Benoît Piédallu
La Quadrature du Net

Claire Dujardin
Syndicat des avocats de France

Kim Reuflet
Syndicat de la magistrature

Geneviève Vidal
CREIS-TERMINAL

Patrick Baudouin
Ligue des droits de l'Homme

Monsieur le président du Conseil constitutionnel,
Mesdames et Messieurs les membres du Conseil constitutionnel

Paris, le 19 avril 2023.

Objet : Contribution extérieure de La Quadrature du Net, du Syndicat des avocats de France, du Syndicat de la magistrature, du CREIS-TERMINAL et de la Ligue des droits de l'Homme sur la loi relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions (affaire nº 2023-850 DC)

Monsieur le président,
Mesdames et Messieurs les membres du Conseil constitutionnel,

La Quadrature du Net est une association qui œuvre à la défense des libertés à l'ère du numérique. Le Syndicat des avocats de France est un syndicat professionnel qui œuvre notamment à la défense des droits et libertés publiques et individuelles. Le Syndicat de la magistrature a notamment pour objet de veiller à la défense des libertés et des principes démocratiques. Le CREIS-TERMINAL est une association de chercheurs et d'enseignants intervenant sur les sujets de l'informatique et de la société, dont la question des libertés. La Ligue des droits de l'Homme est une association qui lutte en faveur du respect des libertés individuelles en matière de traitement des données informatisées.

Durant les débats parlementaires sur le projet de loi relatif aux Jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, nos cinq associations ont attiré l'attention du public et des parlementaires sur l'article 7 (devenu l'article 10 dans la loi définitive) qui introduit en droit français la possibilité d'utiliser des traitements algorithmiques d'analyse des images de vidéosurveillance (plus communément appelé « *vidéosurveillance algorithmique* », ou VSA), sur l'article 11 (devenu l'article 16) qui prévoit la possibilité d'utiliser des scanners à ondes millimétriques à l'entrée des enceintes sportives, ainsi que sur l'article 12 (devenu l'article 17) qui conditionne l'entrée dans un lieu où se déroule une manifestation sportive à la présentation d'un titre d'entrée particulier et sanctionne de manière disproportionnée les accès illicites.

Ces articles nous semblent contraires à la Constitution. Nous avons ainsi l'honneur de vous adresser cette présente contribution extérieure afin de démontrer leur inconstitutionnalité.

I. Sur l'article 10 (article 7 du projet de loi)

L'article 10 de la loi déférée prévoit la mise en œuvre de dispositifs algorithmiques de surveillance de l'espace public. Avant de développer les ingérences créées par ces technologies dans les droits et libertés constitutionnellement garantis (B.), il apparaît nécessaire de présenter aux membres du Conseil, de façon claire et vulgarisée, les éléments techniques permettant d'appréhender pleinement le fonctionnement de cette technologie (A.).

A. En ce qui concerne les éléments techniques de compréhension de la vidéosurveillance algorithmique

La vidéosurveillance algorithmique est un procédé technologique existant depuis de nombreuses années, dont le développement – à la fois économique et scientifique – a pu être documenté. Cette documentation de l'état de l'art permet d'appréhender aujourd'hui comment les concepteurs de ces logiciels parviennent à identifier et détecter des comportements prétendument « suspects » et en déduire les problématiques politiques et juridiques qui en découlent. Nous vous en proposons un exposé synthétique [1].

1. S'agissant du vocabulaire et les définitions

Les dispositifs en cause ont pour objectif d'automatiser le travail d'analyse des images de vidéosurveillance grâce à un logiciel qui se charge de produire des notifications lorsqu'il détecte un événement qu'il a été entraîné à reconnaître. Ces logiciels sont basés sur des algorithmes dits de « *computer vision* » (vision assistée par ordinateur), une technologie basée sur l'apprentissage statistique permettant d'isoler des informations signifiantes à partir d'images fixes ou animées.

Il convient de noter que la notion de « traitement algorithmique » – utilisée à l'article 10 de la loi déférée – recouvre un très vaste champ de techniques allant de calculs statistiques simples comme une régression linéaire, à des opérations très complexes utilisant de nombreuses couches de calculs. En l'occurrence, les algorithmes ayant pour but de reconnaître une information sur une image sont généralement basés sur de l'apprentissage automatique, aussi appelé « *machine learning* » ou « *deep learning* » (parfois traduit par « apprentissage profond »).

Les vidéos sont constituées de successions d'images définies par une quantité plus ou moins grande de pixels de couleurs. Pour pouvoir faire de la reconnaissance sur ces flux vidéos, il est nécessaire de traduire ces informations (nombre de pixels, position, couleur et leurs évolutions dans le temps) en informations statistiques plus intelligibles et manipulables, appelées « caractéristiques ». Pour retrouver les éléments caractéristiques d'une image d'un objet, le statisticien analyse et identifie des caractéristiques spécifiques à cet objet. Ces caractéristiques spécifiques peuvent être les mêmes que celles qui permettent aux humains de reconnaître un objet (par exemple sa forme globale), mais il peut aussi s'agir d'autres caractéristiques moins perceptibles pour les humains mais plus faciles à identifier via des calculs ou des éléments qui ne

1. Pour des explications plus approfondies et exhaustives, voir le rapport d'analyse de La Quadrature du Net sur la vidéosurveillance algorithmique disponible à l'adresse suivante : `https://www.laquadrature.net/wp-content/uploads/sites/8/2023/02/Dossier-VSA-2-LQDN.pdf`

sont pas liés à ce qu'on pensait (par exemple un fond toujours de la même couleur). Plus on dispose de caractéristiques pertinentes, plus le modèle statistique sera précis.

La délimitation des caractéristiques n'est effectuée par un humain que dans des cas relativement simples. Le cas de la reconnaissance automatique d'évènements et de comportements tel que prévu à l'article 10 de la loi déférée est quant à lui assez compliqué et ne peut pas se satisfaire d'une détermination purement humaine des caractéristiques. En effet, la vision assistée par ordinateur nécessite d'avoir recours au « *deep learning* » car les flux vidéo contiennent de grandes quantités de variables impliquant de très nombreux calculs. Une simple image en haute définition compte plus de 2 millions de pixels : il n'est pas imaginable que toutes les dimensions que nécessite son analyse soient supervisées par un humain.

Les calculs que nécessite l'analyse de telles images sont donc effectués dans différentes couches de réseaux de neurones. Chaque couche a un rôle précis et permet de pondérer l'algorithme pour lui faire adopter différents comportements. Certains algorithmes comportent de si nombreuses couches que leur fonctionnement est opaque, y compris pour leurs concepteurs (les « *data scientists* »), qui les manipulent souvent à tâtons sans pouvoir dire exactement pourquoi tel réglage fonctionne mieux que tel autre : on se retrouve face à un divorce entre, d'un côté l'intention du programmeur et ses a priori, et de l'autre ce que la machine produit effectivement comme programme. Les ingénieurs ne peuvent avoir la main que sur la correction des erreurs du résultat (« *est-ce bien une personne qui court ?* », par exemple) et non sur le cheminement pour arriver à ce résultat (« *comment l'algorithme a déduit qu'il s'agissait d'une personne qui court ?* », par exemple).

2. S'agissant de la conception des traitements algorithmiques de vidéosurveillance

Pour avoir une meilleure compréhension des enjeux de l'usage de l'intelligence artificielle dans le cadre de la vidéosurveillance algorithmique, il convient de détailler rapidement les différentes phases qui mènent à la mise en place d'une telle technologie : le choix du jeu de données d'apprentissage (a.) ; le choix définitif des caractéristiques du modèle de l'algorithme et la phase d'apprentissage (b.) ; et le choix d'utiliser cet algorithme à des fins particulières (c.).

a. Quant au choix du jeu de données d'apprentissage

L'entraînement d'un algorithme nécessite une très grande quantité de données afin de reconnaître le comportement défini. Pour les dispositifs de vidéosurveillance algorithmique, il s'agira en l'occurrence de millions d'heures d'images de personnes filmées dans l'espace public. Ces données seront utilisées pour définir le modèle même si elles ne sont pas concernées par l'objet que l'on veut repérer (par exemple, les images de cyclistes sont nécessaires pour apprendre aux modèles qu'il ne s'agit pas de personnes en trottinette).

Le choix du jeu de données influence fortement les décisions finales de l'algorithme. En effet, il faut prendre en considération la construction de ce jeu, à savoir sa représentativité en terme de diversité de genre, d'ethnie, d'âge, etc. Le cas du logiciel COMPAS, utilisé par certaines juridictions américaines et dont l'objectif était de détecter les possibilités de récidive en fonction des éléments d'un dossier de police,

a mis en lumière les dérives de l'automatisation de la prise de décision. Le programme avait appris sur un jeu de données qui embarquait les décisions racistes du dispositif de police américain concerné, et avait déduit qu'une des caractéristiques principales liée à la récidive était la couleur de peau [2].

