La Quadrature du Net

La Quadrature du Net

Mesdames et Messieurs les député·es,
Assemblée nationale
126, rue de l'Université
75007 Paris

Paris, le 22 novembre.

Objet : Note sur l'article 9 de la proposition de loi relative au renforcement de la sûreté dans les transports

Mesdames et Messieurs les député·es,

La proposition de loi relative au renforcement de la sûreté dans les transports que vous vous apprêtez à examiner contient un article 9 prévoyant une nouvelle expérimentation de vidéosurveillance algorithmique (VSA) en France dans le cadre de réquisitions judiciaires.

Au regard de l'état de l'art de ces technologies, couplé au travail de documentation établi par La Quadrature du Net depuis plusieurs années, il apparaît que ce texte vise en réalité à légaliser l'utilisation de logiciels d'analyse, de filtrage et de sélection de personnes en fonction de leurs attributs biométriques, de la même manière que le fait la solution commercialisée par la société Briefcam.

Si cette nouvelle forme de surveillance venait à être adoptée, elle rentrerait directement en contradiction avec le droit de l'Union européenne et exposerait la France à un risque de sanction par la Cour de justice de l'Union européenne. De plus, au prétexte de l'innovation technologique, cette nouvelle expérimentation minore les atteintes aux libertés fondamentales et accentue la répression et la normalisation de la surveillance massive et automatisée de l'espace public.

I. Éléments de compréhension technique

La vidéosurveillance algorithmique repose sur l'analyse et l'exploitation de données personnelles, lesquelles incluent des données biométriques. Les algorithmes de VSA ne sont pas des outils magiques : ils ne font qu'appliquer une série d'instructions. Contrairement à ce que la notion d'« intelligence artificielle » tendrait à faire croire, la machine ne « voit » pas.

Un algorithme de VSA ne fait pas de distinction consciente entre une personne humaine, une benne à ordures ou une voiture. Pour lui, il n'y a que des images composées d'un certain nombre de pixels de couleurs différentes. Les concepteurs des algorithmes doivent recourir à des méthodes probabilistes capables de l'aider à détecter une empreinte – c'est-à-dire une combinaison mathématique entre des positions de pixels les uns par rapport aux autres et leur couleur – pour la rattacher à une appellation précise : par exemple « voiture », « individu humain », « valise », « ordure », voire des catégories plus précises comme « humain avec un haut de couleur rouge et un pantalon de couleur bleue ».

Or, même sans recourir aux empreintes faciales des individus (reconnaissance faciale), plusieurs méthodes de VSA permettent de suivre une personne précise – par exemple à travers la couleur de ses vêtements ou d'autres attributs physiques – à mesure qu'elle évolue dans un espace urbain et passe dans le champ de vision de différentes caméras. **Dès lors que les algorithmes de VSA permettent de retrouver une personne au milieu d'autres à partir de données physiques ou comportementales qui lui sont propres, il s'agit d'identification biométrique**. Ainsi, les algorithmes dits « de filature automatisée » ou « de réidentification » permettent de retrouver une même personne sur plusieurs images à partir de ses attributs physiques et comportementaux. Ces algorithmes procèdent par comparaison entre deux images de vidéosurveillance (deux caméras différentes ou deux moments différents sur une même caméra) afin de pouvoir établir des correspondances entre elles et, ainsi, soit retracer le chemin de la personne lors de son parcours devant plusieurs caméras, soit reconnaître qu'il s'agit bien de la même personne à deux moments distincts, éloignés dans le temps. Pour ce faire, le logiciel dresse là-aussi une **empreinte de la personne, basée sur la combinaison d'une multitude de caractéristiques** qu'il est en mesure de repérer chez une personne, comme le type et la couleur de ses vêtements, sa silhouette, sa taille, la couleur de sa peau, ses accessoires, et bien d'autres. Cette empreinte créée est alors unique par rapport à l'échantillon de toutes les autres personnes filmées.

