Décision n° 2023 – 850 DC

Loi relative aux jeux Olympiques et Paralympiques de 2024
et portant diverses autres dispositions

Liste des contributions extérieures

Services du Conseil constitutionnel - 2023 Plusieurs auteurs peuvent rédiger une contribution commune

	Contributions	
	Date de réception	**Auteur(s)**
1	17/04/2023	Fédération nationale des artisans du taxi (FNAT)
2	17/04/2023	M. David LIBEAU
3	19/04/2023	Groupe Socialistes et apparentés à l'Assemblée nationale
4	19/04/2023	La Quadrature du Net, Syndicat des Avocats de France, Syndicat de la Magistrature, CREIS-TERMINAL, Ligue des Droits de l'Homme
5	24/04/2023	Association canadienne des libertés civiles (*Canadian Civil Liberties Association*, CCLA) Centre des ressources juridiques (*Legal Resources Centre*, LRC, Afrique du Sud) Conseil irlandais pour les libertés publiques (*Irish Council for Civil iberties*, ICCL) Groupe international des droits humains Agora (Russie) Initiative égyptienne pour les droits individuels (*Egyptian Initiative for Personal Rights*, EIPR) Centre européen du droit du secteur non-lucratif (*European Center for Not-for-Profit Law Stichting*) Privacy International
6	02/05/2023	M. le député Philippe LATOMBE

FEDERATION NATIONALE DES ARTISANS DU TAXI
Organisation professionnelle créée en 1939

Monsieur le Président,
Mesdames et Messieurs les membres du
Conseil constitutionnel
2, rue de Montpensier
75OOI PARIS

Par courrier électronique :
contributions-exterieures@conseil-constitutionnel.fr

Paris, le 17 avril 2023

Objet : 2023-850 DC - Contribution extérieure - article 18 de la loi relatif aux jeux Olympiques et Paralympiques de 2024.

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

La loi relative aux jeux Olympiques et Paralympiques de 2024 a été adoptée par l'Assemblée nationale le 11 avril 2023, puis par le Sénat le 12 avril 2023. Elle vous a été transmise le 17 avril 2023, par plus de 60 députés et elle est référencée sous le numéro 2023-850 DC. .

L'article 18 de cette loi modifie la loi n° 2014-1104 du 1er octobre 2014 relative aux taxis et aux voitures de transport avec chauffeur afin de permettre au préfet de police de Paris, à titre expérimental et jusqu'au 31 décembre 2024, de délivrer des autorisations de stationnement nouvelles à des sociétés de taxi et de les faire exploiter avec un véhicule aménagé par un salarié ou un locataire-gérant. Il prévoit également, après un rapport d'évaluation de l'expérimentation, de pérenniser ces autorisations de stationnement dérogatoires au-delà des Jeux Olympiques et de les étendre à l'ensemble du territoire national.

A l'origine, le projet prévoyait de limiter ces nouvelles autorisations au bénéfice des seules personnes morales déjà titulaires d'au moins dix autorisations de stationnements (soit 55 sociétés actuellement sur Paris). Lors de l'examen du texte, les Sénateurs avaient supprimé cette limitation, jugeant ce critère contraire au principe d'égalité, et les députés l'avaient rétablie, estimant qu'il ne paraît pas pertinent d'étendre aux personnes physiques ce dispositif qui ne doit être ouvert qu'aux personnes morales de taille suffisante, du fait de leur capacité à investir et de leur structuration permettant de disposer de retours d'informations fiables.

…/…

La Commission mixte paritaire a retenu une position intermédiaire, en supprimant ce seuil de dix autorisations de stationnement et en réservant ces attributions aux seules sociétés.

La Fédération Nationale des Artisans du Taxi estime que ces dispositions, dont elle avait demandé le retrait, demeurent discriminatoires et anticonstitutionnelles, portant atteinte au principe d'égalité devant la loi.

Cette modification de la loi n° 2014-1104 du 1er octobre 2014, engagée sans concertation avec la profession, va permettre aux sociétés d'obtenir de nouvelles autorisations gratuites leur permettant d'accroitre le parc de leurs véhicules. Par ailleurs, ces autorisations en théorie incessibles pourront être vendues à travers la cession des parts sociales de ces sociétés. Elle leur apportera un avantage économique injustifié, lésant les entreprises individuelles qui ne pourront pas bénéficier de la même faculté. Elle empêchera également les demandeurs inscrits sur liste d'attente d'accéder à ces nouvelles autorisations, malgré plusieurs années d'attente.

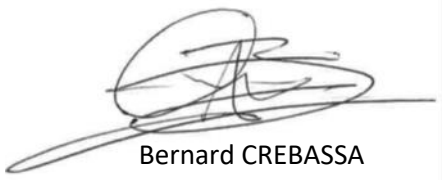
L'article R 3121-12 du code des transports permet déjà au préfet de police de Paris de créer de nouvelles autorisations de stationnement subordonnées à l'utilisation d'équipements permettant l'accès du taxi aux personnes à mobilité réduite. Il est donc possible d'accroitre le parc des taxis aménagés sans avoir recours à cette expérimentation. Cette réforme est donc inutile et n'a pas d'autre objet que de favoriser les sociétés en leur permettant d'obtenir de nouvelles autorisations en dérogeant aux listes d'attente en place et de les exploiter avec un salarié ou un locataire-gérant.

Par ailleurs, il nous apparaît que le Gouvernement a utilisé un véhicule législatif inapproprié pour faire adopter cette mesure. Le Gouvernement a motivé cette mesure par sa volonté de développer la flotte de taxis parisiens accessibles aux personnes se déplaçant en fauteuil roulant à hauteur de 1 000 taxis accessibles d'ici 2024, dans la perspective des jeux Olympiques et Paralympiques. Nous constatons cependant que le texte permet d'attribuer les autorisations de stationnement litigieuses jusqu'au 31 décembre 2024, soit ultérieurement aux épreuves des jeux Olympiques et paralympiques, et qu'il prévoit à terme, après un rapport d'évaluation, leur pérennisation ainsi que leur généralisation à l'ensemble des territoires. Ces dispositions dépassent donc le cadre des jeux Olympiques et Paralympiques et elles auraient dû s'insérer dans un projet de loi relatif aux transports publics particuliers de personnes, comme la loi n° 2014-1104 du 1er octobre 2014 ainsi modifiée.

Pour tous ces motifs, l'article 18 de la loi relatif aux jeux Olympiques et Paralympiques de 2024 doit être déclaré contraire à la Constitution.

Je vous prie de croire, Monsieur le Président, Mesdames et Messieurs les Conseillers, en l'assurance de ma considération respectueuse.

Le Président,



Bernard CREBASSA

Siret : 784 491 672 00050
219 rue de la Croix Nivert 75015 Paris
Tel : 01 44 52 23 50 / Mail : fnat.direction@fnataxi.fr

David Libeau

Le 17 avril 2023 à Paris

Conseil constitutionnel
2 Rue de Montpensier
75001 Paris

Objet : contribution extérieure concernant l'affaire 2023-850 DC

J'ai alerté le Conseil constitutionnel dans une contribution extérieure datée du 18 janvier 2022 du risque que portait l'article 1 du projet de loi renforçant les outils de gestion de la crise sanitaire et modifiant le code de la santé publique concernant la protection des données personnelles et le respect du droit à la vie privée des Français. Dans sa décision n° 2022-835 DC du 21 janvier 2022, le Conseil a jugé que les principales mesures étaient conformes à la constitution. Dans les contributions extérieures publiées par le Conseil, ce dernier a diffusé le QR code d'un pass sanitaire lisible alors que la greffe doit occulter les données personnelles sensibles. **Cette diffusion d'informations de santé a démontré la méconnaissance du Conseil sur le sujet.** Ainsi, je vous propose cette nouvelle contribution extérieure qui concerne cette fois l'article 7 du projet de loi relatif aux jeux Olympiques et Paralympiques de 2024.

Ce projet de loi porte gravement atteinte au respect du droit à la vie privée des citoyens français et étrangers se rendant sur le sol français. L'article 7 introduit la surveillance algorithmique par vidéosurveillance. Sous couvert d'expérimentation, les dispositions précitées sont une première étape, un pied dans la porte, du traitement à grande échelle de données biométriques et de la mise en place de la reconnaissance faciale dans l'espace public. Soumettre toute personne se baladent dans l'espace public à ce type de traitement de données personnelles porte gravement atteinte aux droits fondamentaux de liberté de circulation et droit au respect de la vie privée. Les droits humains sont également bafoués à cause de l'impact environnemental et du micro-travail qu'impliquent ces algorithmes.

Le respect de la vie privée

L'importance du respect de la vie privée comme droit humain est cruciale dans une société démocratique telle que la France. La vie privée est une valeur fondamentale qui garantit la liberté individuelle et la dignité humaine. La protection de la vie privée est essentielle pour préserver la confidentialité des données personnelles et pour éviter l'ingérence de l'État dans la vie privée des citoyens.

La vie privée est considérée comme un droit fondamental Chaque individu a le droit de vivre sa vie sans ingérence indue de la part de l'État ou d'autres personnes. Ce droit inclut la confidentialité des données personnelles, la protection de la correspondance privée, le droit au secret médical et la protection de la vie familiale.

Le respect de la vie privée est également protégé par les traités internationaux, notamment la Convention européenne des droits de l'Homme, qui a été ratifiée par la France en 1974. Selon cet accord, les États membres doivent protéger la vie privée de leurs citoyens et s'abstenir d'interférer dans leur vie privée, sauf dans certaines circonstances exceptionnelles.