Cet exemple illustre un postulat propre à toute conception d'algorithme : les données réelles à partir desquelles on entraîne les machines sont des données produites par des humains et donc teintées d'opinions et portant en leur sein toutes les oppressions existant dans la société. Présenter le problème comme un « biais », c'est penser que le problème est technique alors qu'il s'agit d'un problème politique. Aucune technique n'est neutre mais est nécessairement formatée par ses conditions de production, et par l'intention de ses auteurs. Il est donc impossible d'avoir un jeu de données neutre qui permettrait ainsi d'avoir un algorithme neutre.

Au cas présent, les dispositifs autorisés par l'article 10 de la loi déférée sont mis en œuvre dans les espaces publics. Il y a pourtant dans ces lieux une surreprésentation des personnes précaires et marginalisées par rapport à la population globale. Il y a également plus d'hommes et moins de personnes très jeunes ou très âgées. Cette surreprésentation se retrouve donc aussi dans les flux vidéo issus de la surveillance de ces espaces et utilisés pour l'entraînement des algorithmes. Pour autant, les jeux de données issus de ces captations ne peuvent être qualifiés de « biaisés » : cet état de fait n'est pas la conséquence d'une erreur de constitution d'un jeu de données mais bien d'une réalité politique et sociale qui est propice à certaines discriminations.

b. Quant au choix des caractéristiques et apprentissage

Le processus d'élaboration des dispositifs comporte également des problématiques techniques ayant des incidences pratiques sur les décisions qui seront prises par les autorités administratives sur les personnes filmées.

Premièrement, le choix des évènements et comportements à détecter traduit nécessairement des choix subjectifs sur ce qui peut être qualifié de « situation à risque ». Par exemple, repérer quelqu'un qui est statique à un endroit en particulier n'est pas constitutif d'une infraction mais peut être jugé risqué selon le présupposé des concepteurs de l'algorithme ou des autorités administratives. À titre d'exemple, la société Evitech qui fournit des logiciels de vidéo surveillance algorithmique qualifie de « *comportement suspect* » les comportements individuels comme les « *arrêts fréquents, contresens, vitesse insuffisante ou excessive, silhouette accroupie ou rampante, temps de présence de la même silhouette dans la zone trop long, arrêt près ou dans d'une zone sensible plus d'un certain temps, comptabilisation de présence de la même silhouette successivement sur différentes caméras, groupe, taille du groupement, objet abandonné, déposé ou tag, objet retiré ou volé,combinaison de conditions, autres observations individuelles …* » [3]. En outre, le fait de repérer les personnes allongées (qui inclura notamment les personnes sans abri), les regroupements de personnes (qui concernera aussi celles n'ayant accès qu'à des espaces publics pour se retrouver) tout en qualifiant ouvertement tous ces comportements de « suspects » peut s'avérer discriminatoire et également

2. Jeff Larson, Surya Mattu, Lauren Kirchner and Julia Angwin, « How We Analyzed the COMPAS Recidivism Algorithm », *ProPublica*, 23 mai 2016, URL : `https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm`

3. Voir la présentation du produit Jaguar disponible sur `https://www.evitech.com/fr/produits/produit-jaguar`.

porter atteinte aux droits fondamentaux exercés dans l'espace public.

Deuxièmement, les variables et caractéristiques retenues par l'algorithme pour repérer ces comportements seront nécessairement liées aux attributs du corps humain. En effet, les images des personnes filmées contiennent des données comportementales, physiques et physiologiques. Les caractéristiques retenues étant dans la majorité des cas déterminées par l'algorithme lui-même du fait de la technologie de « *deep learning* » utilisée, celui-ci ne peut se poser aucune question quant à la sensibilité des données prises en compte : le programme infère à partir des données qu'il a à sa disposition de manière indistincte. Rien n'empêche le programme de reconnaître une démarche, des vêtements ou une couleur de peau, de conserver cette information, de lui donner un poids et de prendre des décisions en fonction de ces variables. Afin de reconnaître et d'individualiser une personne de façon unique pour la catégoriser selon un évènement prédéfini, l'algorithme va donc pouvoir utiliser les données biométriques de cette personne. Au demeurant, on relèvera que l'affirmation au III de l'article 10 selon laquelle les dispositifs autorisés « *n'utilisent aucun système d'identification biométrique* [et] *ne traitent aucune donnée biométrique* » est techniquement et juridiquement faux (pour l'analyse juridique, *cf. infra*).

Troisièmement, l'entraînement du modèle, c'est-à-dire le moment où les données sont fournies à l'algorithme pour qu'il établisse des corrélations et converge vers un état final satisfaisant, ne peut être maîtrisé de façon totalement transparente. On peut voir ce processus comme le calibrage de boutons à tourner : en fonction de la position des boutons, les différentes données de l'image sont pondérées différemment dans la décision d'activer, ou non, la détection. Ces boutons sont tournés de façon automatique par l'algorithme pendant la phase d'apprentissage, mais le concepteur avance malgré tout « à l'aveugle » : il favorise un résultat conforme à son attente, mais sans qu'il sache avec quels critères l'algorithme est arrivé à ce résultat. Si, pour rechercher une personne « suspecte », la combinaison finale de boutons tournés aboutit à ce que l'algorithme trouve plus efficace de repérer les personnes en survêtement, ou encore les personnes de telle couleur de peau, le concepteur ne saura même pas que c'est cette information qui est décisive pour l'algorithme. Il connaîtra juste la pondération que l'algorithme a faite et choisira d'opter pour cette configuration de paramètres car c'est celle-ci qui rend ce dernier le plus efficace. Il est donc impossible d'empêcher que des informations biométriques soient utilisées pour le fonctionnement de l'algorithme et le ciblage de comportements individuels.

c. Quant au choix d'usage de l'algorithme

Une fois que l'algorithme est conçu, il doit être lié à une application dans un logiciel et plus particulièrement à une règle pratique, par exemple en affichant un pictogramme sur l'écran lorsque le comportement « suspect » est détecté. Rien n'empêche techniquement que cet algorithme soit utilisé dans des contextes variés, dès lors que l'on dispose de données suffisantes pour mettre en œuvre cette détection.

Les algorithmes entraînés sur les images des évènements sportifs, récréatifs et culturels ainsi que des Jeux Olympiques 2024, pourront donc tout à fait être utilisés à l'avenir pour surveiller les foules dans un contexte différent (une manifestation, par exemple) et vendus à des entreprises privées dans d'autres pays. Il importe donc peu que les données d'entraînement soient supprimées, ou propres à un contexte particulier : c'est le résultat auquel elles ont permis d'aboutir qui comporte de la valeur en tant que traitement distinct. Ce résultat sera conservé et pourra servir à une multitude d'applications qui peuvent être différentes du

contexte premier de l'expérimentation. De même, essayer d'anonymiser les données d'entraînement ne peut suffire à garantir que l'algorithme final sera respectueux des droits et libertés puisque l'ensemble des choix d'apprentissage et des règles associées peut être porteur de choix politiques ou discriminants, comme exposé ci-avant. Il n'existe pour l'instant aucune preuve ou consensus scientifique sur le fait que les méthodes d'anonymisation permettent de masquer entièrement les données d'entraînement sensibles.

Ces considérations techniques présentées, nous estimons que l'article 10 de la loi déférée, compris à la lumière de ces éléments techniques, est contraire à la Constitution.

B. En ce qui concerne l'inconstitutionnalité de l'article 10

L'article 10 de la loi déférée est contraire à la Constitution en ce qu'il souffre d'un défaut de nécessité (1.), en ce qu'il constitue une atteinte au contenu essentiel des droits et libertés constitutionnellement protégés (2.), en ce qu'il est manifestement disproportionné (3.), en ce que le législateur n'a pas épuisé l'étendue de sa compétence (4.) et en ce qu'il s'agit d'une délégation de compétence d'une autorité publique à une personne de droit privé (5.).

1. S'agissant du défaut de nécessité

En premier lieu, l'article 10 de la loi déférée est contraire aux articles 2, 4 et 11 de la Déclaration de 1789 et 34 de la Constitution en ce qu'il autorise des dispositifs qui portent atteinte au droit à la vie privée et à la protection des données personnelles, à la liberté d'aller et venir et à la liberté d'expression sans justifier d'une quelconque nécessité.

En droit, la liberté proclamée par l'article 2 de la Déclaration de 1789 implique le droit au respect de la vie privée et le droit à la protection des données personnelles (*cf.* Cons. const., 22 mars 2012, *Loi relative à la protection de l'identité*, n° 2012-652 DC, cons. 8 ; Cons. const., 27 décembre 2019, *Loi de finances pour 2020*, n° 2019-796 DC, pts. 79 et 81).

Le Conseil constitutionnel a ainsi jugé que les systèmes de vidéosurveillance affectent la liberté d'aller et venir, le droit à la vie privée ainsi que l'inviolabilité du domicile, protégés par les articles 2 et 4 de la Déclaration de 1789, et doivent donc respecter des garanties strictes, notamment poursuivre un objectif de valeur constitutionnelle (*cf.* Cons. const., 18 janvier 1995, *Loi d'orientation et de programmation relative à la sécurité*, n° 94-352 DC, cons. 3 et 4).