Ces algorithmes, bien qu'illégaux en l'état actuel du droit, sont déjà largement déployés et utilisés par les forces de l'ordre et des entreprises comme la SNCF ou la RATP. On les retrouve par exemple dans un projet européen dénommé « Prevent PCP », déployé à Paris et Marseille pour détecter des bagages abandonnés et qui fait l'objet d'une instruction par la CNIL suite à une plainte de La Quadrature du Net[1]. En effet, la méthodolgie utilisée pour établir qu'un bagage est bien abandonné suppose de traiter les données biométriques de toute personne qui est filmée : dans un premier temps pour détecter la situation où un objet « bagage » se détache d'un objet « personne humaine » (c'est la détection de l'abandon) puis, dans un second temps, pour retracer le parcours de la personne propriétaire du bagage dans la gare (c'est la détection du non-retour de la personne auprès du bagage abandonné). Pour cela, l'ensemble des données biométriques des voyageurs sont utilisées et l'appellation « suivi de bagage » fait oublier que c'est avant tout l'humain qui est suivi.

On retrouve également cette surveillance par attributs physiques dans le logiciel « Vidéo Sy-

1. La plainte est accessible en ligne à l'adresse suivante : `https://www.laquadrature.net/wp-content/uploads/sites/8/2024/05/01-LQDN_CNIL_Plainte_Prevent_PCP_anon.pdf`.

nopsis » commercialisé par la société Briefcam. Cette solution d'analyse vidéo est utilisée dans plus de 200 villes en France [2] et a été acquise par la police nationale en 2015 puis par la gendarmerie nationale en 2017. Suite aux révélations du média d'investigation Disclose [3] démontrant que la fonctionnalité de reconnaissance faciale de ce logiciel avait été utilisée, le ministre de l'Intérieur a commandé à l'Inspection générale de l'administration, l'Inspection générale de la gendarmerie nationale et l'Inspection générale de la police nationale un rapport d'évaluation, récemment publié [4], faisant état de l'utilisation de ce logiciel. Ce rapport cite un exemple concret permettant d'illustrer parfaitement comment des attributs physiques, ici un vêtement, suffisent à reconnaître, individualiser puis interpeller une personne :

> « *Dans le cadre d'une enquête visant à identifier et rechercher l'auteur d'une agression violente en scooter, les images de vidéoprotection de l'agression, trop éloignées de la scène et de qualité insuffisante ne permettent pas d'identifier visuellement l'auteur. Les enquêteurs observent toutefois qu'il est porteur d'un T-shirt bicolore, d'un graphisme particulier.* ***C'est la fonctionnalité "similitude d'apparence" qui a donc été activée****, avec la saisie judiciaire récurrente, dans les jours qui ont suivi l'agression, des vidéos de la ville, ensuite injectées dans BriefCam. Une séquence vidéo horodatée sur laquelle, près de dix jours après l'agression, apparaissait un individu portant un* ***T-shirt identique à celui de l'auteur*** *a, grâce à l'activation de cette fonctionnalité, été sélectionnée par BriefCam. Les investigations alors menées dans le secteur considéré permettront* ***d'identifier et d'arrêter****, sur le fondement de la similitude d'apparence, l'auteur de l'agression. L'emploi du logiciel et, en l'occurrence, de cette fonctionnalité, a été ici la condition sine qua non de l'interpellation de l'individu, à partir de l'injection systématique, sur réquisition judiciaire, pendant les jours ayant suivi l'agression, de centaines d'heures de vidéos saisies* » (encadré n° 3, page 35)

Contrairement à la machine, **le droit fait la différence entre les données qui constituent l'empreinte d'un objet et celles qui constituent l'empreinte d'une personne humaine**. Ces données, considérées comme sensibles lors qu'elles se rapportent à l'empreinte physiques d'une personne humaine, bénéficient d'une protection particulière. Il n'est alors pas possible de nier le caractère biométrique des données traitées par ces algorithmes sous peine d'aller à l'encontre des protections exigées par le droit.

2. Thomas Jusquiame, « Les cuisines de la surveillance automatisée », Le Monde diplomatique, février 2023, URL : https://www.monde-diplomatique.fr/2023/02/JUSQUIAME/65535.

3. Mathias Destal, Clément Le Foll et Geoffrey Livolsi, « La police nationale utilise illégalement un logiciel israélien de reconnaissance faciale », Disclose, 14 novembre 2023, URL : https://disclose.ngo/fr/article/la-police-nationale-utilise-illegalement-un-logiciel-israelien-de-reconnaissance-faciale/.