En France, la vie privée est considérée comme un droit fondamental qui est protégé par la Constitution. Le Conseil constitutionnel a affirmé, en 1999, que la liberté proclamée par l'article 2 de la Déclaration des droits de l'Homme et du citoyen de 1789 impliquait le respect de la vie privée. L'article 9 du Code civil stipule que « Chacun a droit au respect de sa vie privée. ». Ce droit inclut la protection des données personnelles, la protection de la correspondance privée, la protection de l'image et de la voix des individus, ainsi que le droit au secret médical.

En outre, la loi française sur la protection des données personnelles, la Loi informatique et libertés, a été adoptée en 1978 pour protéger la vie privée des citoyens. Au niveau européen, le Règlement général sur la protection des données personnelles a été adopté en 2016. Ces lois réglementent le traitement et l'utilisation des données personnelles et établit des obligations pour les organismes ou pour l'État qui traitent ces données.

Le respect de la vie privée est essentiel pour préserver la liberté individuelle et la dignité humaine. Il garantit que les citoyens peuvent exercer leurs droits sans ingérence indue de l'État ou d'autres personnes. La protection de la vie privée est également importante pour prévenir l'utilisation abusive des données personnelles et pour protéger les individus contre la discrimination, l'intimidation et la surveillance illégale.

En outre, le respect de la vie privée est essentiel pour protéger la vie familiale et les relations personnelles. Les individus ont le droit de mener leur vie privée sans avoir à craindre des interférences indésirables, qu'il s'agisse de l'État, d'entreprises ou d'autres personnes. La vie privée est également importante pour protéger la dignité des individus et leur intégrité physique, psychologique et morale.

Dans une société démocratique, le respect de la vie privée est crucial pour garantir la transparence et la responsabilité de l'État. Le gouvernement doit être tenu responsables de ses actions et être transparent dans sa gestion des données personnelles et de la vie privée des citoyens. La vie privée est également importante pour protéger la liberté d'expression et la liberté de la presse, car la confidentialité des sources et des informations confidentielles est essentielle pour le fonctionnement des médias.

En conclusion, le respect de la vie privée est un droit fondamental qui est protégé par les traités internationaux et les lois nationales dans de nombreuses démocraties, dont la France. La vie privée est essentielle pour protéger la liberté individuelle, la dignité humaine et la vie familiale. Le respect de la vie privée est également crucial pour garantir la transparence et la responsabilité de l'État et pour protéger la liberté d'expression et de la presse. Dans une société démocratique, le respect de la vie privée est essentiel pour préserver la liberté et la dignité des individus.

La surveillance généralisée

La surveillance généralisée dans une société démocratique comme la France peut être extrêmement préjudiciable pour les droits et les libertés fondamentales des individus. Elle peut entraîner une violation de la vie privée, de la liberté d'expression, de la liberté de la presse et des droits humains en général.

La surveillance généralisée peut porter atteinte à la vie privée des individus en collectant et en traitant des données personnelles sensibles. Ces données peuvent être utilisées pour profiler les personnes en fonction de leur orientation politique, de leur religion, de leur état de santé et de leur vie privée. Les individus peuvent également être surveillés de manière intrusive, comme la surveillance de leurs conversations téléphoniques et de leurs activités en ligne. Cela peut entraîner une perte de confiance dans les institutions gouvernementales et une violation des droits humains.

Une surveillance généralisée peut également restreindre la liberté d'expression et la liberté de la presse. Les journalistes et les individus peuvent être dissuadés de partager des informations importantes par crainte d'être surveillés ou poursuivis. Cela peut limiter la liberté d'expression et la capacité de la presse à informer le public sur les questions importantes, ce qui peut avoir un impact négatif sur la transparence et la responsabilité du gouvernement.

Les inégalités sociales peuvent être renforcée par la surveillance généralisée lorsqu'elle cible les groupes vulnérables tels que les minorités, les immigrés et les personnes à faible revenu. Ces groupes sont souvent les plus susceptibles d'être surveillés et peuvent être stigmatisés ou discriminés en raison de cette surveillance. Cela peut également renforcer le pouvoir des entreprises et des gouvernements en leur donnant un accès inégal aux données et aux informations.

D’une façon générale, la surveillance généralisée a un impact négatif sur la démocratie en sapant la confiance des citoyens dans le gouvernement et en restreignant la participation citoyenne. Les citoyens peuvent se sentir découragés de participer au processus démocratique si leur vie privée est menacée, leur liberté d’expression limitée et leur participation au processus politique entravée. Cela peut avoir des conséquences graves sur la qualité de la démocratie et la participation des citoyens à la vie publique.

En conclusion, la surveillance généralisée dans une société démocratique comme la France peut être extrêmement dangereuse pour les droits et les libertés fondamentales des individus. Elle peut entraîner une violation de la vie privée, de la liberté d’expression, de la liberté de la presse et des droits humains en général. Il est donc essentiel de prendre des mesures pour protéger ces droits et garantir la transparence, la responsabilité et la participation citoyenne dans le processus démocratique.

La surveillance généralisée ne doit pas être considérée comme une solution miracle pour lutter contre le terrorisme, le crime organisé ou d’autres menaces à la sécurité nationale. Des mesures alternatives doivent être envisagées, comme la coopération internationale, la prévention, la réduction des inégalités sociales et l’amélioration de la qualité de vie des citoyens.

Enfin, il est important de souligner que les dangers de la surveillance généralisée ne sont pas seulement théoriques ou hypothétiques, mais qu’ils ont déjà été observés dans de nombreux pays à travers le monde. Il est donc essentiel de rester vigilant et de s’assurer que les droits et les libertés fondamentales des individus sont protégés en tout temps, même dans des situations de crise ou d’urgence.

Vidéosurveillance

La vidéosurveillance et la *vidéoprotection* sont des technologies de surveillance de plus en plus utilisées sur la voie publique en France. Bien que ces systèmes soient présentés comme des outils efficaces pour prévenir la criminalité et améliorer la sécurité, il convient de rappeler qu’aucune étude sérieuse n’a prouvé l’efficacité de la vidéosurveillance. De plus, ils présentent surtout des dangers importants pour les droits et les libertés fondamentales des citoyens.

Le premier danger de la vidéosurveillance est la violation de la vie privée des citoyens. En effet, la surveillance des espaces publics peut permettre de collecter de nombreuses données personnelles, telles que les déplacements, les habitudes de vie ou les contacts sociaux. Ces données peuvent ensuite être utilisées à des fins de surveillance, de profilage ou de ciblage, sans le consentement des citoyens concernés. Cela constitue une atteinte grave à la vie privée et peut nuire à la confiance des citoyens dans l’État et ses institutions.

Le deuxième danger de la vidéosurveillance est le risque de discrimination et de stigmatisation. En effet, les systèmes de vidéosurveillance peuvent être utilisés de manière sélective pour cibler certains groupes de population, tels que les minorités ethniques, les sans-abris ou les personnes ayant un style vestimentaire particulier. Cela peut conduire à des pratiques discriminatoires et à des préjugés injustifiés à l’encontre de ces groupes, et porter atteinte à leur dignité et à leur intégrité.

Le troisième danger de la vidéosurveillance est le risque de dérive autoritaire. En effet, les systèmes de vidéosurveillance peuvent être utilisés pour surveiller les mouvements de l’opposition politique, des militants, des journalistes ou d’autres groupes considérés comme subversifs ou dangereux pour l’ordre public. Cela peut conduire à une restriction de la liberté d’expression, de la liberté de la presse et de la liberté d’association, qui sont des droits fondamentaux dans une société démocratique.

Le quatrième danger de la vidéosurveillance est le risque de banalisation de la surveillance. En effet, en normalisant la surveillance dans l’espace public, les systèmes de vidéosurveillance peuvent conduire à une acceptation croissante de la surveillance dans d’autres domaines de la vie, tels que la surveillance des lieux de travail, des écoles, des domiciles privés ou des espaces en ligne.

Cela peut conduire à une surveillance généralisée de la société, qui porte atteinte à la liberté individuelle et à la vie privée.

Il convient également de noter que la vidéosurveillance peut également avoir des conséquences négatives sur la sécurité publique. En effet, le déploiement de systèmes de vidéosurveillance peut donner l'illusion d'une sécurité accrue, mais peut ne pas être efficace pour prévenir la criminalité. Les criminels peuvent s'adapter en utilisant des moyens pour éviter la détection, tels que le port de masques ou la désactivation des caméras. De plus, la vidéosurveillance peut conduire à un détournement de ressources et de personnel, qui pourrait être mieux utilisé pour des mesures préventives ou des interventions sur le terrain.

En outre, la vidéosurveillance peut également être coûteuse en termes de ressources financières et humaines. Les coûts de déploiement et de maintenance des systèmes de vidéosurveillance peuvent être élevés, en particulier pour les petites villes et les municipalités. De plus, la surveillance constante des images capturées par les caméras peut nécessiter un personnel dédié, qui pourrait être utilisé pour des tâches plus essentielles. A Paris, dans un référé daté du 2 décembre 2021, la Cour de comptes préconise d'engager sans tarder une évaluation de l'efficacité du plan de *vidéoprotection* de la préfecture de police de Paris qui devait initialement couter 225,1 M€, a atteint, au 31 décembre 2020, 343 M€ et devrait couter au total entre 433 à 481 M€ soit deux fois plus que le cout initial [1].