Il a, par ailleurs, reconnu qu'une mesure de surveillance généralisée est susceptible, par la dissuasion qu'elle induit, de porter atteinte à la liberté d'expression et de manifestation protégée par l'article 11 de la Déclaration de 1789 (*cf.* Cons. const., 27 décembre 2019, *Loi de finances pour 2020*, préc., pt. 83) et doit donc être nécessaire, adaptée et proportionnée (*ibid.* , pt. 82).

En l'espèce, le I de l'article 10 prévoit de mettre en œuvre des traitements de données personnelles ayant pour objet de « *détecter, en temps réel, des événements prédéterminés susceptibles de présenter ou de révéler* » des « *risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes* » en vue de « *la mise en œuvre des mesures nécessaires par les services de la police nationale et de la gendarmerie*

*nationale, les services d'incendie et de secours, les services de police municipale et les services internes de sécurité de la SNCF et de la Régie autonome des transports parisiens dans le cadre de leurs missions respective*s ». La finalité générale du dispositif est « *d'assurer la sécurité de manifestations sportives, récréatives ou culturelles* ».

Or, ni les travaux préparatoires à la loi déférée, ni les débats parlementaires n'ont permis de démontrer en quoi les traitements de données en question permettraient d'atteindre les larges objectifs liés aux finalités décrites ci-dessus. En effet, aucune étude ou document technique tangible n'a été produit ou mis au débat pour illustrer comment fonctionnent ces traitements algorithmiques ni comment ils pourraient éventuellement permettre de présenter et révéler des risques de terrorisme ou d'atteintes graves à la sécurité, de façon certaine et efficace. Il est dès lors impossible d'établir la nécessité de telles techniques au regard de l'objectif poursuivi.

En outre, il n'a jamais été démontré en quoi les moyens actuellement mis en œuvre pour assurer la sécurité des manifestations sportives, récréatives et culturelles, déjà très importants et attentatoires à la vie privée, ne suffiraient pas à remplir cet objectif.

Au surplus, le Conseil constitutionnel pourra s'inspirer d'une récente affaire de la Cour constitutionnelle allemande concernant un dispositif d'analyse automatisée de données personnelles afin de prévenir des troubles à l'ordre public (*cf.* Bundesverfassungsgericht, 16 février 2023, *Automatisierte Datenanalyse*, n[os] 1 BvR 1547/19 et 1 BvR 2634/20[4]). Pour considérer que le dispositif litigieux était contraire à la Constitution allemande, la Cour constitutionnelle a, entre autres, d'une part rappelé que seul un danger grave, avéré et circonstancié permettrait de justifier le dispositif au vu de l'ingérence portée aux droits fondamentaux puis, d'autre part, relevé que la prévention de délits est un objectif insuffisamment étayé, dans le sens où aucun danger suffisamment caractérisé n'était identifié.

Il en résulte que, à défaut d'être nécessaires à la poursuite des finalités qui leur sont associées, et alors qu'ils causent de graves atteintes aux libertés fondamentales tel que démontré ci-après, les dispositifs de vidéosurveillance algorithmique prévus par l'article 10 ne sauraient être autorisés sans violer la Constitution. De ce chef déjà, le Conseil constitutionnel pourra déclarer l'article 10 contraire à la Constitution.

2. S'agissant de l'atteinte au contenu essentiel des droits fondamentaux

En deuxième lieu, l'article 10 de la loi déférée est contraire à l'article 34 de la Constitution et aux articles 2, 4 et 11 et 16 de la Déclaration de 1789 en ce qu'il crée une atteinte au contenu essentiel du droit à la vie privée et à la protection des données personnelles, du droit d'aller et venir et du droit à la liberté d'expression.

En droit, comme rappelé ci-avant, en matière de surveillance de l'espace public, l'article 34 de la Constitution exige du législateur que celui-ci opère une conciliation entre, d'une part, un objectif de valeur constitutionnel et, d'autre part, les droits et libertés constitutionnellement protégés (*cf.* Cons. const., 18

4. Communiqué de presse accessible sur https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2023/bvg23-018.html et décision intégrale disponible sur https://www.bundesverfassungsgericht.de/SharedDocs/Downloads/DE/2023/02/rs20230216_1bvr154719.pdf?__blob=publicationFile&v=1

janvier 1995, *Loi d'orientation et de programmation relative à la sécurité*, préc.). Ces atteintes doivent être nécessaires, adaptées et proportionnées à l'objectif poursuivi (*cf.* Cons. const., 27 décembre 2019, *Loi de finances pour 2020*, préc., pt. 82).

Par ailleurs, comme rappelé ci-avant, le Conseil constitutionnel a reconnu qu'une mesure de surveillance généralisée est susceptible de porter atteinte à la liberté d'expression et de manifestation protégée par l'article 11 de la Déclaration de 1789 (*cf.* Cons. const., 27 décembre 2019, *Loi de finances pour 2020*, préc., pt. 83).

Bien que les moyens tirés de la méconnaissance du droit de l'Union européenne soient inopérants devant le Conseil constitutionnel, celui-ci pourra s'inspirer de la jurisprudence de l'UE en matière de contrôle de proportionnalité. En effet, la Charte des droits fondamentaux de l'UE (ci-après « la Charte de l'UE ») exige au 1 de son article 52 que le contenu essentiel des droits fondamentaux soit respecté : « *Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.* »

Ainsi, en droit de l'Union, le contrôle du respect du contenu essentiel d'un droit fondamental est préalable au contrôle de proportionnalité : une atteinte au contenu essentiel d'un droit fondamental suffit à ce que la mesure litigieuse soit contraire à la Charte de l'UE, indépendamment de toute nécessité et de toutes les garanties que le législateur aurait pu assortir.

Par ailleurs, la CJUE a, de façon notoire, reconnu qu'une « *réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte* » (*cf.* CJUE, gr. ch., 6 octobre 2015, *Schrems*, aff. C-362/14, pt. 94). Dans la continuité de ce mouvement, concernant la conservation et l'accès des données de connexion, la Cour a affirmé que « *le législateur de l'Union a concrétisé les droits consacrés aux articles 7 et 8 de la Charte* [droit à la vie privée et droit à la protection des données personnelles]*, de telle sorte que les utilisateurs des moyens de communications électroniques sont en droit de s'attendre, en principe, à ce que leurs communications et les données y afférentes restent, en l'absence de leur consentement, anonymes et ne puissent pas faire l'objet d'un enregistrement.* » (*cf.* CJUE, gr. ch., 6 octobre 2020, *La Quadrature du Net e.a.*, aff. C-511/18, pt. 109).

Il apparaît ainsi que le contenu essentiel des droits et libertés reconnus aux articles 7 (droit à la vie privée), 8 (droit à la protection des données personnelles) et 11 (droit à la liberté d'expression) de la Charte de l'UE comprend un droit à ne pas faire l'objet d'une surveillance constante et généralisée dans l'espace public.

Le Conseil constitutionnel peut saisir l'occasion de cette affaire pour faire évoluer son contrôle de proportionnalité dans un sens plus exigeant et plus conforme au standard de l'UE. En droit constitutionnel français, il peut rattacher le contrôle du contenu essentiel d'un droit fondamental à l'article 34 de la Constitution ainsi qu'aux articles 4 et 16 de la Déclaration de 1789.

En l'espèce, comme exposé ci-avant (*cf.* « En ce qui concerne les éléments techniques de compréhen-

sion de la vidéosurveillance algorithmique », p. 2) et tel qu'il sera complété ci-après (*cf.* « S'agissant de la disproportion manifeste des dispositifs autorisés », p. 9), les dispositifs visés à l'article 10 permettent la mise en œuvre d'un traitement d'une ampleur considérable, aussi bien au regard du nombre important des évènements qui seront concernés que du nombre de personnes dont les données personnelles seront traitées, tant pour l'apprentissage que pour la mise en œuvre de cette technologie.

Aussi, comme analysé ci-avant, le fonctionnement intrinsèque de ces traitements algorithmiques présuppose une analyse continue des caractéristiques physiques, physiologiques et comportementales des personnes filmées, à laquelle elles ne peuvent se soustraire. Les comportements des personnes sont donc nécessairement catégorisés en permanence, afin de déterminer si les dispositifs autorisés par l'article 10 doivent ou non déclencher une alerte. Ces dispositifs transforment donc de façon extrêmement importante le rapport de chacun à l'espace public et affecte la liberté d'expression dans ces espaces.

Une telle analyse biométrique des corps va ainsi frontalement contre l'idée du droit à la vie privée et à la protection de ses données personnelles, de même qu'elle va contre l'idée d'un droit à la liberté d'expression et à la liberté d'aller et venir qui puissent être exercés 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 – ce qui reviendrait à une absurdité. Il n'est donc plus possible d'exercer convenablement ses droits et libertés constitutionnellement protégés. Par ailleurs, alors qu'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 liberté.

Il en résulte que les dispositifs autorisés à l'article 10 de la loi déférée portent une atteinte au contenu essentiel du droit à la vie privée et à la protection des données personnelles, au droit à la liberté d'expression et au droit à la liberté d'aller et venir et doit alors être déclaré, de ce chef, contraire à la Constitution.

