé. En 2020, la Cour des comptes n'avait relevé « aucune corrélation globale […] entre l'existence de dispositifs de vidéoprotection et le niveau de la délinquance commise sur la voie publique, ou encore les taux d'élucidation ».

Cette technologie représente par ailleurs un gouffre financier qui mériterait un débat parlementaire actualisé puisque les crédits publics consacrés à la vidéosurveillance devraient tripler entre 2023 et 2027, comme le prévoit la loi d'orientation et de programmation du ministère de l'intérieur (LOMPI). En réalité, les technologies de surveillance constituent une jonction entre des intentions politiques et le développement d'un nouveau marché.

Ces dernières années, le gouvernement a franchi un nouveau pas, en expérimentant la vidéosurveillance algorithmique (VSA) en totale opacité. Ce système vise à automatiser le traitement d'images de caméras de surveillance en temps réel. Celles-ci sont analysées par des algorithmes, entraînés à détecter des situations prédéfinies et à signaler les situations considérées « suspectes ».

La loi Jeux olympiques et paralympiques 2024 a permis de légaliser la vidéosurveillance algorithmique. En effet, la loi n° 2023-380 du 19 mai 2023 relative aux Jeux olympiques et paralympiques de 2024 et portant diverses autres dispositions dispose dans son article 10 que,

jusqu'au 31 mars 2025, tous les lieux accueillant des événements sportifs, festifs et culturels ainsi que leurs abords, l'intérieur des véhicules et emprises de transport public et les voies les desservant, pourront faire l'objet de traitements algorithmiques en temps réel.

La VSA est actuellement autorisée sous forme expérimentale. Mais, de la même manière que les règles dérogatoires de l'état d'urgence de 2015 ont été pérennisées, sa pérennisation à terme est déjà en cours de négociation et ce, malgré les promesses du gouvernement.

Lors de l'orientation des crédits du fonds interministériel de prévention de la délinquance et de la radicalisation pour 2023, le ministère de l'intérieur intimait ainsi aux préfets de région et de département de veiller à ce que les projets d'installation de VSA présentent un « intérêt de sécurité publique » au-delà des seuls Jeux.

Depuis, nos craintes semblent se confirmer puisque lors de son audition par la Commission des Lois de l'Assemblée nationale le 25 septembre 2024, le préfet de police de Paris s'est dit favorable à la pérennisation de la VSA, bien qu'il ne fournisse aucune donnée objective sur son efficacité.

De plus, malgré un rapport d'évaluation de l'expérimentation remis au Parlement largement en demie teinte, la prolongation de l'expérimentation jusqu'en 2027 vient d'être votée au sein de la loi dîtes « sûreté dans les transports ».

La VSA est une technologie intrusive et liberticide par la catégorisation des comportements qu'elle suppose. Les systèmes algorithmiques comportent de nombreux biais potentiels, difficiles à contrôler pour les autorités compétentes, qui perpétuent et amplifient les discriminations existantes.

En outre, la notion de « comportement suspect » n'est pas définie dans la loi Jeux olympiques et paralympiques 2024, les situations prédéterminées ayant été précisées par un décret ultérieur. La VSA permet donc de catégoriser les comportements des individus selon une norme et des paramètres déterminés par les concepteurs et utilisateurs de ces outils. Cette technologie relève ainsi du contrôle social, à rebours des droits fondamentaux. Elle porte atteinte au droit à la vie privée, au principe de non-discrimination, ainsi qu'aux libertés fondamentales.

Les algorithmes évaluent des situations, en analysant des données corporelles et comportementales, qui sont des données personnelles protégées.

L'effet dissuasif d'une telle surveillance de l'espace public comporte également un risque d'auto-censure, pouvant notamment amener les personnes à ne pas exercer leur droit à la liberté d'expression.

Enfin, ces technologies ne sont pas exemptes de biais discriminatoires, qui pourraient être amplifiés par l'automatisation de la surveillance. Des groupes déjà marginalisés pourraient être ciblés de manière disproportionnée par cette surveillance.

En mai 2023, la France est devenue le premier État membre de l'Union européenne à légaliser de tels dispositifs, s'éloignant ainsi de plus en plus des droits humains pour épouser la culture de la surveillance de masse de pays autoritaires tels que la Russie, la Chine, et le Qatar, qui ont eux aussi profité d'événements sportifs pour normaliser ces technologies. À partir de l'expérience de la VSA, et faute de gardes fous établis par la loi, la France pourrait bien confirmer sa place de pionnière de la surveillance de masse en Europe, en normalisant ces outils et en ouvrant la voie à l'usage de technologies biométriques, dont la reconnaissance faciale fait partie.