Enfin, la vidéosurveillance peut également contribuer à une culture de la peur et de la méfiance. Les citoyens peuvent se sentir surveillés et surveiller les uns les autres, ce qui peut conduire à une atmosphère de suspicion et de paranoïa. De plus, la surveillance constante peut conduire à une perte de confiance dans les institutions et les autorités, ce qui peut nuire à la légitimité de l'État et de ses institutions.

En conclusion, la vidéosurveillance et la *vidéoprotection* sur la voie publique présentent de nombreux dangers pour les droits et les libertés fondamentales des citoyens, ainsi que pour la sécurité publique et la confiance dans les institutions. Il est donc essentiel de considérer ces risques lors de la mise en place de systèmes de surveillance, et de prendre des mesures pour garantir le respect des droits fondamentaux, ainsi que la transparence et la responsabilité dans le processus décisionnel. De plus, il est important de considérer des alternatives à la vidéosurveillance, telles que la prévention et l'intervention sur le terrain, qui peuvent être plus efficaces pour assurer la sécurité publique et préserver les droits fondamentaux.

IA et algorithmes décisionnels

L'utilisation de l'intelligence artificielle (IA) peut être utile dans certains cas. Par exemple, cette contribution extérieure a été très largement rédigée par *ChatGPT* un logiciel permettant de générer du texte selon des instructions précises permettant un gain temps considérable. L'utilisation de cet outil est d'autant plus à propos dans notre cas que probablement personne ne va lire cette contribution extérieure.

Cependant, les algorithmes dits « d'intelligence artificielle » doivent être nourrit pas une quantité astronomique de données pour leur phase d'entrainement. Ces données d'entrainement peuvent comporter des données personnelles et des données sensibles qu'il est souvent très difficile à détecter et à supprimer. Récemment, *ChatGPT* a fait scandale pour l'utilisation des données personnelles et a été interdit en Italie. Partout dans le monde les autorités chargées de la protection des données ont lancé des enquêtes. A cause de leur conception opaque, de tels algorithmes pourraient ne jamais respecter totalement les dispositions du RGPD [2].

L'utilisation croissante de ce type d'algorithme par les autorités soulève de nombreuses préoccupations quant aux risques pour les droits et les libertés fondamentales des citoyens, ainsi que pour la confiance dans les institutions publiques. En effet, l'utilisation de ces technologies peut potentiellement renforcer les stéréotypes et les biais, violer la vie privée, conduire à une surveillance de masse et à une discrimination systémique.

Tout d'abord, l'utilisation de l'IA et des algorithmes décisionnels peut renforcer les stéréotypes et les biais, qui peuvent affecter négativement les groupes de population déjà marginalisés. Les algorithmes sont souvent formés sur des données historiques, qui peuvent refléter les préjugés et les stéréotypes de la société. Par conséquent, l'IA peut reproduire ces préjugés et renforcer les stéréotypes existants, ce qui peut conduire à une discrimination systémique. Dans le cas de la police, l'utilisation de l'IA peut conduire à une discrimination accrue envers les minorités ethniques et les groupes marginalisés, en particulier dans le domaine du profilage.

De plus, l'utilisation de l'IA et des algorithmes décisionnels peut porter atteinte à la vie privée des citoyens. Les technologies d'IA peuvent être utilisées pour collecter, stocker et traiter de grandes quantités de données personnelles, telles que les données de localisation, les historiques de navigation sur Internet, les achats en ligne et les habitudes de consommation. Ces données peuvent être utilisées pour profiler les individus, pour les suivre et les surveiller, ce qui peut compromettre leur vie privée et leur liberté individuelle. Dans le cas de la police, cela peut conduire à une surveillance de masse et à une violation des droits à la vie privée des citoyens.

En outre, l'utilisation de l'IA et des algorithmes décisionnels par la police peut également conduire à une discrimination systémique. Si les algorithmes sont formés sur des données historiques qui reflètent les préjugés et les stéréotypes de la société, cela peut conduire à une discrimination accrue envers les minorités ethniques et les groupes marginalisés. Par exemple, les systèmes de reconnaissance faciale peuvent être biaisés envers les personnes de couleur, conduisant à des erreurs de reconnaissance et à des arrestations injustes.

Enfin, l'utilisation de l'IA et des algorithmes décisionnels par la police peut également affecter la confiance dans les institutions publiques. Si les citoyens estiment que les décisions importantes sont prises sans intervention humaine, cela peut nuire à la confiance dans les institutions publiques et remettre en question leur légitimité. De plus, si les décisions importantes sont prises par des algorithmes automatisés, cela peut réduire la participation citoyenne et l'engagement dans le processus décisionnel.

En conclusion, il est essentiel de prendre des mesures pour garantir la transparence et la responsabilité dans l'utilisation de ces technologies, afin de minimiser les risques pour les droits des citoyens. Le gouvernement doit être conscients des risques potentiels et doit mettre en place des garde-fous stricts pour garantir que l'utilisation de l'IA et des algorithmes décisionnels ne viole pas les droits humains.

Il est également important de garantir la participation citoyenne et la transparence dans le processus de développement et d'utilisation de l'IA et des algorithmes décisionnels notamment en garantissant l'auditabilité des algorithmes par tous grâce à l'ouverture des codes source. Le gouvernement doit impliquer les citoyens et les groupes de la société civile dans le processus décisionnel, afin de garantir que les préoccupations des citoyens sont prises en compte et que les décisions sont prises de manière responsable.

Impact environnemental de l'IA

Nous devons prendre la mesure de l'urgence climatique mondiale et refuser les technologies destructrices de notre planète. Les algorithmes d'intelligence artificielle sont connus pour avoir un impact non négligeable sur l'environnement. Or, la Charte de l'environnement de 2004 confère à chacun le droit de vivre dans un environnement équilibré et respectueux de la santé.

Le premier danger de l'IA pour l'environnement est la consommation d'énergie. Les réseaux de neurones artificiels sont connus pour être gourmands en énergie, car ils nécessitent de nombreux calculs pour traiter des quantités massives de données. Pour entrainer un algorithme d'intelligence artificielle, ce sont des centaines de processeurs graphique (GPU) qui sont utilisés. Les serveurs qui alimentent les réseaux de neurones consomment donc une quantité considérable d'électricité, ce qui augmente la demande en énergie et contribue à l'émission de gaz à effet de serre.

De plus, les centres de données qui abritent ces ordinateurs peuvent également avoir des effets négatifs sur l'environnement en raison de la production de chaleur qui nécessite une climatisation, et donc une consommation supplémentaire d'énergie ainsi qu'une consommation astronomique d'eau [3].

Un troisième danger est la destruction de l'habitat naturel par la production de déchets électroniques ou l'extraction de minerais. Les entreprises minières qui extraient les minéraux appelés « terres rares » nécessaires à la fabrication de composants électroniques, tels que le cobalt et le coltan, peuvent entraîner la destruction d'habitats naturels et de terres agricoles, ce qui peut avoir des effets négatifs sur les communautés locales et la biodiversité. De plus, les ordinateurs utilisés pour l'IA ont une durée de vie limitée et deviennent rapidement obsolètes, entraînant ainsi la production de déchets électroniques.

En conclusion, l'IA peut avoir des conséquences négatives sur l'environnement, notamment en termes de consommation d'énergie, de production de déchets électroniques, de destruction de l'habitat naturel et d'augmentation des émissions de gaz à effet de serre. Il est donc primordial d'interdire la création des technologies destructrices de l'environnement ou a minima de prévoir des mesures compensatoires fortes.

Micro-travail pour l'IA

L'intelligence artificielle nécessite des quantités massives de données pour être entraînée, et pour cela, les entreprises font souvent appel à des travailleurs et travailleuses du micro-travail pour effectuer des tâches répétitives et fastidieuses de classification de données. Cela pose de réels problèmes en termes de respect des droits humains.

Le micro-travail est souvent effectué par des travailleurs peu qualifiés dans des pays en développement, qui sont payés des salaires très bas pour effectuer des tâches fastidieuses et souvent ennuyeuses. Ces travailleurs sont souvent exposés à des conditions de travail précaires, à des pressions pour travailler de longues heures et à des violations des normes de santé et de sécurité. De plus, ils n'ont souvent pas accès aux avantages sociaux tels que les congés payés, l'assurance maladie et les pensions.

En outre, pour la vidéosurveillance algorithmique implique la reconnaissance de comportements à partir de données issues de la vidéosurveillance ce qui consistera en la classification de vidéos. Dans ce cas, les travailleurs sont susceptibles d'être exposés à des images choquantes et potentiellement traumatisantes, ainsi qu'à des contenus violents ou offensants ce qui peut compromettre leur santé mentale.

De plus, le micro-travail peut également affecter les droits à la vie privée et à la protection des données des individus. Les travailleurs du micro-travail peuvent avoir accès à des données personnelles sensibles, telles que des images biométriques. En plus, ces travailleurs sont souvent situés dans des pays étrangers et leur travail de classification implique donc une transmission de données personnelles à l'étranger dans des pays où la législation en matière de protection des données n'est pas adéquat. Cela peut entraîner des violations de la vie privée.

Enfin, le micro-travail peut également contribuer à renforcer les inégalités économiques et sociales existantes. Les travailleurs du micro-travail sont souvent payés beaucoup moins que les travailleurs dans des emplois traditionnels, ce qui peut créer une pression à la baisse sur les salaires. De plus, le travail du micro-travail est souvent effectué par des personnes dans des pays en développement, ce qui peut renforcer les déséquilibres économiques entre les pays.