3. S'agissant de la disproportion manifeste des dispositifs autorisés

En troisième lieu, l'article 10 de la loi déférée est contraire aux articles 2, 4 et 11 de la Déclaration de 1789 et 34 de la Constitution en ce qu'il autorise des dispositifs qui créent une atteinte manifestement disproportionnée au droit à la vie privée et à la protection des données personnelles, à la liberté d'aller et venir et à la liberté d'expression.

En droit, comme indiqué ci-avant, de l'article 2 de la Déclaration de 1789 est dégagé le droit à la vie privée et à la protection des données personnelles et de l'article 4 découle le droit d'aller et venir. L'article 11 de la Déclaration de 1789 proclame quant à lui le droit à la liberté d'expression.

De plus, découle de l'article 34 de la Constitution l'obligation, pour le législateur, d'assurer la conciliation entre, d'une part, la sauvegarde de l'ordre public et la recherche des auteurs d'infractions, d'autre part, le respect des autres droits et libertés constitutionnellement protégés, en prévoyant des garanties appropriées et spécifiques. Pour cet examen de la proportionnalité d'un traitement de données personnelles, le Conseil prend en compte « *la nature des données enregistrées, l'ampleur de ce traitement, ses caractéristiques techniques et les conditions de sa consultation* » (*cf.* Cons. const., 22 mars 2012, *Loi relative à la*

protection de l'identité, préc., cons. 11).

Le Conseil a estimé qu'un traitement de données personnelles qui concernait une partie importante de la population, collectait des données biométriques, c'est-à-dire des données particulièrement sensibles, et dont les caractéristiques techniques permettait l'interrogation à d'autres fins que celle prévues par les textes constituait une atteinte disproportionnée au droit à la vie privée (*cf.* Cons. const., 22 mars 2012, *Loi relative à la protection de l'identité*, préc., cons 10).

Par ailleurs, bien que les moyens tirés de la méconnaissance du droit de l'Union soient inopérants devant le Conseil constitutionnel, celui-ci pourra utilement s'inspirer de la jurisprudence européenne en matière de protection des données personnelles dans la présente affaire.

En effet, la jurisprudence de la Cour de justice de l'Union européenne (CJUE) considère que l'image d'une personne collectée par une caméra constitue une « *donnée à caractère personnel* », dès lors qu'elle permet d'identifier la personne concernée (*cf.* CJUE, 14 février 2019, *Buivids*, n° C-345/17, pt. 31 ; CJUE, 11 décembre 2014, *Ryneš*, n° C-212/13, pt. 22). Par suite, dès lors qu'il est possible de voir ou d'entendre la personne sur la vidéo en cause, les images des personnes ainsi traitées constituent des données personnelles (*cf.* CJUE, 14 février 2019, *Buivids*, préc., pt. 32) dont la protection est garantie par l'article 8 de la Charte de l'UE et qui, à ce titre aussi, ne peut être traitée que dans de strictes limites, notamment définies par la directive UE n° 2016/680 (dite « 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 Liberté »), et par le règlement UE n° 2016/679 du 27 avril 2016 (dit « règlement général sur la protection des données », ci-après « RGPD »).

Or, les articles 5 du RGPD et 4 de la directive « police-justice » prévoient notamment que les données personnelles doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités. Ce principe est repris à l'article 4 de la loi Informatique et Libertés.

Le Conseil pourra également s'inspirer de la jurisprudence de la Cour européenne des droits de l'Homme (CEDH) qui protège des atteintes disproportionnées au droit à la vie privée y compris dans le cas d'une surveillance sur la base d'informations publiques. La CEDH a notamment jugé qu'il ressort de l'article 8 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales (CESDH), qui proclame le droit à la vie privée et familiale, qu'un internaute conserve une attente raisonnable relative au respect de sa vie privée lorsque son adresse IP est traitée lors de sa navigation en ligne, alors même que l'adresse IP est, dans ce contexte, une donnée personnelle rendue publique par la navigation (*cf.* CEDH, 24 avril 2018, *Benedik c. Slovénie*, n° 62357/14, §§ 100–119).

Par ailleurs, la CEDH a également, au visa de l'article 10 de la CESDH qui protège le droit à la liberté d'expression, posé un principe de droit à l'anonymat sur Internet (*cf.* CEDH, gr. ch., 16 juin 2015, *Delfi AS c. Estonie*, n° 64569/09, § 147), au sens où les personnes ont droit à ne pas être identifiées par défaut en ligne. Ce principe s'applique, *mutatis mutandis*, au cas d'une surveillance de l'espace public.

Enfin, le Conseil constitutionnel pourra également s'inspirer d'éléments de droit comparé, notamment l'interprétation donnée par la Cour constitutionnelle allemande concernant un dispositif d'analyse automatisée de données personnelles (*cf.* Bundesverfassungsgericht, 16 février 2023, *Automatisierte Datenanalyse*,

préc.). La Cour constitutionnelle allemande a considéré que l'utilisation d'un dispositif de surveillance fondé sur l'intelligence artificielle, en l'occurrence le traitement automatisé d'un ensemble de données aux fins de prévenir la commission de délits était contraire à la Constitution allemande.

Dans sa décision, la Cour constitutionnelle allemande opère une distinction entre la collecte initiale des données fournies au logiciel et le traitement algorithmique ultérieur fondé sur ces données. Elle estime que ce deuxième traitement aboutit à la création de nouveaux renseignements sur les personnes, à partir d'interconnexions et de croisements qui n'auraient pu être déduits simplement de la première collecte. Pour la Cour, la création de ces nouvelles informations, plus complexes, génère une nouvelle ingérence dans les droits et libertés, potentiellement plus attentatoire. Elle considère que cette nouvelle ingérence doit elle aussi faire l'objet d'un contrôle de proportionnalité stricte, en prenant en compte les nouvelles finalités pour lesquelles les données personnelles sont alors traitées. Elle relève qu'un croisement algorithmique de données peut être particulièrement intrusif et que plus le renseignement tiré de l'analyse automatisée est large et complexe, plus la marge d'erreur et le risque de discrimination sont grands. La Cour relève que dans ce cas, il est difficile d'examiner la façon dont le logiciel a effectué des corrélations entre les informations. Elle constate alors que ces méthodes d'analyse automatisée engendrent des ingérences graves et exige en conséquence un contrôle strict de proportionnalité.

Pour considérer que, dans le cas d'espèce allemand, le contrôle de proportionnalité n'était pas satisfait, la Cour constitutionnelle relève notamment que les dispositions ne prévoient pas de restrictions sur la quantité ou le type de données analysées et que le dispositif ne différencie pas les personnes pour lesquelles il existe des raisons valables de penser qu'elles pourraient commettre un crime et les autres. De plus, elle retient que les techniques en cause comportent des systèmes d'intelligence auto-apprenants pouvant être utilisés dans un but de simple détection d'anomalies statistiques et que le cadre en question n'impose aucune limite aux résultats fournis par la machine, qui permet de fournir un pronostic sur le potentiel de danger de certaines personnes. Elle souligne, enfin, que la finalité du dispositif litigieux qui est de prévoir des troubles à l'ordre public ne justifie pas une moins grande protection des droits constitutionnellement protégés. Pour cela, la Cour constitutionnelle exige que les finalités du dispositif soient particulièrement détaillées, l'évaluation de la nécessité étant intégrée dans le contrôle de proportionnalité ensuite effectué (*cf. supra*, « S'agissant du défaut de nécessité », p. 6).

De plus, le Conseil constitutionnel pourra procéder à un contrôle *in concreto* de l'article 10 de la loi déférée pour conclure à la disproportion manifeste des dispositifs autorisés (*cf.* Cons. const., 18 juin 2020, *Loi visant à lutter contre les contenus haineux sur internet*, n° 2020-801 DC, pt. 19).

En l'espèce, l'article 10 de la loi déférée est manifestement disproportionné. Le I de cet article prévoit la mise en œuvre de traitements algorithmiques ayant pour objet de « *détecter, en temps réel, des événements prédéterminés susceptibles de présenter ou de révéler* » des « *risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes* » sur les images collectées au moyen de systèmes de vidéoprotection autorisés sur le fondement de l'article L. 252-1 du code de la sécurité intérieure ou au moyen de caméras installées sur des aéronefs autorisées sur le fondement du chapitre II du titre IV du livre II du même code.

Concernant l'entraînement de ces algorithmes, le VIII de l'article 10 prévoit que, afin « *d'améliorer la qualité de la détection des événements prédéterminés par les traitements mis en œuvre, un échantillon d'images collectées, dans des conditions analogues à celles prévues pour l'emploi de ces traitements, au*

moyen de systèmes de vidéoprotection autorisés sur le fondement de l'article L. 252-1 du code de la sécurité intérieure et de caméras installées sur des aéronefs autorisées sur le fondement du chapitre II du titre IV du livre II du même code et sélectionnées, sous la responsabilité de l'État, conformément aux exigences de pertinence, d'adéquation et de représentativité mentionnées au 1° du V du présent article peut être utilisé comme données d'apprentissage pendant une durée strictement nécessaire et maximale de douze mois à compter de l'enregistrement des images ».