4. « Usage de logiciels d'analyse vidéo par les services de la police et la gendarmerie nationales », février 2024, URL : https://www.interieur.gouv.fr/content/download/137154/1085003/file/23114R%20-%20Breifcam.pdf.

II. Cadre juridique

A. Définition et modalités de traitement des données sensibles

En France, le règlement UE n° 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après « RGPD ») ainsi que la directive n° 2016/680 du 27 avril 2016 (ci-après directive « police-justice ») transposée au titre III de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après « loi Informatique et Libertés »), constituent le corpus législatif relatif à la protection des données personnelles. Celui-ci prévoit les conditions et modalités selon lesquelles un traitement de données personnelles peut être effectué de façon légale.

Parmi ces règles, le droit des données personnelles prévoit une catégorie juridique particulière pour les données personnelles dites « sensibles », car particulièrement révélatrices de l'intimité des personnes, qui comprend notamment, selon l'article 6 de la loi Informatique et Libertés, les données qui « *révèlent* […] *les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique* », ainsi que « [l]*es données génétiques,* [l]*es* ***données biométriques*** *aux fins d'identifier une personne physique de manière unique,* [l]*es données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique* ».

Le traitement de ces données est interdit par principe par la loi Informatique et Libertés, et autorisé uniquement selon quelques exceptions. Il s'agit d'une stricte application des articles 9 du RGPD et 10 de la directive « police-justice ». Comme l'a rappelé la Cour de justice de l'Union européenne dans son arrêt *Ministerstvo na vatreshnite raboti* (*cf.* CJUE, 26 janvier 2023, aff. C-205/21) :

> « *116. L'article 10 de la directive 2016/680 constitue une disposition spécifique régissant les traitements des catégories particulières de données à caractère personnel, y compris les données biométriques et génétiques. Ainsi qu'il ressort de la jurisprudence, la finalité de cet article est d'assurer une* ***protection accrue*** *à l'égard de ces traitements qui, en raison de la sensibilité particulière des données en cause et du contexte dans lequel elles sont traitées, sont susceptibles d'engendrer, ainsi qu'il ressort du considérant 37 de ladite directive,* ***des risques importants pour les libertés et les droits fondamentaux****, tels que le droit au respect de la vie privée et le droit à la protection des données à caractère personnel, garantis par les articles 7 et 8 de la Charte* »

Les données sensibles ne peuvent donc être traitées que **selon quelques exceptions prévues par les textes**. De plus, ces traitements ne peuvent être mis en oeuvre qu'en cas de « nécessité absolue ». Pour la Cour, cette exigence doit être interprétée « *comme définissant des* ***conditions renforcées*** *de licéité du traitement des données sensibles* » par rapport aux règles relatives aux

traitements de données « classiques ».

Elle explique ainsi que « *d'une part, l'emploi de l'adverbe "uniquement" devant l'expression "en cas de nécessité absolue" souligne que le traitement de catégories particulières de données, au sens de l'article 10 de la directive 2016/680, ne pourra être considéré comme nécessaire que dans un nombre limité de cas. D'autre part, le caractère "absolu" de la nécessité d'un traitement de telles données implique que cette nécessité soit appréciée de manière* ***particulièrement rigoureuse***. » (*op. cit.*, §§ 117 et 118).

Dans ce même arrêt, la CJUE rappelle en particulier que « *l'exigence de nécessité est remplie lorsque l'objectif poursuivi par le traitement de données en cause* ***ne peut raisonnablement être atteint de manière aussi efficace par d'autres moyens moins attentatoires*** *aux droits fondamentaux des personnes concernées, en particulier aux droits au respect de la vie privée et à la protection des données à caractère personnel garantis par les articles 7 et 8 de la Charte [...]* » (*op. cit.*, § 126). Et lorsque des données biométriques sont traitées et que n'est donc plus seulement exigée une « nécessité » mais bien une « nécessité absolue », la Commission européenne souligne que cela n'est possible que lorsqu'il est « ***totalement impossible****, d'atteindre l'objectif du traitement par d'autres moyens* »[5].