En conclusion, l'utilisation de travailleurs du micro-travail pour entraîner des algorithmes d'intelligence artificielle peut avoir des conséquences négatives importantes pour les travailleurs eux-mêmes, ainsi que pour les droits humains et la vie privée des individus. Il est donc important que le gouvernement interdise le micro-travail déshumanisant et oppressant pour l'entrainement des algorithmes de la vidéosurveillance.

Traitement de données biométriques

Le traitement de données biométriques est de plus en plus répandu dans le monde, y compris en France. Les données biométriques comprennent des informations telles que les empreintes digitales, les images faciales, les empreintes rétiniennes, les empreintes palmaires et la reconnaissance vocale. Bien que ces technologies aient des utilisations potentiellement positives, comme l'identification précise des criminels, il existe également de graves dangers pour la vie privée et la sécurité des citoyens lorsque ces données sont mal utilisées ou piratées.

Le premier danger est celui de la violation de la vie privée. Les données biométriques sont des données personnelles sensibles et leur traitement doit être soumis à des règles strictes en matière de protection de la vie privée. Si ces données sont collectées et utilisées sans le consentement des citoyens, cela peut constituer une violation de leur vie privée. De plus, si ces données tombent entre de mauvaises mains, cela pourrait avoir des conséquences désastreuses pour la sécurité des individus. Les identités peuvent être volées, la vie privée peut être compromise, et les citoyens pourraient être victimes de chantage.

Un deuxième danger est lié à l'utilisation de ces données biométriques dans les technologies de surveillance de masse, telles que la reconnaissance faciale. Bien que ces technologies puissent être utilisées pour identifier les criminels, elles peuvent également être utilisées pour surveiller les citoyens innocents. Lorsque les citoyens sont soumis à une surveillance constante, cela peut créer un climat de méfiance et de peur, qui peut saper la confiance dans l'État et les institutions démocratiques.

Un autre danger est la possibilité de discrimination et de biais dans les décisions prises en utilisant ces technologies. Les algorithmes utilisés pour traiter les données biométriques peuvent avoir des biais intégrés, ce qui signifie que les décisions prises sur la base de ces données peuvent être discriminatoires et injustes. Par exemple, si un algorithme est conçu pour reconnaître les visages blancs, il peut avoir du mal à reconnaître les visages de personnes de couleur, ce qui pourrait entraîner des erreurs dans les décisions prises sur la base de ces données.

Enfin, il existe également un risque de piratage des données biométriques. Les données biométriques sont des informations très précieuses, car elles sont uniques à chaque individu et ne peuvent pas être modifiées. Si ces données sont piratées, elles peuvent être utilisées pour voler l'identité des citoyens ou pour accéder à des informations confidentielles.

En conclusion, le traitement de données biométriques dans une société démocratique comme la France présente de nombreux dangers pour la vie privée, la sécurité et la justice. Leur utilisation doit être étroitement contrôlée et réglementée. Les citoyens doivent avoir un droit de regard sur leurs données biométriques et de décider comment elles sont utilisées, afin de protéger leur vie privée et leur sécurité.

Reconnaissance faciale

La reconnaissance faciale est une technique d'identification biométrique qui utilise les caractéristiques du visage d'un individu pour l'identifier de manière unique. Elle est de plus en plus utilisée dans les systèmes de vidéo surveillance sur la voie publique en France, notamment pour lutter contre le terrorisme et la criminalité. Toutefois, l'utilisation de cette technologie soulève des préoccupations importantes en matière de respect de la vie privée et de la protection des données personnelles.

Le premier danger de la reconnaissance faciale est la possibilité d'erreurs et de biais dans les algorithmes utilisés pour l'identification. En effet, les algorithmes de reconnaissance faciale peuvent ne pas reconnaître correctement les visages en fonction de leur couleur de peau, de leur sexe ou de leur âge, ce qui peut conduire à des erreurs d'identification ou à des arrestations injustifiées. De plus, les erreurs de reconnaissance peuvent être amplifiées en cas de mauvaise

qualité des images de surveillance, de contre-jour, de flou ou de mauvaise angle de vue, ce qui peut conduire à des erreurs graves.

Le deuxième danger est lié à la surveillance de masse. La reconnaissance faciale peut être utilisée pour surveiller de manière indiscriminée et systématique les citoyens français sur la voie publique, ce qui constitue une atteinte à leur vie privée et à leur liberté de mouvement. Les systèmes de reconnaissance faciale peuvent être utilisés pour identifier et suivre les individus en temps réel, dresser des profils de leur comportement et collecter des données sur leurs déplacements et leurs habitudes. Cela peut créer une situation de surveillance constante et généralisée qui limite la liberté et l'autonomie des citoyens.

Le troisième danger est lié à la sécurité des données personnelles. Les systèmes de reconnaissance faciale nécessitent la collecte et le stockage de données biométriques sensibles, telles que les images du visage, qui peuvent être utilisées pour identifier les individus même sans leur consentement. La collecte de ces données personnelles peut être effectuée sans transparence ni contrôle de la part des individus concernés, ce qui peut conduire à des abus et des violations de la vie privée. De plus, les données biométriques stockées peuvent être piratées, volées ou utilisées à des fins malveillantes, ce qui peut causer des préjudices graves aux individus concernés.

Le quatrième danger est lié à l'utilisation abusive de la reconnaissance faciale par les autorités. Les systèmes de reconnaissance faciale peuvent être utilisés à des fins illégales ou discriminatoires, telles que la surveillance politique, la surveillance de groupes minoritaires ou la surveillance de manifestants. Ils peuvent également être utilisés pour violer les droits de la défense ou pour contourner les procédures légales, en permettant l'identification de suspects sans preuve suffisante ou sans mandat judiciaire.

En plus de ces préoccupations, la reconnaissance faciale soulève également des inquiétudes quant à la discrimination. Les systèmes de reconnaissance faciale ont tendance à être moins précis pour les personnes de couleur et les femmes, ce qui peut entraîner une surveillance et des accusations injustes. Cela est particulièrement préoccupant dans un pays comme la France, qui lutte contre les discriminations raciales et ethniques.

De plus, la reconnaissance faciale a le potentiel de restreindre la liberté d'expression et de rassemblement. Les manifestants peuvent craindre que leur présence ne soit enregistrée et qu'ils soient identifiés par la suite, ce qui peut dissuader certaines personnes de participer à des manifestations politiques légitimes. En outre, la reconnaissance faciale peut être utilisée pour restreindre l'accès à certains espaces publics ou événements en fonction de critères de sécurité arbitraires et opaques.

Enfin, la reconnaissance faciale peut contribuer à la constitution d'un état de surveillance, où les citoyens sont constamment surveillés et leurs mouvements sont suivis. Cela peut créer un climat de peur et de méfiance dans la société, ce qui peut avoir des conséquences néfastes sur la santé mentale et le bien-être des citoyens.

En conclusion, la reconnaissance faciale par les systèmes de vidéo surveillance soulève de nombreuses préoccupations en matière de vie privée, de discrimination, de liberté d'expression et de rassemblement, ainsi que de surveillance généralisée. Si elle est utilisée de manière inappropriée ou abusive, elle peut porter atteinte aux droits fondamentaux des citoyens français et remettre en question les principes démocratiques de la société. Par conséquent, il est essentiel que les autorités prennent en compte ces risques et établissent des règles claires et des mécanismes de contrôle pour encadrer l'utilisation de cette technologie

Vidéosurveillance algorithmique

L'intelligence artificielle appliquée aux images de vidéosurveillance est envisagé en France. Les algorithmes de la vidéosurveillance algorithmique doivent détecter des événements anormaux dont la liste n'est pas précisée par la loi. L'utilisation de cette technologie soulève de nombreux dangers pour les droits et les libertés fondamentales des citoyens.

Tout d'abord, l'utilisation de l'IA pour détecter des événements anormaux peut conduire à une surveillance de masse généralisée, où chaque mouvement et chaque action des citoyens sont surveillés. Cela peut avoir un effet dissuasif sur la liberté de mouvement et d'expression des citoyens, car ils peuvent craindre d'être constamment surveillés et de faire l'objet d'un examen minutieux.

De plus, l'utilisation de l'IA pour la surveillance peut entraîner des erreurs de jugement et des décisions arbitraires. Les algorithmes peuvent être biaisés en raison des données sur lesquelles ils sont formés, ce qui peut entraîner des erreurs de classification ou des discriminations. Par exemple, un algorithme peut considérer qu'un groupe de jeunes rassemblés est une foule violente, alors qu'il s'agit simplement d'une réunion de famille ou d'amis. Il est également important de rappeler que le profilage et la prise de décision automatisée sont interdites par l'article 22 du RGPD. Pourtant ce projet de loi prévoit le déclenchement automatique d'alertes qui informeront les autorités d'événement anormaux.

Ensuite, la loi précise qu'aucune donnée biométrique ne doit être traitée. Lors du débat parlementaire, des députés ont évoqué le traitement de « points » et de « vecteurs ». Cette description des données traitées élude la question des données biométriques. Dans un récent article scientifique, des chercheurs ont démontré qu'avec quelques secondes d'enregistrement des mouvements de la tête et des mains, il était possible d'identifier les personnes [4]. Cela s'apparente bien à un traitement de données biométrique tel de défini au 14 de l'article 4 du RGPD.