Ainsi, les dispositifs de vidéosurveillance algorithmique mis en œuvre par l'article 10 de la loi déférée reposent sur l'analyse préalable (pour l'entraînement) et en temps réel (pour l'application) des images initialement captées par les caméras installées sur la voie publique en application du code de la sécurité intérieure. Cette analyse aboutit à donner de nouvelles informations sur les personnes filmées à travers un nouveau traitement (l'analyse algorithmique des images) fondé sur des images collectées pour des finalités initiales différentes, ce qui constitue un traitement supplémentaire de données personnelles créant une nouvelle ingérence dans les droits et libertés constitutionnellement garantis, dont il convient d'évaluer la proportionnalité.

Premièrement, les traitements algorithmiques autorisés analysent un nombre très important de données personnelles sensibles. En effet, d'une part, les images utilisées pour l'entraînement et les tests des algorithmes sont issues des caméras filmant toute situation ayant « *des conditions analogues* » aux manifestations sportives, récréatives et culturelles exposées à des risques. En pratique, cela signifie que seront utilisées des milliers d'heures d'images filmant un nombre important et potentiellement illimité de personnes dans ces situations qui ne sont pas définies et laissées à l'appréciation des autorités administratives. Les données de ces personnes seront traitées, sans que ces personnes puissent donner leur consentement ou valablement faire valoir leur droit d'effacement.

D'autre part, une fois que l'algorithme sera conçu, son utilisation par les autorités concernera ces mêmes « *manifestations sportives, récréatives et culturelles* », dont le champ reste potentiellement très large, et le nombre de personnes y assistant très élevé. Le traitement de données personnelles est donc d'une ampleur considérable.

Au surplus, dans les deux cas, les traitements auront pour objet de catégoriser les comportements des personnes filmées en fonction des évènements prédéfinis. Contrairement à ce qui a été avancé lors des débats parlementaires, ces technologies visent à reconnaître des situations comprenant des comportements humains individuels. En pratique, comme cela a été expliqué ci-avant (*cf.* « Quant au choix des caractéristiques et apprentissage », pp. 4 et s.), les algorithmes devront nécessairement se fonder sur l'analyse des attributs physiques, physiologiques et comportementaux de chaque personne filmée pour opérer cette catégorisation en identifiant chaque corps de façon unique, c'est-à-dire en individualisant les personnes, pour les reconnaître sur l'écran et inviter l'agent de police destinataire de l'alerte d'agir sur la personne dont un « comportement suspect » aurait été détecté. En effet, comme le rappelle le Comité européen pour la protection des données [5], cette identification unique n'implique pas de connaître l'identité civile d'une personne mais de pouvoir affirmer qu'il s'agit d'une même et seule personne. Comme cela a été évoqué

5. Lignes directrices sur les vidéos contenant des données personnelles 3/2019, version 2.0, pt. 82 p. 19, URL : `https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_fr.pdf`.

lors des débats parlementaires et dénoncé par des organisations internationales [6] et des députés européens [7], et contrairement à ce qui a été inscrit par le législateur, les traitements algorithmiques autorisés par l'article 10 constituent donc bien des traitements de données biométriques au sens du droit de l'Union européenne.

Deuxièmement, les traitements de données sont justifiés par la détection de seuls « *risques* » d'atteinte à la sécurité des personnes, c'est-à-dire uniquement par la potentialité que des évènements se réalisent, sans que ceux-ci ne donnent nécessairement lieu à la commission d'une infraction.

À titre de comparaison, la Cour constitutionnelle allemande exige que l'ingérence grave créée par des traitements algorithmiques ne peut être justifiée que si ces technologies servent un intérêt public prééminent (« *herausragenden öffentlichen Interesse* ») et ne doivent être autorisés que pour la protection d'« *objets juridiques* » particulièrement importants (« *besonders gewichtigen Rechtsgütern* »). Enfin, elles doivent servir à prévenir des dangers concrets et suffisamment caractérisés (« *hinreichend konkretisierte Gefahr* »), selon des dispositions claires et limitant les possibilités d'analyse automatisée (*cf.* Bundesverfassungsgericht, 16 février 2023, *Automatisierte Datenanalyse*, préc.).

Or, selon l'état de l'art de ces technologies, et comme cela a été illustré ci-avant (*cf. supra*, « En ce qui concerne les éléments techniques de compréhension de la vidéosurveillance algorithmique », p. 2), les traitements algorithmiques qui seront mis en œuvre détectent des situations ne présentant pas de caractère de gravité suffisant pour justifier une atteinte aussi importante aux droits et libertés (par exemple le fait de rester allongé ou de se regrouper). Ce point n'a pas été démenti lors des débats parlementaires au cours desquels le ministre de l'intérieur Gérald Darmanin expliquait lui-même lors de la séance publique du 22 mars 2023 à l'Assemblée nationale : « *Il s'agit de situations qui, considérées isolément, peuvent ne pas être problématiques, mais qui le sont parfois : lorsque quelqu'un pose un sac à dos par terre, par exemple, ce peut être un geste problématique s'il contient une bombe, mais ce peut aussi n'être qu'un geste banal.* » [8] Les objectifs affichés pour justifier de l'ingérence à la vie privée ne constituent donc aucunement un danger concret et caractérisé de façon suffisamment claire.

Troisièmement, le traitement algorithmique en cause repose sur une technologie complexe de « *deep learning* » (*cf. supra*, « Quant au choix des caractéristiques et apprentissage », p. 4 pour une explication technique), qui ne permet pas de retracer comment les corrélations entre les données personnelles sont effectuées afin de parvenir au résultat générant une alerte auprès des autorités administratives. Ces autorités obtiendront alors une information relative à une présomption de culpabilité de personnes filmées qui prendra la forme d'un pourcentage de probabilité que la personne concernée par l'alerte ait un comportement anormal, sans qu'il ne soit possible de comprendre quelles données et quelles interconnexions ont permis au traitement algorithmique d'arriver à la production de cette information. Ce fonctionnement porte donc une atteinte manifeste aux droits et libertés des personnes filmées. En outre, ces corrélations intrinsèquement

6. Voir la lettre ouverte signée par 38 associations internationales, le 7 mars 2023 : https://ecnl.org/sites/default/files/2023-03/Lettre%20ouverte_Soci%C3%A9t%C3%A9%20civile__Article%207_PJLJO_Final_FR_0.pdf

7. Voir le courrier envoyé par 41 eurodéputés à l'Assemblée nationale, le 17 mars 2023 : https://www.patrick-breyer.de/wp-content/uploads/2023/03/Lettre-des-eurodepute.e.s-contre-la-surveillance-biometrique-de-masse-dans-la-loi-sur-les-JO2024.pdf

8. Compte-rendu de la séance disponible à l'adresse suivante : https://www.assemblee-nationale.fr/dyn/16/comptes-rendus/seance/session-ordinaire-de-2022-2023/deuxieme-seance-du-mercredi-22-mars-2023#3061733

discriminantes (au sens premier comme au sens figuré du terme) sont consubstantielles au fonctionnement de ces technologies : il n'existe aucune manière de les limiter, aussi bien techniquement que par la loi, ce qui empêche toute limitation effective aux ingérences sur les droits et libertés qui en résultent.

Quatrièmement, l'apprentissage puis la mise en œuvre de ces algorithmes reposent sur l'exploitation de l'infrastructure existante de caméras dans l'espace public. L'installation de ces caméras a été autorisée au cours des dernières décennies après examen, pour chacune, de la nécessité et la proportionnalité de la ou des finalités poursuivies, parmi celles prévues par l'article L. 251-2 du code de la sécurité intérieure. Utiliser ces images dans un autre contexte, et pour produire de nouvelles informations plus sensibles et complexes, qui créent de nouvelles ingérences dans les droits et libertés, contrevient aux principes d'adéquation et de limitation des finalités prévue par le RGPD, la loi Informatique et Liberté et la directive « police-justice ».

Il en résulte que, au regard de l'ampleur du traitement, de la sensibilité des données traitées, de la largeur des finalités justifiant le traitement et des caractéristiques techniques du dispositif empêchant tout encadrement strict permettant de limiter les ingérences dans les droits et libertés, les dispositifs de vidéosurveillance algorithmique autorisés par l'article 10 doivent être considérés comme disproportionnés et emporter violation à la fois de la Constitution et du droit européen. Partant, cet article 10 doit être déclaré contraire à la Constitution.

4. S'agissant de l'incompétence négative

En quatrième lieu, l'article 10 de la loi déférée est contraire à l'article 34 de la Constitution et aux articles 4, 5, 6 et 16 de la Déclaration de 1789 en ce que le législateur a méconnu l'étendue de sa compétence.