En résumé, le traitement de donnée sensibles doit respecter un régime strict de proportionnalité et de prévisibilité de la loi.

B. Définition des données biométriques

Parmi les données sensibles, on trouve les données biométriques qui sont définies par le 14 de l'article 4 de la directive « police-justice » et l'article 6 de la loi Informatique et Libertés comme désignant des données « *résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales* ».

Trois conditions cumulatives sont donc nécessaires pour qu'un dispositif puisse être qualifié de traitement de données biométriques : il faut qu'il y ait un traitement spécifique, qui analyse des caractéristiques physiques, physiologiques ou comportementales des personnes, et qui vise à identifier ces dernières de manière unique.

Un traitement technique spécifique s'entend comme incluant tout type d'algorithme ou programme informatique qui serait appliqué aux flux vidéos pour isoler, caractériser, segmenter ou encore rendre apparente une information relative à une personne physique filmée. Ce traitement peut également consister à extraire du flux vidéo, même *a posteriori*, des données biométriques de

5. Observations écrites à la Cour de justice de l'UE présentée par la Commission européenne dans l'affaire C-205/21, *Ministerstvo na vatreshnite raboti*, pt. 44, URL : `https://www.asktheeu.org/en/request/ec_written_observations_in_c_205`.

cette personne.

En ce qui concerne **l'analyse des caractéristiques physiques ou physiologiques**, celles-ci peuvent se rapporter au corps d'une personne filmée au sens large, tels que des visages, des silhouettes ou toute caractéristique isolée du corps, telle la couleur des cheveux, la couleur des yeux, la forme du visage, la taille, le poids, l'âge. Les données comportementales, quant à elles, visent toute information relative à l'action du corps dans l'environnement et l'espace. Pourront être qualifiés de biométriques **un vêtement ou accessoire** portés par la personne à un instant *t*, un geste, une expression d'émotion, une direction de déplacement, une position dans l'espace et le temps (assis, debout, statique, allure de la marche, etc.).

En ce qui concerne **l'identification unique**, celle-ci **n'implique pas nécessairement de révéler l'état civil d'une personne** mais, plus largement, de pouvoir l'individualiser au sein d'un groupe, généralement afin de lui appliquer des mesures spécifiques (les versions anglaises de la directive « police-justice » et du RGPD utilisent l'expression « *single out* »).

Le **Comité européen de la protection des données** (ci-après le « CEPD »), autorité européenne chargée de garantir l'application effective des règles européennes en matière de données personnelles, a détaillé, dans ses lignes directrices n° 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo[6], ce qu'il faut entendre par « identification unique ». Au point 82, le CEPD qualifie de traitement de données biométriques un traitement permettant de suivre le trajet d'une personne entre plusieurs zones à partir de ses caractéristiques physiques, et sans que cela n'implique de pouvoir en connaître l'état civil :

> « *Toutefois, l'article 9* [du RGPD et, *mutatis mutandis*, l'article 10 de la directive « police-justice »] *s'applique si le responsable du traitement conserve des données biométriques* [...] *afin d'identifier une personne de manière unique. Si un responsable du traitement souhaite détecter une personne concernée qui pénètre à nouveau dans l'espace surveillé ou dans une autre zone* [...] *la finalité serait alors d'identifier de manière unique une personne physique, ce qui signifie que l'opération relèverait d'emblée de l'article 9* [...]. *Dès lors que le système se fonde sur l'analyse de caractéristiques physiques pour détecter des personnes spécifiques qui entrent dans le champ de la caméra (comme les visiteurs d'un centre commercial) et les suivre, il constitue une méthode d'identification biométrique, car il vise la reconnaissance par l'utilisation d'un traitement technique spécifique.* »

En effet, comme expliqué précédemment, même sans recourir aux empreintes faciales des individus (reconnaissance faciale), plusieurs méthodes de VSA permettent de suivre une personne précise – par exemple à travers la couleur de ses vêtements ou sa démarche – à mesure qu'elle évolue dans un espace urbain et passe dans le champ de vision de différentes caméras. Cette capacité

6. Disponible en ligne à l'adresse suivante : `https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_fr.pdf`.

de suivi des personnes repose sur des algorithmes dits de « réidentification ».