Enfin, les données collectées par ces algorithmes peuvent être utilisées à des fins de profilage et de discrimination. Les gouvernements ou les entreprises pourront utiliser ces données ultérieurement officiellement pour entrainer les algorithmes d'intelligence artificielle, mais ce qui est artificiel sera le contrôle de la CNIL. Sans moyens supplémentaires, cette autorité indépendante ne pourra contrôler efficacement l'utilisation qu'il sera fait de ces données. Nous avons vu récemment la CNIL indiquer n'avoir déclenché aucune enquête sur *ChatGPT* alors que son homologue italien avait interdit l'outil. Il a fallu attendre des plaintes de citoyens pour que la CNIL commence à étudier la question. Un autre exemple, concernant la vidéosurveillance, la CNIL n'a pas traité à temps une plainte sur l'exercice du droit d'accès aux images de *vidéoprotection* me concernant. Les images ont donc été détruites bafouant ainsi mon droit d'accès.

En conclusion, l'utilisation de l'intelligence artificielle pour la surveillance à travers les images de vidéosurveillance soulève de nombreux risques pour les droits et les libertés fondamentales des citoyens. L'actuel projet de loi ne garantit pas un bon équilibre des droits et ouvre la porte à la surveillance biométrique dans l'espace public.

Conclusion

L'expérimentation de la vidéosurveillance algorithmique telle que proposée à l'article 7 du projet de loi relatif aux jeux Olympiques et Paralympiques de 2024 pose de nombreux problèmes.

En premier lieu, **sur le droit à l'information**, le II bis de l'article 7 indique que « Le public est préalablement informé, par tout moyen approprié, de l'emploi de traitements algorithmiques sur les images collectées au moyen de systèmes de *vidéoprotection* […] ». Il apparaît que le législateur fait preuve d'incompétence négative en (i) ne précisant pas les modalités d'information de la mise en place de ces traitements, (ii) en omettant d'informer les personnes lors de la détection d'événements les concernant et l'enregistrement automatique des signalements tel que prévu au 2 du V du même article et (iii) en omettant d'informer les personnes lors de l'utilisation et la conservation d'échantillon d'images collectées filmant les personnes pour l'entrainement des algorithmes d'intelligent artificielle tel que prévu au VIII du même article.

En outre, **sur la durée de conservation des données**, le législateur fait également preuve d'incompétence négative en (i) ne précisant aucun durée de conservation des signalements tel que prévu au 2 du V de l'article 7 et (ii) au VIII du même article, par les mots « peut être utilisé comme données d'apprentissage pendant une durée strictement nécessaire et maximale de douze mois à

compter de l'enregistrement des images », ne prévoit qu'une durée d'utilisation et non une durée de conservation ainsi que (iii), réitéré par les mots « Ces images sont détruites, en tout état de cause, à la fin de l'expérimentation. », le législateur ne prévoit aucune durée de conservation des données d'apprentissage et seulement une durée de conservation des images utilisées pour l'apprentissage.

Ensuite, **sur la destination des données**, le législateur fait également preuve d'incompétence négative mais aussi a fait preuve d'insincérité lors des débats (i) en indiquant au V de l'article 7 que « L'État assure le développement du traitement ainsi autorisé, en confie le développement à un tiers ou l'acquiert. », le législateur confond traitement et algorithme, ne prévoit aucune mesure sur la responsabilité du traitement et de garanties dans l'éventualité où le traitement est confié par l'État à un tiers et notamment concernant les échantillons d'images collectées filmant les personnes pour l'entrainement des algorithmes d'intelligent artificielle tel que prévu au VIII du même article et (ii) en déclarant le 23 mars 2023 lors des débats à l'Assemblée Nationale que « l'État a-t-il lui-même les moyens de développer ces traitements algorithmiques ? La réponse est non » Sacha Houlié, président de la commission des lois et rapporteur, ajoute de la confusion au débat parlementaire et rend le débat insincère à cause de cette déclaration erronée et en contradiction avec le V de l'article 7 qui indique bien que « L'État assure le développement ».

Enfin, **sur l'impact environnemental et humain**, le législateur fait également preuve d'incompétence négative en ne prévoyant aucune mesure d'interdiction ou mesures compensatoires liées aux impacts environnementaux graves qu'implique l'entrainement des algorithmes d'intelligence artificielle prévu au VIII de l'article 7, ainsi qu'aucune interdiction liée au micro-travail ni aucune mesure sur les conditions de travail pour la classification des images de vidéosurveillance pour l'entrainement des algorithmes d'intelligence artificielle.

Pour tous ces motifs, j'estime que **l'article 7 du projet de loi relatif aux jeux Olympiques et Paralympiques de 2024 est contraire à la constitution**.

Amnesty International, *Access Now*, *AlgorithmWatch*, *Centre for Democracy & Technology*, *European Digital Rights*, *Human Rights Watch*, de nombreuses organisations internationales de défense des droits humains ont appelé la France à rejeter la vidéosurveillance algorithmique [5]. Entériner la surveillance algorithmique généralisée de la voie publique serait un grave recul de nos libertés publiques en France.

David Libeau

Références :

[1] Référé : Le plan de vidéoprotection de la préfecture de police de Paris, Cour des comptes, 2022 : https://www.ccomptes.fr/fr/publications/le-plan-de-videoprotection-de-la-prefecture-de-police-de-paris
[2] ChatGPT will probably never comply with GDPR, David Libeau, 2023 : https://blog.davidlibeau.fr/chatgpt-will-probably-never-comply-with-gdpr/
[3] Making AI Less "Thirsty": Uncovering and Addressing the Secret Water Footprint of AI Models, Li *et al.*, 2023 : https://arxiv.org/abs/2304.03271
[4] Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data, Nair *et al.*, 2023 : https://arxiv.org/abs/2302.08927
[5] Rejeter la surveillance dans la loi sur les Jeux Olympiques 2024, 38 organisations, 2023 : https://www.hrw.org/fr/news/2023/03/07/france-rejeter-la-surveillance-dans-la-loi-sur-les-jeux-olympiques-2024

2023-850 DC- Reçu au greffe du Conseil constitutionnel le 19 avril 2023

ASSEMBLÉE NATIONALE

Paris, le 18 avril 2023

Monsieur le Président, Mesdames et Messieurs les membres du Conseil Constitutionnel, les membres du groupe Socialistes et apparentés de l'Assemblée nationale ont l'honneur de vous communiquer les présentes observations concernant la *loi relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions* et singulièrement les dispositions de son article 7 qui autorisent l'expérimentation du système de vidéosurveillance combiné à des traitements algorithmiques.

La mise en œuvre de ces deux technologies – trois si l'on compte l'utilisation des drones – soulève de nombreuses questions puisqu'elles sont susceptibles *« de porter atteinte aux garanties fondamentales apportées aux citoyens pour l'exercice des libertés publiques »* pour reprendre les termes de l'étude d'impact accompagnant le projet de loi visé par les présentes observations. Évoquant, dans une étude de 2022, les systèmes d'intelligence artificielle *« les plus intrusifs ou coercitifs »*, le Conseil d'État mentionne *« l'analyse automatisée d'images captées dans l'espace public par des dispositifs fixes ou embarqués permettant la détection de situations anormales, d'infractions ou de menaces, sans même qu'il soit procédé à l'identification des personnes physiques. En dépit de l'absence d'identification et, en particulier, de mise en œuvre de traitements de reconnaissance faciale, de tels SIA sont susceptibles d'avoir des incidences plus ou moins importantes sur les libertés publiques selon l'usage auquel ils sont destinés. Selon la CNIL, ils présentent « le risque de généraliser un sentiment de surveillance chez les citoyens, de créer un phénomène d'accoutumance et de banalisation de technologies intrusives »*[1]. Anticipant l'intervention du législateur, le Conseil d'État recommandait alors *« la fixation de garanties spécifiques ».*

La question n'est donc pas de savoir si le législateur pouvait permettre une telle expérimentation mais de déterminer si les garanties légales qu'il a édictées sont suffisantes – ou suffisamment spécifiques – pour éviter autant que possible les atteintes aux droits humains et libertés fondamentales qui peuvent en résulter. Il résulte en effet de l'article 34 de la Constitution qu'il appartient au législateur de fixer *« les règles concernant : […] les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ».* Selon les termes de votre jurisprudence, cette disposition de la Constitution impose 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*

[1] Conseil d'État, Étude à la demande du Premier ministre, *Intelligence artificielle et action publique : construire la confiance, servir la performance*, 31 mars 2022, p.137.

*dont la détermination n'a été confiée par la Constitution qu'à la loi » (*Décision n° 2005-512 DC du 21 avril 2005, cons. 9.)