En droit, le Conseil constitutionnel fait découler, d'une part, de l'article 34 de la Constitution un principe de clarté de la loi et, d'autre part, des articles 4, 5, 6 et 16 de la Déclaration de 1789 l'objectif de valeur constitutionnelle d'intelligibilité et d'accessibilité. Ces principes et objectifs imposent au législateur « *d'adopter des dispositions suffisamment précises et des formules non équivoques afin de prémunir les sujets de droit contre une interprétation contraire à la Constitution ou contre le risque d'arbitraire, sans reporter sur des autorités administratives ou juridictionnelles le soin de fixer des règles dont la détermination n'a été confiée par la Constitution qu'à la loi* » (*cf.* Cons. const., 21 avril 2005, *Loi d'orientation et de programme pour l'avenir de l'école*, n° 2005-512 DC, cons. 9 ; V. aussi Cons. const., 22 mars 2012, *Loi relative à la protection de l'identité*, préc., cons. 13).

Pour ne pas se placer en situation d'incompétence négative, le législateur doit donc déterminer avec une précision suffisante les conditions dans lesquelles est mis en œuvre le principe ou la règle qu'il vient de poser.

Ainsi, le Conseil constitutionnel a estimé qu'est entachée d'incompétence négative une disposition prévoyant la mise en œuvre d'un traitement de données personnelles pour les besoins de la prévention de la fraude qui, d'une part, « *est ambiguë quant aux infractions auxquelles s'applique le terme de "fraude"* » et, d'autre part, « *laisse indéterminée la question de savoir dans quelle mesure les données traitées pourraient être partagées ou cédées, ou encore si pourraient y figurer des personnes sur lesquelles pèse la simple crainte qu'elles soient capables de commettre une infraction* » (*cf.* Cons. const., 29 juillet 2004,

Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, n° 2004-499 DC, cons. 12).

Le Conseil y précisait « *qu'au regard de l'article 34 de la Constitution, toutes ces précisions ne sauraient être apportées par les seules autorisations délivrées par la Commission nationale de l'informatique et des libertés ; qu'en l'espèce et eu égard à la matière concernée, le législateur ne pouvait pas non plus se contenter, ainsi que le prévoit la disposition critiquée éclairée par les débats parlementaires, de poser une règle de principe et d'en renvoyer intégralement les modalités d'application à des lois futures* » (*ibid*.).

Dans sa décision relative à l'analyse automatique de données (*cf*. Bundesverfassungsgericht, 16 février 2023, *Automatisierte Datenanalyse*, préc.), la Cour constitutionnelle allemande rappelle l'exigence d'encadrement strict par la loi de ce type de dispositifs au regard de leur intrusivité. Elle estime notamment nécessaire qu'un texte législatif détermine de façon suffisamment claire les « *dangers identifiables* » afin de limiter le plus possible les potentialités d'analyse des logiciels. Ce n'est que sur cette base que des dispositions administratives peuvent ensuite être prises pour préciser l'application du dispositif.

En l'espèce, le IV de l'article 10 prévoit que le recours aux traitements algorithmiques sont autorisés par un décret pris après avis de la Commission nationale de l'informatique et des libertés. Ce décret « *fixe les caractéristiques essentielles du traitement* » et « *indique notamment les événements prédéterminés que le traitement a pour objet de signaler* [et] *le cas échéant les spécificités des situations justifiant son emploi* [. . .]. »

L'article 10 de la loi déférée ne définit à aucun moment les notions de « *manifestation particulièrement exposée à des risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes* » ni d'« *évènements prédéterminés susceptibles de présenter ou de révéler ces risques* », laissant ainsi le soin à l'autorité administrative de les déterminer.

Les débats parlementaires n'ont, à aucun moment, permis de fournir des indications concrètes et éclairantes sur la nature et la teneur de ces évènements et de ces risques ou de ces évènements, le gouvernement et les rapporteurs renvoyant régulièrement à l'appréciation future de la Commission nationale de l'informatique et des libertés, dont l'avis n'est au demeurant que consultatif. Ainsi, le ministre de l'intérieur Gérald Darmanin assurait durant la séance du 22 mars 2023 à l'Assemblée nationale que « *la Cnil, qui fera office de contre-pouvoir en donnant son avis, saura au besoin éviter tout abus, tout dévoiement du texte* » [9] et durant celle du 23 mars que celle-ci « *dira si nous prenons des décisions disproportionnées ou si nous utilisons mal les dispositions prévues par le législateur* » [10].

Au cours de la même séance du 23 mars 2023, le rapporteur et président de la commission des lois Sacha Houlié répondait aux députés s'interrogeant sur la nature de ces évènements que « *si certains d'entre vous peuvent avoir des doutes vis-à-vis du Gouvernement, vous ne pouvez pas en avoir vis-à-vis de la Cnil*

9. Compte-rendu de la séance disponible à l'adresse suivante : https://www.assemblee-nationale.fr/dyn/16/comptes-rendus/seance/session-ordinaire-de-2022-2023/deuxieme-seance-du-mercredi-22-mars-2023#3061446

10. Compte-rendu de la séance disponible à l'adresse suivante : https://www.assemblee-nationale.fr/dyn/16/comptes-rendus/seance/session-ordinaire-de-2022-2023/premiere-seance-du-jeudi-23-mars-2023#3061414

dont les travaux comme les avis sont impartiaux et font l'objet d'une légitime confiance de la part de tous les parlementaires ».

Ainsi, le législateur n'a pas défini clairement ni sans ambiguïté l'objet même du traitement en cause et s'est contenté de renvoyer la définition de cet élément essentiel à l'appréciation arbitraire de l'autorité administrative. En conséquence, le législateur n'a pas respecté les principes de clarté de la loi ni les objectifs d'intelligibilité et d'accessibilité de la loi, violant manifestement la Constitution.

Par ailleurs, il est important de souligner que le caractère « expérimental » du dispositif ne saurait justifier ce manque de précision suffisante dans la loi. En effet, renvoyer à l'évaluation future des dispositifs ne saurait suffire à pallier l'atteinte grave aux droits et libertés qui est créée pendant toute la durée de cette expérimentation, soit quasiment deux années, par le manque d'encadrement préalable dans la loi et l'absence de garanties. De plus, les algorithmes conçus au cours de cette expérimentation seront mis en œuvre et cédés par les entreprises les ayant développés au-delà de cette période.

Il en résulte que le législateur, en ne précisant pas à l'article 10 de la loi déférée l'étendue des situations concernées par cette disposition, n'a pas épuisé l'étendue de sa compétence et s'est, dès lors, placé en situation d'incompétence négative. De ce chef, cet article 10 doit être déclaré contraire à la Constitution.

5. S'agissant de la délégation de compétence d'une autorité publique à une personne de droit privé

En cinquième lieu, l'article 10 de la loi déférée est contraire à l'article 12 de la Déclaration de 1789 en ce qu'elle prévoit une délégation de compétence d'une autorité publique à une personne de droit privé.

En droit, l'article 12 de la Déclaration de 1789 prévoit que « *La garantie des droits de l'Homme et du Citoyen nécessite une force publique : cette force est donc instituée pour l'avantage de tous, et non pour l'utilité particulière de ceux auxquels elle est confiée.* »

Dans sa décision n° 2011-625 DC du 10 mars 2011, le Conseil constitutionnel a analysé la constitutionnalité d'une disposition de la loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI). L'un des articles prévoyait que les salariés du délégataire privé puissent visionner les images prises par l'autorité publique sur la voie publique. Le Conseil constitutionnel a considéré que, « *en autorisant toute personne morale à mettre en œuvre des dispositifs de surveillance au-delà des abords "immédiats" de ses bâtiments et installations et en confiant à des opérateurs privés le soin d'exploiter des systèmes de vidéoprotection sur la voie publique et de visionner les images pour le compte de personnes publiques, les dispositions contestées permettent d'investir des personnes privées de missions de surveillance générale de la voie publique ; que chacune de ces dispositions rend ainsi possible la délégation à une personne privée des compétences de police administrative générale inhérentes à l'exercice de la "force publique" nécessaire à la garantie des droits ; que, par suite, doivent être déclarés contraires à la Constitution le douzième alinéa du 1° ainsi que les b) et c) du 2° de l'article 18* […] » (cons. 19).

Il est par ailleurs indiqué dans le commentaire autorisé de la décision que « *le Conseil a jugé que chacune des dispositions en cause conduisaient à déléguer une mission de surveillance générale de la voie publique et que, par conséquent, elles méconnaissaient l'exigence, résultant de l'article 12 de la Déclaration des droits de l'homme et du citoyen de 1789, selon laquelle la garantie des droits est assurée par une*

“force publique” » (commentaire de la décision n° 2011-625 DC du 10 mars 2011, p. 10).

Il ressort donc de la jurisprudence du Conseil que la mise en œuvre d'un dispositif déléguant à une personne privée une mission de surveillance générale de la voie publique est contraire à l'article 12 de la Déclaration de 1789.

En l'espèce, les traitements algorithmiques autorisés par l'article 10 de la loi déférée visent à « *détecter, en temps réel, des événements prédéterminés susceptibles de présenter ou de révéler* [des risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes] ». Pour cela, l'ensemble des images de vidéosurveillance est analysé, en temps réel, de manière systématique.