Le **Défenseur des droits** interprète de façon similaire cette définition de « traitement biométrique ». Dans son enquête sur la « Perception du développement des technologies biométriques en France » publiée en octobre 2022[7], l'institution estime que les traitements de données biométriques doivent, au sens du droit européen des données personnelles, s'entendre notamment comme l'identification ou l'évaluation des personnes.

L'identification consiste à « ***retrouver une personne au sein d'un groupe d'individus**, dans un lieu, sur une image, ou dans une base de données à partir notamment des traits du visage (reconnaissance faciale), de la voix (reconnaissance du locuteur), du comportement (reconnaissance de la démarche) ou de tout autre type de données biométriques.* » L'évaluation quant à elle, vise notamment à « *inscrire la ou les personnes visées dans des **catégories spécifiques**, par exemple de sexe, d'âge, de couleur de cheveux, de couleur des yeux, d'origine ethnique ou d'orientation sexuelle ou politique en vue de prendre des mesures spécifiques (on parle alors de systèmes de "catégorisation")* », à partir du moment où les données traitées pour cette évaluation sont « *des données corporelles et/ou issues de systèmes biométriques* » (page 3).

Au sein de la **doctrine juridique** telle qu'elle ressort des travaux universitaires, différents chercheurs en droit ayant abordé cette question abondent dans le même sens. Caroline Lequesne, maîtresse de conférences en droit public à l'Université Côte d'Azur, a co-publié un livre blanc en 2023 intitulé « *Surveiller les foules* » qui formule des propositions pour encadrer les intelligences artificielles qu'elle appelle « physiognomoniques », c'est-à-dire les technologies de surveillance permettant d'identifier les individus dans les espaces accessibles au public, notamment à partir de leurs données biométriques. Caroline Lequesne y explique que ces systèmes « *recouvrent* [...] *les technologies de reconnaissance faciale, émotionnelle, comportementale et de nombreux dispositifs entourant la vidéo surveillance dite "intelligente". Le choix d'aborder ces technologies dans un même mouvement, et sous l'empire d'une catégorie commune, procède de motifs d'ordre divers. D'une part, d'un point de vue technologique, ces systèmes ne se distinguent pas tant en termes de nature qu'en termes de degrés ; **ils recourent aux mêmes dispositifs techniques** et répondent le plus souvent aux mêmes finalités sécuritaires* » (voir page 14 du livre blanc).

Plus récemment, Robin Médard Inghilterra, maître de conférence à l'Université Paris I, a publié dans la Revue des droits de l'Homme un article intitulé « L'instauration d'une "technopolice" administrative en milieu urbain : les droits et libertés sur un fil »[8]. Ce juriste constate qu'une version « *douce des usages de la biométrie dans l'espace public s'est déjà frayé un chemin en France sous les traits de la VSA.* » Pour lui, l'exclusion de la qualification du caractère biométrique de la VSA dans la loi relative aux Jeux Olympiques ne s'applique qu'au dispositif ainsi défini :

7. Disponible en ligne à l'adresse suivante : `https://www.defenseurdesdroits.fr/sites/default/files/2023-07/ddd-enquete-perception-du-developpement-des-technologies-biom%C3%A9triques-en-France-20221004.pdf`

8. Disponible à l'adresse suivante : `https://journals.openedition.org/revdh/19033`.

> « *Elle n'exclut pas, en revanche, que soient qualifiés de biométriques des usages de la VSA accomplis grâce aux logiciels acquis par les collectivités territoriales et leurs groupements, qui les mobilisent en dehors de l'expérimentation de la loi JOP, sur réquisitions ou non, à des fins de police administrative ou de police judiciaire.* ***Or, les fonctionnalités biométriques de ces logiciels sont patentes****. À titre d'illustration, le logiciel de VSA commercialisé par BriefCam, qui équipe déjà des dizaines de collectivités, comprend un module Review qui permet un traitement différé de l'image pour afficher simultanément des évènements survenus à différents moments. Il autorise la recherche multicaméras d'"objets" (personnes ou véhicules) ayant une "similarité d'aspect". Plusieurs filtres permettent de singulariser des personnes au sein d'une "classe" (homme, femme, enfant), comme les attributs, qu'il s'agisse d'un sac (sac à dos, sac à main), d'un chapeau, d'un vêtement (sans manches, à manches courtes, à manches longues, short/jupe, pantalon), le cas échéant d'une couleur et d'une taille déterminés. Dans ce cas,* ***la qualification de biométrie ne saurait être écartée****. Il y a bien, par l'apposition de ces différents filtres, singularisation d'une personne au sein d'un environnement, et donc identification unique, après traitement technique spécifique de données physiques, physiologiques ou comportementales* ». (§ 31)