Or il apparaît que les dispositions de l'article 7 manquent manifestement de précision et de clarté et rendent de ce fait indéterminée l'application qui sera faite de cette expérimentation. En effet, l'alinéa 1er prévoit que ces traitements *« ont pour unique objet de détecter, en temps réel, des évènements prédéterminés susceptibles de présenter ou de révéler ces risques [d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes] et de les signaler »*. Cette disposition détermine ainsi les objectifs d'un tel dispositif technologique mais n'explicite pas ce que seront *« les évènements prédéterminés »* que la machine sera chargée de détecter. Cette lacune a été largement soulignée durant les débats parlementaires et le Gouvernement n'a pas souhaité la combler. Il reviendra donc à un décret d'application le soin de préciser *« les évènements prédéterminés que le traitement a pour objet de signaler ».*

Il s'agit là d'un cas classique et manifeste d'incompétence négative, celui où le législateur renvoie au pouvoir réglementaire le soin de déterminer des garanties qui ne relevaient que de la loi. Nous sommes au cœur de la notion telle que la définit Ariane Vidal Naquet : *« Lorsque le législateur commet une incompétence négative, il renonce à fixer les règles et les principes fondamentaux et permet, explicitement ou implicitement, à une autre autorité d'intervenir à sa place. »*[2] Il eut été loisible au législateur, soit d'énumérer les comportements à détecter, soit de fixer des limites précises à respecter dans l'établissement de la liste de ces comportements. À cet égard, durant les débats à l'Assemblée nationale, un amendement qui proposait d'inscrire dans la loi que les traitements algorithmiques ne pouvaient induire de discriminations prohibées par le code pénal a été rejeté. Le pouvoir d'appréciation ainsi laissé au pouvoir réglementaire n'est pas encadré et expose les individus au risque d'arbitraire. En laissant au Gouvernement déterminer, sans limitation aucune, les types de comportement susceptibles de révéler un risque, le législateur a méconnu l'étendue de la compétence qu'il tient de l'article 34 de la Constitution (voir à cet égard notamment votre décision n° 2004-499 DC du 29 juillet 2004, cons.12).

Eu égard aux risques que ces technologies font peser sur les droits et libertés garantis par la Constitution – ce que le Conseil d'État, la CNIL et le Gouvernement reconnaissent – il appartenait au législateur de fixer plus précisément le cadre de leur utilisation et surtout les limites à ne pas franchir.

Ainsi, par les présentes observations, les députés du groupe Socialistes et apparentés demandent à votre Conseil de censurer les dispositions visées.

---

[2] « L'état de la jurisprudence du Conseil constitutionnel sur l'incompétence négative », *Nouveaux cahiers du Conseil constitutionnel*, n°46, janvier 2015, pp.7-15.

Députés signataires :

Boris VALLAUD, Joël AVIRAGNET, Christian BAPTISTE, Marie-Noëlle BATTISTEL, Mickaël BOULOUX, Philippe BRUN, Elie CALIFER, Alain DAVID, Arthur DELAPORTE, Stéphane DELAUTRETTE, Inaki ECHANIZ, Olivier FAURE, Guillaume GAROT, Jérôme GUEDJ, Johnny HAJJAR, Chantal JOURDAN, Marietta KARAMANLI, Fatiha KELOUA HACHI, Gérard LESEUL, Philippe NAILLET, Bertrand PETIT, Anna PIC, Christine PIRES BEAUNE, Dominique POTIER, Valérie RABAULT, Claudia ROUAUX, Isabelle SANTIAGO, Hervé SAULIGNAC, Mélanie THOMIN, Cécile UNTERMAIER, Roger VICOT, députés du Groupe Socialistes et apparentés.

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 respectives ». 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 nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, nº 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

Monsieur le Président du Conseil constitutionnel
2, rue Montpensier
75001, Paris
France

Toronto — Braamfontein — Dublin — Kazan —
Le Caire — La Haye — Londres, le 24 avril 2023

En l'affaire n° 2023-850 DC

concernant la constitutionnalité de la loi relative aux Jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions

CONTRIBUTION EXTÉRIEURE COMMUNE DE 7 ORGANISATIONS NON-GOUVERNEMENTALES INTERNATIONALES ET ÉTRANGÈRES

Monsieur le Président,

Mesdames et Messieurs les membres du Conseil constitutionnel,

Les organisations non-gouvernementales soussignées ont l'honneur de vous présenter la contribution extérieure commune dont la teneur suit :

A. Introduction

1. La présente contribution est produite par l'Association canadienne des libertés civiles, le Centre des ressources juridiques (*Legal Resources Centre*, Afrique du Sud), le Conseil irlandais pour les libertés publics (*Irish Council for Civil Liberties*) le Groupe international des droits humains Agora (Russie), l'Initiative égyptienne pour les droits individuels (*Egyptian Initiative for Personal Rights*), organisations non-gouvernementales, membres du Réseau international des organisations pour les libertés publiques (*International Network of Civil Liberties' Organizations*, INCLO), par le Centre européen du droit du secteur non-lucratif (*European Center for Not-for-Profit Law Stichting*), une ONG de droit néerlandais, et par *Privacy International*, une ONG de droit britannique (ci-après « organisations intervenantes », v. l'annexe). Nos organisations possèdent de l'expérience et l'expertise dans le contentieux et le plaidoyer concernant, notamment, le respect des droits fondamentaux dans la mise en œuvre de mesures de surveillance.

2. Les Jeux olympiques auront lieu en 2024 à Paris. Cet événement d'envergure incomparable à aucun autre va attirer des participants et des supporters du monde entier dans la capitale française. Il est donc évident que les mesures de surveillance adoptées pour les Jeux concernent les étrangers de la même façon que les français. Par conséquent, nos organisations de protection des droits humains internationales et étrangères ont un intérêt à présenter leurs observations au Conseil.

3. La présente contribution a pour objet de critiquer la constitutionnalité de l'article 10 de la loi déférée, de la façon suivante. Après avoir exposé quelques remarques préliminaires sur la pertinence du droit européen pour le présent cas (*infra*, B) les auteurs vont traiter de l'incompétence négative du législateur quant à la définition insuffisante de la technologie de « vidéosurveillance algorithmique » et l'atteinte disproportionnée aux droits fondamentaux (*infra*, C). Enfin, une section sera consacrée à l'applicabilité du Règlement général sur la protection des données de l'Union européenne et le non-respect des principes de traitement des données personnelles (*infra*, D).

B. Remarques préliminaires

4. La présente contribution traite principalement du droit européen (tant celui de l'Union européenne que celui du Conseil de l'Europe), du droit international et du droit comparé concernant la surveillance et les droits fondamentaux. Les auteurs sont conscients de la jurisprudence bien-établie du Conseil issue de sa décision n° 74-54 DC du 15 janvier 1975 dite « IVG »[1]. Cependant, les normes européennes, ainsi que les éléments issus du droit comparé ne sont pas sans incidence sur le contrôle de constitutionnalité des lois par le Conseil. La pratique employée par le Conseil appelle trois remarques à cet égard.

5. *Premièrement*, le Conseil aligne sa jurisprudence avec celle des cours européennes. Le développement de l'objectif de valeur constitutionnelle de l'accessibilité et de l'intelligibilité de la loi suite à la condamnation de la France par la Cour européenne des droits de l'homme dans l'affaire *Zielinski et Pradal*[2] en est un exemple classique.

6. *Deuxièmement*, l'on trouve les extraits des traités internationaux, du droit de l'Union européenne, des arrêts de la Cour européenne des droits de l'homme et de la Cour de justice de l'Union européenne, ainsi que des hautes cours des États

[1] JORF du 16 janvier 1975.
[2] Cour EDH, *Zielinski et Pradal & Gonzalez et autres c. France*, arrêt du 28 octobre 1999, Recueil 1999-VII ; CC, déc. n° 99-421 DC du 16 décembre 1999, « *Codification par ordonnances* », JORF du 22 décembre 1999.

européens dans les dossiers documentaires publiés sur le site Internet du Conseil[3].

7. Enfin, *troisièmement*, la loi déférée elle-même fait référence au Règlement général sur la protection des données du Parlement européen et du Conseil n° UE 2016/679 du 27 avril 2016 (le « RGPD »)[4]. Dès lors, son interprétation ne peut être réalisée, et sa constitutionnalité appréciée, qu'en prenant en compte des dispositions dudit règlement.

C. Incompétence négative résultant en une atteinte disproportionnée au droits constitutionnels

8. Selon la jurisprudence bien-établie du Conseil, le grief d'incompétence négative du législateur implique que celui-ci a renoncé, à fixer les règles et les principes fondamentaux et a permi, explicitement ou implicitement, à une autre autorité d'intervenir à sa place[5].

9. La technologie de vidéosurveillance algorithmique porte atteinte à plusieurs droits constitutionnels, dont la liberté d'aller et venir, le respect de la vie privée[6], et éventuellement, la liberté d'expression et de manifestation. Comme la Cour européenne des droits de l'homme l'a souligné dans sa composition la plus solennelle, dans le domaine du contrôle des technologies de surveillance, la sécurité juridique (légalité) et la proportionnalité des ingérences sont liées l'une à l'autre et s'apprécient ensemble[7]. Tel est le cas de l'article 10 de la loi déférée qui, étant entaché d'incompétence négative, porte une atteinte disproportionnée aux droits garantis.

10. En espèce, le I de l'article 10 de la loi déférée prévoit l'introduction de la technologie de « vidéosurveillance algorithmique » (« les images collectées au moyen de systèmes de vidéoprotection… peuvent faire l'objet de traitements algorithmiques ») dont la définition est constitutionnellement insuffisante, et ce, à plusieurs égards.

---

[3] V., par ex., CC, déc. n° 2004-505 DC du 19 novembre 2004, *Traité établissant une Constitution pour l'Europe*, JORF du 24 novembre 2004 ; déc. n° 2021-940 QPC du 15 octobre 2021, *Air France*, JORF du 16 octobre 2021.

[4] Règlement UE 2016/679 du Parlement européen et du Conseil 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, et abrogeant la directive 95/46/CE, JOUE n° 119 du 4 mai 2016.