Or, le V de cet article prévoit que « *L'État assure le développement du traitement ainsi autorisé, en confie le développement à un tiers ou l'acquiert.* » Il ressort de ces dispositions que les traitements algorithmiques visés peuvent être conçus par des entreprises privées. Le recours en priorité à ce type d'acteurs a d'ailleurs été totalement assumé lors des débats parlementaires. Le rapporteur à l'Assemblée nationale Guillaume Vuilletet affirmait lors des débats en commission des lois que : « *Cependant, compte tenu de l'état du marché de l'intelligence artificielle, l'État devra avoir recours à des tiers, au moins dans un premier temps, afin de développer le traitement ou de l'acquérir. Il est illusoire, alors que l'usage de caméras augmentées nécessite l'établissement d'un cadre légal, de penser que l'État peut tout faire tout seul, dans un domaine où les acteurs privés ont déjà plusieurs longueurs d'avance*. » [11]

Dès lors, hors du cas où l'État conçoit lui-même ces traitements algorithmiques, ce sont bien des personnes privées qui seront, indirectement, chargées d'un grand nombre de pouvoirs de surveillance de la voie publique et de pouvoirs de police administrative. En effet, ces personnes privées se verront déléguer la mission de caractérisation d'évènements anormaux pouvant générer une alerte et déclencher la surveillance active d'opérateurs humains. Il reviendra au dispositif conçu par la personne privée d'identifier, de catégoriser et de générer des alertes sur certains évènements ayant lieu sur la voie publique. Cette surveillance, automatique, concerne des évènements que l'opérateur lui-même n'aurait pas pu remarquer.

Il en résulte que l'article 10 de la loi déférée est contraire à la Constitution en ce qu'il entraîne une délégation à une personne privée de compétences de police administrative générale inhérentes à l'exercice de la force publique. De ce chef encore, l'article 10 doit être déclaré contraire à la Constitution.

II. Sur l'article 16 (article 11 du projet de loi)

L'article 16 de la loi déférée est contraire à l'article 2 de la Déclaration de 1789 et 34 de la Constitution en ce qu'il vient ajouter la possibilité de prévoir des scanners à ondes millimétriques à l'entrée des enceintes sportives de manière disproportionnée.

En droit, comme rappelé ci-avant, découle de l'article 2 de la Déclaration de 1789 le droit à la vie privée et à la protection des données personnelles.

11. Compte-rendu de la séance en commission des Lois du mercredi 8 mars 2023 disponible à l'adresse suivante : https://www.assemblee-nationale.fr/dyn/16/comptes-rendus/cion_lois/l16cion_lois2223041_compte-rendu

Or, **en l'espèce**, l'article 16 de la loi déférée porte une atteinte manifestement disproportionnée au droit à la vie privée. Concrètement, les scanners à ondes millimétriques créent une représentation en trois dimensions de la personne scannée. L'opérateur visualisant cette représentation verra donc un avatar d'un corps sans habits, l'objectif étant de pouvoir « voir » en dessous d'un vêtement pour détecter plus rapidement une tentative d'introduction dans un lieu un objet qui aurait été caché par la personne scannée. Comme le rappelle le Conseil d'État dans son avis, « *Ces dispositifs sont des traitements de données personnelles régis par le RGPD et par la loi du 17 janvier 1978 qui, en raison de leur caractère intrusif, appellent des garanties particulières.* »

Pourtant, force est de constater que la nécessité de ces dispositifs fait cruellement défaut. En effet, l'étude d'impact met en avant la faculté de ces outils de « *fluidifier* » l'entrée dans les enceintes sportives en évitant que les files de spectateurs ne stagnent au moment des palpations de sécurité. Une telle fluidification ne permet pas, alors que l'atteinte de ces dispositifs au droit à la vie privée et à la protection des données personnelles est importante, de remplir l'exigence de nécessité.

De nombreuses compétitions d'envergures ont été – et sont encore – organisées sans qu'il ne soit recouru à de tels dispositifs techniques, aujourd'hui réservés aux aéroports et aux prisons. Une simple facilité d'organisation apparaît donc insuffisante pour justifier le recours à ces scanners à ondes millimétriques.

En outre, si le législateur a prévu la possibilité de bénéficier d'un autre mode de contrôle alternatif, on sait que le simple refus de se soumettre à ces contrôles sera de nature à générer une suspicion à l'égard de la personne ayant exprimé son désaccord. En pratique, alors que l'article 16 ne prévoit aucune sanction contre un opérateur qui imposerait de fait l'utilisation de ces scanneurs à ondes millimétriques, le dispositif litigieux risque d'être très souvent obligatoire.

De manière générale, on ne peut que constater que – même lorsque les alternatives existent – le manque de moyens humains mis en œuvre par l'administration poussera les spectateurs à se soumettre à ces dispositifs en vue de gagner du temps. C'est d'ailleurs ce risque de manque de moyens à disposition de l'administration qui justifie pour elle le recours à ces scanneurs : les atteintes aux droits fondamentaux induits sont donc justifiés par le choix délibéré de l'administration de ne pas mettre assez de moyens humains. Le consentement des personnes concernées ne sera donc, en pratique, pas libre, spécifique et éclairé.

Le Conseil constitutionnel pourra donc procéder à un contrôle *in concreto* de ces dispositions pour conclure à l'impossibilité, en pratique, de s'assurer de la proportionnalité de ces dispositifs (*cf.* Cons. const., 18 juin 2020, *Loi visant à lutter contre les contenus haineux sur internet*, préc., pt. 19).

Il en résulte que, alors qu'il n'est pas démontré le caractère nécessaire de ce dispositif, le législateur n'a pas opéré une balance équilibrée entre la préservation de l'ordre public et le droit à la vie privée et à la protection des données personnelles. L'article 16 de la loi déférée ne peut donc qu'être déclaré contraire à la Constitution.

III. Sur l'article 17 (article 12 du projet de loi)

L'article 17 de la loi déférée est contraire à l'article 34 de la Constitution, aux articles 5, 8 et 11 de la Déclaration de 1789 en ce qu'il crée une nouvelle incrimination pénale qui, car souffrant d'un manque de

clarté et d'intelligibilité, est disproportionnée et porte atteinte à la liberté d'expression.

En droit, comme rappelé ci-avant, l'article 11 de la Déclaration de 1789 proclame le droit à la liberté d'expression. Par ailleurs, de l'article 34 de la Constitution découle l'exigence de clarté de la loi (*cf.*Cons. const., 21 avril 2005, *Loi d'orientation et de programme pour l'avenir de l'école*, cons. 9).

De plus, aux termes de l'article 8 de la Déclaration de 1789 :

> « *La loi ne doit établir que des peines strictement et évidemment nécessaires, et nul ne peut être puni qu'en vertu d'une loi établie et promulguée antérieurement au délit, et légalement appliquée.* »

Enfin, aux termes de son article 5 :

> « *La loi n'a le droit de défendre que les actions nuisibles à la société. Tout ce qui n'est pas défendu par la loi ne peut être empêché, et nul ne peut être contraint à faire ce qu'elle n'ordonne pas.* »

Il résulte de ces dispositions que le principe de nécessité des peines est constitutionnellement garanti. Il signifie que le législateur incrimine les faits qui lui paraissent suffisamment graves pour justifier d'une réponse pénale et que la sévérité de la peine doit correspondre à la gravité des faits. C'est ainsi que le Conseil constitutionnel a estimé qu'il ressort de l'article 8 de la Déclaration de 1789 « *qu'il appartient au Conseil constitutionnel de vérifier, qu'eu égard à la qualification des faits en cause, la détermination des sanctions dont sont assorties les infractions correspondantes n'est pas entachée d'erreur manifeste d'appréciation* » (*cf.* Cons. const., 16 juillet 1996, *Loi tendant à renforcer la répression du terrorisme et des atteintes aux personnes dépositaires de l'autorité publique ou chargées d'une mission de service public et comportant des dispositions relatives à la police judiciaire*, n° 96-377 DC, cons. 7).

Le Conseil constitutionnel en a déduit que « *si la nécessité des peines attachées aux infractions relève du pouvoir d'appréciation du législateur, il incombe au Conseil constitutionnel de s'assurer de l'absence de disproportion manifeste entre l'infraction et la peine encourue* » (*cf.* Cons. const., 7 avril 2017, *M. Amadou S. [Entreprise individuelle terroriste]*, n° 2017-625 QPC, pt. 13).

Ainsi le Conseil constitutionnel a-t-il censuré la pénalité liée au manquement des obligations à la charge d'une société en matière de recherche d'un repreneur et de consultation du comité d'entreprise au motif que la pénalité pouvait « *atteindre vingt fois la valeur mensuelle du salaire minimum interprofessionnel de croissance par emploi supprimé* » et que dès lors elle revêtait « *un caractère manifestement hors de proportion avec la gravité du manquement réprimé* » (*cf.* Cons. const., 27 mars 2014, *Loi visant à reconquérir l'économie réelle*, n° 2014-692 DC, cons. 13 et 25).