Ainsi, la qualification juridique de traitement des données biométriques **ne se limite aucunement à la reconnaissance faciale mais inclut toute analyse et catégorisation de personnes en fonction de leurs attributs physiques, physiologiques et comportementaux**, dès lors qu'elles visent à les identifier et singulariser dans un environnement.

III. Conséquences pour l'examen de la proposition de loi

Il convient de tirer les conclusions nécessaires des éléments techniques et juridiques détaillés ci-dessus pour l'examen de l'article 9 de la proposition de loi relative au renforcement de la sûreté dans les transports.

Pour rappel, le I de cet article propose d'autoriser les services internes de sécurité de la SNCF et de la RATP à « *mettre en œuvre des logiciels de traitement de données non biométriques pour extraire et exporter les images ainsi réquisitionnées* ». D'autre part, le V de cet article 9 dispose que ces traitements « *n'utilisent aucun système d'identification biométrique, ne traitent aucune donnée biométrique et ne mettent en œuvre aucune technique de reconnaissance faciale* ». Il y a là une contradiction flagrante et insurmontable.

En effet, les traitements algorithmiques comportant des fonctionnalités d'analyse, d'individualisation et de reconnaissance par les attributs physiques, physiologiques et comportementaux (tel que le logiciel proposé par l'entreprise Briefcam ou ceux utilisés par la SNCF ou la RATP dans le cadre de Prevent PCP) ne peuvent constituer juridiquement « *des traitements de données non biométriques* », comme l'affirme pourtant la formulation de ces dispositions.

Dès lors, si le texte venait à être adopté en l'état, non seulement il comporterait en son sein des dispositions contradictoires et vides de sens mais, surtout, il ne respecterait pas les exigences prévues par le droit de l'Union européenne concernant le traitement des données sensibles, notamment l'exigence de démontrer une nécessité absolue. **La France s'exposerait donc directement à une sanction par la Cour de justice de l'Union européenne.**

IV. D'autres atteintes disproportionnées aux libertés fondamentales

Enfin, au-delà de cet examen juridique de la notion de biométrie, il est crucial pour votre commission d'avoir à l'esprit les nombreuses conséquences sociales et sociétales qu'engendre la multiplication des dispositifs des surveillances algorithmiques dans l'espace public. La Quadrature du Net avait déjà alerté le Parlement lors de l'examen du projet de loi relatif aux Jeux olympiques et paralympiques de 2024[9]. Ces inquiétudes n'ont pas changé ; au contraire, elles se sont renforcées.

Du point de vue des libertés publiques, l'analyse biométrique des corps va frontalement **contre l'idée du droit à la vie privée et à la protection de ses données personnelles**. Comme l'a rappelé la CNIL dans son avis sur le projet de loi relatif aux Jeux Olympiques, « *le déploiement, même expérimental, de ces dispositifs constitue un tournant qui va contribuer à définir le rôle général qui sera attribué à ces technologies, et plus généralement à l'intelligence artificielle* »[10]. Cette même institution avait d'ores et déjà expliqué dans sa position sur la VSA en temps réel de 2022 que « *des risques importants pour les libertés individuelles et collectives existent du simple fait de la multiplication, actuelle et anticipée, des dispositifs de vidéo "augmentée" qui pourrait aboutir à un sentiment de surveillance généralisée* »[11].