[5] V., par ex., CC, déc. n° 2013-336 QPC du 1er août 2013, cons. 16-20 ; déc. n° 2013-684 QPC du 29 décembre 2013, cons. 26.

[6] CC, déc. n° 99-416 DC du 23 juillet 1999, *Loi portant création d'une couverture maladie universelle*, JORF du 28 juillet 1999.

[7] Cour EDH, *Roman Zakharov c. Russie* [GC], n° 47143/06, 4 décembre 2015, CEDH 2015-VIII, para. 236.

11. *Premièrement*, la technologie en cause, tout comme sa définition législative, et malgré plusieurs modifications de la loi déférée lors des débats parlementaires, reste opaque, indéfinie et manque de transparence. En effet, la loi déférée prévoit un traitement des images collectées par les caméras de vidéosurveillance aux fins 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] ».

12. Même si le V de l'article 10 de la loi déférée renvoie au décret pour déterminer ces « événements prédéterminés », le législateur n'a formulé aucun critère permettant d'établir le cadre de l'action du pouvoir réglementaire.

13. Dans la mesure où la technologie est fondée sur le traitement algorithmique des données obtenues par l'apprentissage automatique, la Cour constitutionnelle fédérale d'Allemagne a récemment annulé les lois des *Länder* de Hambourg et de Hesse sur le traitement algorithmique des données par la police. La Cour de Karlsruhe a estimé que ce traitement aboutissait à la production de nouvelles informations pour le renseignement, car le logiciel ouvrait de nouvelles possibilités de compléter les informations disponibles sur une personne, en prenant en compte des données et des hypothèses algorithmiques. Or, ces procédés permettaient ainsi à la police, en un seul clic, de créer des profils complets de personnes, de groupes et de cercles et de soumettre de nombreuses personnes présumées innocentes au regard de la loi, à d'autres mesures policières, si leurs données avaient été collectées dans un certain contexte et que l'évaluation automatisée de ces données conduisait la police à les identifier à tort comme suspects. La Cour a jugé que l'absence de limites légales sur ce type de traitement de données constituait une ingérence disproportionnée dans l'exercice des droits fondamentaux[8].

14. *Deuxièmement*, le V de l'article 10 de la loi déférée prévoit que le décret soit accompagné d'une étude d'impact. Cette étude devra porter sur les bénéfices et les risques posés par le système, ainsi que sur les mesures permettant de rendre ces risques acceptables. Le législateur, sans poser aucun cadre sur le fonctionnement de la technologie, a ainsi établi un cadre restrictif quant à l'étude d'impact. En effet, l'alinéa 7 de l'article 35 du RGPD, applicable en l'espèce (v. le C *infra*), exige que l'analyse d'impact contienne au moins :

> a) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement;
>
> b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités;

[8] BVerfG, 1 BvR 1547/19 und 1 BvR 2634/20, 16. Februar 2023.

> c) une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1 [impact sur la protection des données personnelles]; et
>
> d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

15. Il s'ensuit qu'en ne reprenant qu'une partie des exigences de l'alinéa 7 de l'article 35 du RGPD, le législateur a omis de soumettre les futurs auteurs d'étude d'impact à une obligation d'analyser l'intégralité du fonctionnement de la technologie en cause, la nécessité et la proportionnalité d'atteintes aux droits fondamentaux et la preuve du respect des normes obligatoires sur le traitement des données personnelles.

16. De plus, le législateur a reconnu que la technologie de la « vidéosurveillance algorithmique » peut être entachée de biais, tels que ceux fondés sur le sexe ou la race[9], et les a interdit par principe (le 1° du VI de l'article 10 de la loi déférée). Néanmoins, il n'a assorti cette interdiction d'aucune obligation effective de l'exécutif quant à son exécution d'autant que la conception de la technologie (notamment le choix des échantillons pour l'apprentissage automatique) est déléguée à un tiers. Il n'est ainsi jamais impératif d'obtenir une étude d'impact ou, au minimum, de requérir l' avis d'organismes spécialisés dans la lutte contre les discriminations et du respect des droits de l'homme, comme la Haute autorité de la lutte contre les discriminations et pour l'égalité, la Commission nationale consultative des droits de l'homme ou le Défenseur des droits.

17. *Troisièmement*, l'objet et le but du recours à la « vidéosurveillance algorithmique » est la « mise en œuvre des mesures » contre « des risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes ». Or, de tels risques ne sont jamais définis de façon claire et prévisible. En effet, le Code pénal - que les agents de police et de gendarmerie nationale sont chargés d'appliquer -, définit les atteintes à la personne humaine au titre II du livre II de la partie législative.

18. Parmi ces atteintes, l'on trouve non seulement les violences ayant entraîné une mutilation (article 222-9) et l'exposition d'autrui à un risque de mort (article 223-1), mais aussi la violation du secret professionnel (article 226-13) ou encore le traitement irrégulier des données personnelles (article 226-16), toutes ces

---

[9] L'absence d'une telle étude et l'opacité du choix des échantillons pour l'apprentissage de la technologie ont été les fondements de l'illégalité d'une technologie comparable au Pays de Galles constatée par la Cour d'appel d'Angleterre et du Pays de Galles dans l'affaire *Bridges v. South Wales Police* [2020] EWCA Civ 1058 at 176 and 193. V. aussi CJUE [GC], avis n° 1/15, 27 juillet 2017, para. 172, insistant sur la non-discrimination dans le choix des échantillons à partir desquels les algoritmes du traitement des données sont élaborés.

infractions étant, d'ailleurs, de nature délictuelle. Ces mêmes policiers et gendarmes, tout comme les agents de la SNCF et de la RATP, sont chargés de la « prévention des atteintes à l'ordre public et de protection de la sécurité des personnes et des biens » (pour les agents de la SNCF et de la RATP, v. article L2251-4-1 du Code des transports) sans distinction des atteintes graves et moins graves. La nature des risques à éviter n'étant pas strictement délimitée, le mot « grave » ne permet pas d'établir un critère de distinction, contrairement aux autres définitions plus précises (e.g., « criminelles » ou l'autorisation du traitement des données lors de grands événements limitée par l'article L211-11-1 aux cas de seule menace terroriste).

19. La situation est alors comparable à celle de l'affaire *Roman Zakharov* par laquelle la Cour européenne des droits de l'homme a condamné la Russie au regard d'une législation qui autorisait l'emploi de mesures de surveillance pour des infractions passibles d'au moins 5 ans d'emprisonnement, mais parmi lesquelles se trouvait, entre autres, le vol à la tire (« pickpocketing »)[10].

20. *Quatrièmement*, le I de l'article 10 de la loi déférée autorise la prise d'images par les caméras installées sur les aéronefs. Même si la jurisprudence du Conseil n'interdit pas l'autorisation législative à recourir aux aéronefs, les conditions de constitutionnalité de leur utilisation ne sont pas remplies. Tout comme dans la décision sur la loi dite « sécurité globale », la loi déférée ne précise ni les infractions pour la prévention desquelles les aéronefs sont utilisés, ni aucune limite maximale à la durée d'une autorisation, ni aucune limite au périmètre dans lequel la surveillance peut être mise en œuvre[11].

21. De surcroît, le recours à la « vidéosurveillance algorithmique » pourra commencer dès l'adoption du décret prévu par la loi déférée et durera jusqu'au 31 mars 2025, à savoir 6 mois et 23 jours après la cérémonie de clôture des Jeux paralympiques le 8 septembre 2024. Aucun objectif constitutionnel n'explique le maintien de la technologie une fois les participants et les supporters rentrés chez eux.

D. Violation de l'objectif de valeur constitutionnelle de l'accessibilité et l'intelligibilité de la loi en ce qui concerne le traitement des données personnelles

22. Cette partie de la présente contribution aborde la question du traitement des données personnelles à caractère biométrique au sens du RGPD (a), le procédé du traitement de ces données (b), les objectifs de ce traitement (c) et, enfin, les critères permettant d'assurer sa légalité (d).

---

[10] Cour EDH, *Roman Zakharov c. Russie*, précité, para. 244.
[11] CC, n° 2021-817 DC du 20 mai 2021, *Loi pour une sécurité globale préservant les libertés*, cons. 138-139, JORF du 26 mai 2021.

(a) le traitement des données biométriques et l'applicabilité du RGPD

23. Selon le II de l'article 10 de la loi déférée, le RGPD s'applique aussi bien lors de la conception que de la mise en œuvre de la « vidéosurveillance algorithmique ». Le RGPD régit en premier lieu la protection des données personnelles, notamment biométriques (v., par ex., articles 1, 4 et 9). L'alinéa 14 de l'article 4 du RGPD définit les données biométriques comme :

> les données à caractère personnel 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 ou des données dactyloscopiques.

24. Comme la définition du RGPD comprend les « caractéristiques comportementales », il s'ensuit que le I et le II de l'article 10 de la loi déférée instaure un système de collecte des données biométriques, puisque les « événements prédéterminés susceptibles de présenter ou de révéler des risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes » seront majoritairement des comportements humains, comme résulte, notamment, du 1° du VI du même article qui fait référence à l'« éthique ».

25. Les images collectées par les caméras de vidéosurveillance peuvent non seulement servir à l'identification d'une personne spécifique, mais y sont explicitement destinées. En effet, le I *in fine* du même article prévoit la prise des mesures nécessaires par la police, la gendarmerie etc., qui peuvent être individuelles et individualisées. Aucune disposition de la loi critiquée n'exclut la prise de ces mesures qui relèvent, de toute évidence, de la compétence des autorités susmentionnées.