De plus, le Conseil constitutionnel considère qu'est un « *objectif de valeur constitutionnelle* [le principe] *d'accessibilité et d'intelligibilité de la loi* » (*cf.* Cons. const., 16 décembre 1999, *Loi portant habilitation du Gouvernement à procéder, par ordonnances, à l'adoption de la partie législative de certains codes*, n° 99-421 DC, cons. 13). Le double objectif de clarté et d'intelligibilité (bien que leur fondement et leur nature diffèrent) vise à une finalité proche, à savoir « *prémunir les sujets de droit contre une interprétation contraire à la Constitution ou contre le risque d'arbitraire, sans reporter sur des autorités administratives*

ou juridictionnelles le soin de fixer des règles dont la détermination n'a été confiée par la Constitution qu'à la loi » (*cf.* Cons. const., 21 avril 2005, *Loi d'orientation et de programme pour l'avenir de l'école*, préc., cons. 9). Pour satisfaire à l'exigence d'intelligibilité, la loi doit être claire et doit satisfaire à la « *double exigence de loyauté et de clarté* » (*cf.* Cons. const., 2 juin 1987, *Loi organisant la consultation des populations intéressées de la Nouvelle-Calédonie et dépendances prévue par l'alinéa premier de l'article 1er de la loi no 86-844 du 17 juillet 1986 relative à la Nouvelle-Calédonie*, no 87-226 DC, cons. 7 ; Cons. const., 4 mai 2000, *Loi organisant une consultation de la population de Mayotte*, no 2000-428 DC, cons. 15). Bien plus, cet objectif commun prohibe la « *complexité inutile* » (*cf.* Cons. const., 26 juin 2003, *Loi habilitant le Gouvernement à simplifier le droit*, no 2003-473 DC, cons. 5) et « *excessive* » de la loi au regard de l'aptitude de ses destinataires (*cf.* Cons. const., 29 décembre 2005, *Loi de finances pour 2006*, no 2005-530 DC, cons. 77), favorise la simplification du texte législatif (*cf.* Cons. const., 2 décembre 2004, *Loi de simplification du droit*, no 2004-506 DC, cons. 5), combat la contradiction et l'inintelligibilité (*cf.* Cons. const., 18 juillet 2001, *Loi relative à la prise en charge de la perte d'autonomie des personnes âgées et à l'allocation personnalisée d'autonomie*, no 2001-447 DC, cons. 29) et pose simultanément une exigence de précision (*cf.* Cons. const., 19 décembre 2000, *Loi de financement de la sécurité sociale pour 2001*, no 2000-437 DC, cons. 3), préalable nécessaire à l'effectivité de la mise en œuvre de la disposition.

En l'espèce, les dispositions de l'article 17 de la loi déférée créent deux nouvelles infractions : le fait de pénétrer dans une enceinte sportive par force ou par fraude ; les faits de pénétration ou de maintien, sans motif légitime, sur l'aire de compétition d'une enceinte sportive lors du déroulement ou de la retransmission en public d'une manifestation sportive.

Pourtant, le code du sport réprime déjà l'introduction dans les enceintes sportives et pendant le déroulement ou la retransmission en public d'une manifestation sportive de certains objets dangereux ou susceptibles de provoquer des troubles à l'ordre public. Il réprime également certains comportements dangereux lorsqu'ils sont commis au cours d'une manifestation sportive ou de la retransmission en public d'une telle manifestation.

Par ailleurs, les infractions prévues par le code pénal sont applicables lorsqu'elles sont commises au cours de manifestations sportives (atteintes volontaires ou involontaires à la vie, violences, mise en danger d'autrui par violation manifestement délibérée d'une obligation particulière de sécurité ou de prudence imposée par la loi ou le règlement, destructions légères ou dangereuses, etc.).

En particulier, alors que l'article L. 332-10 du code du sport sanctionne actuellement « *le fait de troubler le déroulement d'une compétition ou de porter atteinte à la sécurité des personnes ou des biens, en pénétrant sur l'aire de compétition d'une enceinte sportive* », l'article L. 332-10-1 nouveau du code du sport, créé par l'article 17 de la loi déférée, vient ajouter une nouvelle infraction, sans reprendre l'exigence d'un « *trouble dans le déroulement de la compétition* » ou de l'atteinte à la sécurité des personnes ou des biens. Il s'agira donc seulement, pour entrer dans le champ mal défini de cet article, de se maintenir sur une aire de compétition pour que l'infraction soit constituée, alors même qu'il ne pourrait en résulter aucun trouble pour la compétition.

L'étude d'impact ne vient nullement justifier le caractère nécessaire de ces peines et ne fait qu'affirmer – sans commencement de démonstration – l'existence d'un trouble public par la seule intrusion. Ainsi, il est indiqué :

« *Le fait d'accéder à une enceinte sportive lors du déroulement ou de la retransmission en public d'une manifestation sportive est incriminé lorsqu'il est commis en état d'ivresse ou en état d'ivresse et par force et par fraude.*

Toutefois, le seul fait d'accéder par force ou par fraude à une telle enceinte lors du déroulement ou de la retransmission en public d'une manifestation sportive ne fait l'objet d'aucune incrimination. Or, un tel comportement est de nature à porter atteinte au bon déroulement de la manifestation et à en troubler la tranquillité.

Le fait de pénétrer sur l'aire de compétition d'une enceinte sportive n'est réprimé que lorsqu'il trouble le déroulement d'une compétition ou porte atteinte à la sécurité des personnes ou des biens. En revanche, le seul fait de pénétrer sur l'aire de compétition d'une enceinte sportive lorsqu'il ne trouble pas le déroulement d'une compétition ou ne porte pas atteinte à la sécurité des personnes ou des biens ne fait l'objet d'aucune incrimination. Or, le fait de pénétrer sur l'aire de compétition d'une enceinte sportive, sans motif légitime, est de nature à troubler la tranquillité d'une manifestation sportive alors même que de tels faits ne troublent pas directement le déroulement de la compétition ou ne portent pas atteinte à la sécurité des personnes ou des biens.

Il s'agit par exemple de l'hypothèse de personnes qui entreraient sur la pelouse à l'issue d'une manifestation sportive et qui refuseraient de quitter l'enceinte sportive sans pour autant porter directement atteinte à la sécurité des personnes ou des biens. »

Les objectifs poursuivis sont indiqués comme nécessaires et proportionnés par le seul fait que la mesure « *vise à permettre de poursuivre et sanctionner les personnes qui pénètrent ou se maintiennent sur l'aire de compétition d'une enceinte sportive, sans motif légitime, en réunion ou en récidive. Il s'agit, par exemple, de permettre de sanctionner les personnes, qui à l'issue d'une manifestation sportive, pénètrent sur l'aire de compétition alors qu'elles n'y sont pas autorisées* ».

Si l'étude d'impact met en avant la sécurité de l'évènement, la rédaction retenue est susceptible de concerner des faits sans lien avec la sécurité publique ou des personnes et apporte plus de confusion que de précision. Par exemple, les évènements sportifs d'envergure sont parfois l'occasion pour des militants de la cause environnementale de faire passer des messages au grand public en bénéficiant de l'exposition médiatique générée par les compétitions sportives. Ces actions sont l'expression d'une opinion et entrent dans le champ de la liberté d'expression constitutionnellement protégée.

Or, les nouvelles dispositions pourraient leur être applicables, entraînant la possibilité de les interpeller, les placer en garde à vue et les poursuivre devant un tribunal. Ces dispositions créent donc un risque et peuvent porter atteinte à la liberté d'expression.

L'institution de cette infraction pénalement punissable est donc manifestement disproportionnée et non nécessaire au regard des catégories de personnes qu'elle entend sanctionner et des risques que cela fait peser pour d'autres catégories de personnes.

En outre, l'importance du montant des amendes retenu apparaît non nécessaire et totalement disproportionnée, encore plus lorsque des libertés fondamentales peuvent être en cause.

Enfin, s'agissant des billets infalsifiables, il s'agit vraisemblablement de répondre à l'échec du stade de France lors de l'organisation, en 2022, lors de la finale de la Ligue des Champions. Toutefois, si le ministère de l'intérieur avait au début de l'affaire évoqué des dizaines de milliers de faux billets, il est aujourd'hui acquis que les troubles ont été principalement dus à un concours de circonstances (grève dans les transports publics, politique agressive de maintien de l'ordre, etc.). L'UEFA a elle-même démenti la version présentée par les autorités françaises.

Il en résulte que, cette nouvelle incrimination souffre d'un manque total de nécessité et de proportionnalité. L'article 17 de la loi déférée encourt par conséquent la censure dans sa totalité.

**

Par ces motifs, La Quadrature du Net, le Syndicat des avocats de France, le Syndicat de la magistrature, le CREIS-TERMINAL et la Ligue des Droits de l'Homme estiment que les articles 7, 11 et 12 de la loi relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions sont contraires à la Constitution.

Nous vous prions de croire, Monsieur le président, Mesdames et Messieurs les membres du Conseil constitutionnel, l'assurance de notre plus haute et respectueuse considération.

Pour La Quadrature du Net,
Benoît Piédallu, membre du Collège solidaire

Pour le Syndicat des avocats de France,
Claire Dujardin, présidente

Pour le Syndicat de la magistrature,
Kim Reuflet, présidente

Pour le CREIS-TERMINAL,
Geneviève Vidal, présidente

Pour la Ligue des droits de l'Homme,
Patrick Baudouin, président