Les données biométriques et le régime qui leur est applicable sont définis dans le règlement (UE) 2016/679 du 27 avril 2016, dit règlement général de protection des données (RGPD), retranscrit en France par la loi n° 78-17 du 6 janvier 1978. Sont des données biométriques les « données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, psychologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique ». L'article 9 du RGPD, repris par l'article 6 de la loi n° 78-17 du 6 janvier 1978 interdit entre autres le traitement des données personnelles qui révèlent l'origine raciale ou ethnique, ou encore les données biométriques aux fins d'identifier une personne physique de manière unique. Il interdit donc en principe la reconnaissance faciale, qui consiste au traitement technique de ces données (selon le Comité européen de la protection des données EDPB). Cependant, cette interdiction peut faire l'objet d'exceptions au titre du même article 9 du RGPD, auquel renvoie l'article 6 de la loi n° 78-17 du 6 janvier 1978. C'est le cas notamment si le traitement est « nécessaire pour des motifs d'intérêt public important ». En vertu du III de l'article 6, ces exceptions valent également pour « les traitements automatisés justifiés par l'intérêt public ».

Ainsi, et bien que la reconnaissance faciale ne soit expressément autorisée par aucun texte à ce jour, elle relève toutefois de ce régime qui connaît de nombreuses exceptions. Elle pourrait donc dans les faits être autorisée. Outre cette possibilité légale, le développement de la reconnaissance faciale est aussi une possibilité technique. Ces outils reposent sur les mêmes algorithmes d'analyse d'images que les logiciels de VSA. Ils sont généralement développés par les mêmes sociétés, et il suffit souvent d'activer une simple option.

Faute d'interdiction claire, ces dispositifs pourraient envahir les espaces publics et accessibles au public au détriment de nos droits. Les organisations non gouvernementales (ONG) comme Amnesty International ont largement documenté les risques que la reconnaissance faciale fait peser sur les droits humains et demandent pour cette raison son interdiction explicite et totale, c'est-à-dire sans exception. L'ère de surveillance généralisée et de surveillance ciblée discriminatoire qu'elle ouvrirait est en effet incompatible avec les droits et libertés fondamentaux. L'usage de ces logiciels, conçus pour identifier et suivre des personnes où qu'elles aillent et à grande échelle dans l'espace public, y compris en l'absence d'infraction, ne peut qu'avoir un effet dissuasif sur le bon exercice des libertés d'expression (article 11 de la Déclaration des droits de l'Homme et du citoyen de 1789), de réunion pacifique (article 11 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales) dont découle la liberté de manifestation (Conseil constitutionnel, décision du 4 avril 2019), ainsi que de la liberté de circulation (articles 2 et 4 de la DDHC). La Commission nationale de l'informatique et des libertés (CNIL) confirme que la reconnaissance faciale risque d'attenter à la liberté d'aller et venir anonymement. Au-delà de cet effet d'autocensure, une technologie visant à identifier et tracer les individus ne peut que renforcer le mouvement de répression et de criminalisation de manifestations pacifiques déjà en cours (Défenseure des droits, rapport pour 2023).

Le respect du droit au respect de la vie privée (article 8§1 de la CESDH), qui doit aussi être garanti dans l'espace public (Conseil constitutionnel, décision du 23 juillet 1999), et dont découle le droit à la protection des données personnelles, est en jeu. À l'instar des libertés d'expression et de réunion, le droit à la vie privée peut connaître certaines restrictions. Celles-ci doivent être proportionnées et nécessaires dans une société démocratique à la sauvegarde de certains objectifs légitimes. Or, la surveillance par reconnaissance faciale implique une collecte à grande

échelle de données qui ne peut, par définition, reposer sur cet examen de proportionnalité. Son usage est donc toujours une atteinte à nos droits.

À la surveillance de masse liberticide s'ajoute la surveillance ciblée discriminatoire. Ces outils identifient et catégorisent les personnes en fonction de leurs caractéristiques physiques, y compris des attributs protégés qui peuvent être observés ou déduits, tels que la couleur de peau, l'ethnie ou religion supposée, le handicap ou le genre. Les personnes déjà structurellement discriminées sur la base de ces caractéristiques seront donc particulièrement vulnérables à la généralisation de ces dispositifs. Les évolutions historiques du maintien de l'ordre montrent que l'utilisation expérimentale de technologies de surveillance incrimine d'abord les populations marginalisées, notamment les populations de couleur déjà victimes du racisme structurel. Le Comité des Nations Unies pour l'élimination de la discrimination raciale l'a confirmé en 2019 : la reconnaissance faciale fait courir à certains groupes un risque disproportionné d'atteinte à leur liberté de se réunir ou de s'associer librement. Enfin, et étant donné le paradigme sécuritaire et répressif qui gouverne la gestion des migrations en France et en Europe, ces technologies seront aussi sans doute employées pour cibler les personnes exilées, déjà contraintes de devoir céder leurs données biométriques aux frontières françaises et européennes. Ces effets de biais sont inhérents aux logiciels de reconnaissance faciale, qui sont basés sur l'apprentissage automatique et donc pensés à partir des biais intrinsèques de leurs concepteurs, comme le montre la Déclaration de Toronto de 2018. Par la différence de traitements qu'ils vont générer, ces logiciels sont donc en contradiction directe avec le principe d'égalité, socle de notre identité républicaine et protégé par notre Constitution, dès son article 1er. De ce droit découle le droit à ne pas être discriminé, consacré par les textes internationaux ratifiés par la France, tels que le Pacte international relatif aux droits civils et politiques, la Charte des droits fondamentaux de l'Union Européenne, ou encore la Convention européenne des droits de l'Homme.