De plus, la VSA porte **atteinte au droit à la liberté d'expression et à la liberté d'aller et venir** qui sont exercées dans l'espace public. En effet, ces dispositifs rendent impossible, par nature, la jouissance par les personnes concernées de ces droits constitutionnellement protégés : par cette surveillance permanente et systématique de l'espace public, le seul moyen de se soustraire à l'analyse comportementale induite est de ne pas circuler dans l'espace public. Par ailleurs, dans la mesure où une mesure de surveillance a un effet dissuasif avéré sur les personnes surveillées et constitue une atteinte grave à la liberté d'expression, une surveillance généralisée implique une négation par nature de cette même liberté.

Également connu sous le nom de « *chilling effect* », Robin Medard Inghilterra explique que

9. Voir le dossier d'analyse du 17 février 2023 disponible à l'adresse suivante : `https://www.laquadrature.net/wp-content/uploads/sites/8/2023/02/Dossier-VSA-2-LQDN.pdf`

10. Délibération n° 2022-118 du 8 décembre 2022 portant avis sur un projet de loi portant sur les jeux Olympiques et Paralympiques de 2024 (demande d'avis n° 22017438), disponible en ligne à l'adresse suivante : `https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046865563`.

11. CNIL, « Caméras dites « intelligentes » ou « augmentées » dans les espaces publics – Position sur les conditions de déploiement », juillet 2022, page 9, disponible à l'adresse suivante : `https://www.cnil.fr/sites/cnil/files/atoms/files/cameras-intelligentes-augmentees_position_cnil.pdf`.

« *cette autocensure limite l'occurrence de comportements dont certains pourraient s'avérer illégaux, mais dont la plupart sont parfaitement légaux. La renonciation est simplement motivée par la peur que ces comportements deviennent préjudiciables, en raison d'une instrumentalisation postérieure ou d'une perception défavorable liée à leur dimension controversée, clivante, militante ou radicale* » (*op. cit.*, § 41). La CNIL avait d'ailleurs pris en compte cet effet lors de son contrôle du projet de surveillance sonore dans les rues de Saint-Étienne. Elle avait estimé que les libertés d'expression, de réunion, de manifestation, d'association, comme la liberté d'aller et venir étaient menacées, considérant que « *les personnes concernées peuvent être amenées à* ***altérer leur comportement*** *par exemple en censurant eux-mêmes leurs propos tenus sur la voie publique ou encore en modifiant leurs déplacements* [...] *pour éviter les zones d'installation de capteurs sonores* »[12].

Enfin, le Conseil constitutionnel considère qu'une mesure de surveillance a un effet dissuasif sur l'exercice des libertés fondamentales, notamment la liberté d'expression, et exige du législateur qu'il trouve un juste équilibre avec les objectifs à valeur constitutionnelle poursuivis (Cons. const., 27 décembre 2019, *Loi de finances pour 2020*, n° 2019-796 DC, pt. 83, *in fine*), ce qui n'est manifestement pas le cas avec un dispositif de surveillance continue et systématique tel qu'un dispositif de VSA (v., pour analogie, Cons. const. 25 février 2022, *M. Habib A. et autre*, n° 2021-976/977 QPC, pt. 12).

La légalisation d'un nouveau dispositif de surveillance algorithmique ne peut donc être abordée uniquement sous le prisme de l'efficacité technologique, des intérêts économiques ou d'une demande « pragmatique » du terrain. Recourir à l'analyse et l'identification algorithmique des corps humains dans l'espace public, même de façon expérimentale, aura des conséquences majeures sur les droits et libertés des personnes. La France est aujourd'hui le premier pays de l'Union européenne à avoir adopté des législations autorisant la surveillance algorithmique de sa population. En s'enfonçant ainsi dans une spirale techno-sécuritaire, notre pays restreint de plus en plus l'exercice des droits dans l'espace public, qui demeure pourtant un lieu crucial pour l'application des droits politiques et la constitution de relations sociales, la rapprochant davantage de régimes autoritaires que des valeurs des droits humains censées être incarnées par l'Union européenne.

Pour ces raisons, La Quadrature du Net vous invite à supprimer l'article 9 de la proposition de loi relative au renforcement de la sûreté dans les transports.

Je vous prie de croire, Mesdames et Messieurs les député·es, en l'assurance de ma plus respectueuse considération.

Pour La Quadrature du Net,

12. CNIL, courrier du 25 octobre 2019, obtenu par la Quadrature du Net, p. 5.