Interdire la reconnaissance faciale reviendrait donc à refuser un modèle de société de suspicion, de contrôle et d'autocensure, mais aussi le renforcement des discriminations à l'égard de certains groupes. En dépit de ces évidences documentées, les expérimentations de cette technologie se multiplient en France, comme l'a documenté Amnesty international. En 2019, la ville de Nice a mené la première expérimentation de reconnaissance faciale en France lors de son carnaval, via le logiciel israélien Anyvision, impliquant tardivement la CNIL. En 2018, la région Provence-Alpes-Côte-d'Azur a souhaité déployer des dispositifs de

reconnaissance faciale dans deux lycées, à Nice et à Marseille notamment à des fins de “suivi de trajectoire” des lycéens et visiteurs, avant que le tribunal administratif de Marseille n’annule finalement le dispositif. Le secteur privé ne rechigne pas non plus à mener de telles expérimentations. En 2020, le club de football FC Metz aurait testé cette technologie lors d’un match afin notamment d’identifier à leur insu les spectateurs interdits de stade. Seule une interdiction totale prévue par la loi permettra d’éviter que ces expérimentations, souvent menées sans une information suffisante du public, ne se généralisent et se normalisent.

Interdire la reconnaissance faciale est d’autant plus impératif et urgent que le gouvernement français montre un attrait certain pour le développement de la surveillance biométrique. Lorsque l’interdiction des technologies d’identification biométrique à distance s’est posée au Conseil de l’Union européenne à l’occasion des discussions pour un règlement européen sur l’intelligence artificielle (AI Act), adopté en mars 2024, le gouvernement a activement plaidé pour introduire des exceptions liées à la sécurité nationale. Surtout, ce dernier s’est montré particulièrement timoré lorsqu’en novembre 2023 une enquête du média Disclose a révélé que la police nationale utilise depuis 2015, en dehors de tout cadre légal et sans en informer la CNIL, le logiciel de VSA et de reconnaissance faciale israélien Briefcam sur lequel la fonction reconnaissance faciale est activée par défaut depuis 2018. À ce jour, aucune décision ni sanction n’a été prise quant à l’usage illégal de ce dispositif, malgré la promesse faite par le ministre de l’intérieur d’ouvrir une « enquête administrative indépendante » dont les conclusions devaient être rendues publiques sous trois mois. En mai 2024, enfin, le Président de la République Emmanuel Macron a confirmé sa volonté de faire de l’intelligence artificielle son nouveau cheval de bataille, en annonçant que Paris accueillerait l’édition 2025 du sommet sur l’IA. De l’aveu même du ministre de l’économie et des finances, « la France a fait le choix d’être le pays leader en Europe sur l’IA ».

Enfin, ne pas interdire la reconnaissance faciale reviendrait également à laisser aux entreprises conceptrices le soin de définir ce qui relève du comportement « anormal » dans l’espace public. Cela équivaudrait à poursuivre une logique de privatisation et de marchandisation de la sécurité publique, prérogative régalienne par excellence. Au contraire de cette logique de casse des services publics, que le groupe La France Insoumise dénonçait déjà lors de la légalisation de la VSA, nous pensons que seuls des moyens humains suffisants de police et d’investigation, entraînés et formés, y compris à la protection des droits et libertés, sont qualifiés pour

assurer la sûreté de toutes et tous dans le respect de la vie privée. Les chiffres de la lutte contre le terrorisme mis en avant par la Direction générale de la sécurité intérieure (DGSI) le corroborent : entre 2013 et 2019, 98 % des attentats qui ont été empêchés en France l'ont été grâce aux renseignements humains.

PROPOSITION DE LOI

Article unique

① Après l'article 2 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, il est inséré un article 2 *bis* ainsi rédigé :

② « *Art. 2 bis* – Il est interdit d'installer, d'activer ou d'utiliser une technologie de reconnaissance faciale à des fins d'identification d'une personne physique de manière unique.

③ « Constitue la reconnaissance faciale toute technologie basée sur le traitement automatisé de données biométriques du visage aux fins d'établir l'identité d'une personne ou de l'authentifier par comparaison des données biométriques de cette personne avec les données biométriques de personnes stockées dans une base de données de référence, que la personne ait donné ou non son approbation ».