26. En même temps, le IV du même article prévoit que les traitements des données par le système de la « vidéosurveillance algorithmique » « n'utilisent aucun système d'identification biométrique, ne traitent aucune donnée biométrique et ne mettent en œuvre aucune technique de reconnaissance faciale ». Or, un texte viole l'objectif de valeur constitutionnelle de l'accessibilité et de l'intelligibilité de la loi quand une partie de celui-ci est contraire à l'autre[12]. Tel est le cas des II et IV de l'article 10 de la loi déférée.

(b) procédés du traitement des données biométriques

27. Quel que soit le mode de traitement des données biométriques, qu'il comprenne la reconnaissance faciale (interdite par le IV de l'article 10) ou non, un tel traitement comprend les étapes suivantes :

---

[12] A comparer, CC, déc. n° 2005-530 DC du 29 décembre 2005, *Loi de finances pour 2006*, cons. 77, JORF du 31 décembre 2005.

a) acquisition d'une mesure de référence d'une ou plusieurs caractéristiques physiques, physiologiques ou comportementales d'une personne ;
b) création d'une représentation de cette mesure dans un modèle ;
c) association de ce modèle à un code ou à un objet utilisé pour identifier la personne (le composé du modèle et du code/objet étant souvent appelé le « *master template* ») ;
d) stockage du *master template* dans une base de données ;
e) acquisition de nouvelles mesures (souvent appelées le « *live template* ») des mêmes caractéristiques biologiques ;
f) établissement d'une correspondance entre le *live template* avec le *master template* ;
g) application d'un algorithme pour générer un résultat à partir de la concordance[13].

28. Même si l'article 10 de la loi déférée interdit le recours à la reconnaissance faciale, la « vidéosurveillance algorithmique » utilise exactement le même procédé[14]. Par conséquent, de façon similaire à la question de l'applicabilité du RGPD, le législateur a posé en même temps une norme et son contraire, en violation de l'objectif de valeur constitutionnelle d'intelligibilité de la loi.

(c) objectifs du traitement des données biométriques

29. L'objectif immédiat des systèmes de traitement des données biométriques est généralement l'*identification* d'une personne (c'est-à-dire l'établissement de qui la personne est par rapport à d'autres personnes) ou l'*authentification* (également appelée vérification) d'une personne (c'est-à-dire l'établissement de si une personne est celle qu'elle prétend être). L'identification consiste généralement à comparer les données d'une personne avec les données de plusieurs autres personnes (comparaison 1:n), tandis que l'authentification implique généralement la comparaison des données d'une personne avec les données d'une autre personne (comparaison 1:1), pour établir s'il existe une concordance qui confirme que la première personne est la même que la deuxième[15].

---

[13] V., *The EU General Data Protection Regulation (GDPR): A Commentary*, ed. by Chr. Kuner, Lee A. Bygrave, Chr. Docksey, Oxford University Press 2020, p. 212 (ci-après « *GDPR Commentary* »), description du traitement en général.
[14] Dans l'affaire *Bridges*, précitée, at 9, précisément le même procédé a été appliqué à la reconnaissance faciale.
[15] Article 29 Working Party, *Opinion 3/2012 on Developments in Biometric Technologies*, WP 193, 27 April 2012, pp. 5-6 (Le Groupe de travail « Article 29 » (GT art. 29) est le groupe de travail européen indépendant qui traitait les questions relatives à la protection de la vie privée et aux données à caractère personnel jusqu'au 25 mai 2018, c'est-à-dire avant l'entrée en vigueur du RGPD).

30. Isoler les personnes de la foule (c'est-à-dire, reconnaître leur comportement comme « suspect »), même sans établir les correspondances avec la base de données de référence, les inscrire 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 répond à la définition d'un traitement de données biométriques[16]. Ce que la technologie en question vise finalement, c'est la *catégorisation* biométrique qui est une forme de l'identification biométrique au sens du RGPD (comparaison 1:plusieurs).

31. La définition des données biométriques dans l'alinéa 14 de l'article 4 du RGPD couvre tant l'identification des personnes que leur authentification, ce qui est confirmé par le considérant 51 du préambule[17]. Pour autant que la « vidéosurveillance algorithmique » collecte et traite les données personnelles biométriques, et cela dans le but d'identification des personnes sur les images pour que des mesures de police - individuelles ou individualisées - soient prises, l'article 9 du RGPD s'applique.

(d) critère de la légalité du traitement des données biométriques

32. La dualité des objectifs du traitement des données biométriques (authentification ou identification) n'est cependant pas reprise dans l'article 9 du RGPD. Cette disposition interdit notamment le traitement des données biométriques précisément dans l'objectif de l'identification des personnes. Le fondement de cette mesure est que les systèmes d'identification basés sur la biométrie présentaient une plus grande menace pour les droits et libertés fondamentaux des personnes concernées que les systèmes utilisés à des fins de vérification. En effet, l'utilisation de données biométriques à des fins d'identification est souvent considérée comme plus problématique du point de vue de la protection des données que leur utilisation à des fins de vérification/authentification, principalement parce que cette dernière utilisation ne nécessite pas le stockage de données à caractère personnel dans une base de données centralisée et, parallèlement, implique généralement un traitement des données sur un nombre inférieur de personnes[18].

33. Les exceptions à cette interdiction sont énumérées à l'alinéa 2 de l'article 9 du RGPD de manière exhaustive. Seuls le (a)/(e) et le (g) ce cet alinéa peuvent être pertinents pour justifier la légalité des traitements des données biométriques, c'est-à-dire le traitement des données sur consentement explicite ou des données

---

[16] V. Défenseur des droits, Enquête « Perception du développement des technologies biométriques en France : Entre manque d'information et demande d'encadrement », octobre 2022, p. 3.
[17] *GDPR Commentary*, p. 213.
[18] Article 29 Working Party, *Working Document on Biometrics*, WP 80, 1 August 2003, p. 4.

qui sont manifestement rendues publiques par la personne concernée et/ou le traitement pour des motifs d'intérêt public important.

34. Cependant, le seul fait d'entrer dans une zone surveillée et désignée comme telle (par exemple, les visiteurs sont invités à emprunter un couloir ou un portail spécifique pour pénétrer dans l'espace concerné) ne constitue ni une déclaration ou un acte positif clair indiquant le consentement des personnes concernées[19], ni, par le même biais, le fait de rendre ses données publiques.

35. De même, si l'on admet que la lutte contre la criminalité constitue un motif d'intérêt public important, elle ne justifie pas à elle seule le traitement massif des données personnelles, surtout biométriques[20]. Le préambule du RGPD indique aux considérants 46 et 56 les exemples des motifs d'intérêt public important, à savoir, respectivement, les fins humanitaires, y compris pour suivre des épidémies et leur propagation, ou dans les cas d'urgence humanitaire, notamment les situations de catastrophe naturelle et d'origine humaine et le fonctionnement du système démocratique, en particulier, les activités liées aux élections. Le RGPD ne traite donc pas tous les individus comme des suspects[21]. Et même si le traitement de données biométriques dans ce contexte se trouvait être justifié par un intérêt public, l'article 9(g) du RGPD requiert une appréciation stricte du principe de proportionnalité, ainsi que des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts des personnes concernées - ce que la loi déférée ne prévoit pas.

E. Conclusion

36. La loi déférée tente d'introduire une technologie comparable à la reconnaissance faciale sans l'admettre et tout en le niant. Il est à rappeler que la reconnaissance faciale a été pour la première fois utilisée lors des grands événements sportifs pendant la Coupe du monde de football en Russie en 2018. Loin de la démanteler après la remise du trophée à Hugo Lloris, les autorités russes l'ont étendue d'une région à l'autre, notamment pour poursuivre des opposants.

37. Le législateur français propose aux citoyens du monde entier venus célébrer les Jeux olympiques et paralympiques de se soumettre à un système de surveillance inconnu et opaque dont la réglementation législative est pleine de contradictions internes. La loi elle-même proclame le respect du RGPD et contient plusieurs

---

[19] Comité européen de la protection des données, *Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo*, 29 janvier 2020, para. 46.
[20] V., quoique dans le contexte de discrimination, CJUE [GC], *Huber c. Bundesrepublik Deutschland*, aff. n° C-524/06, 16 décembre 2008, paras. 77-80.
[21] Rétention des données biométriques des personnes non condamnées pénalement serait contraire à l'article 8 de la Convention EDH. V., Cour EDH [GC], *S. et Marper c. Royaume-Uni*, n°30562/04 30566/04, 4 décembre 2008, CEDH 2008-V, para. 125.

dispositions incompatibles avec celui-ci. Le système restera fonctionnel pendant plus de 6 mois après la clôture des Jeux pour des raisons obscures.

Association canadienne des libertés civiles (*Canadian Civil Liberties Association*, CCLA)

Centre des ressources juridiques (*Legal Resources Centre*, LRC, Afrique du Sud)

Centre européen du droit du secteur non-lucratif (*European Center for Not-for-Profit Law Stichting*)

Conseil irlandais pour les libertés publiques (*Irish Council for Civil Liberties*, ICCL)

Groupe international des droits humains Agora (Russie)

Initiative égyptienne pour les droits individuels (*Egyptian Initiative for Personal Rights*, EIPR)

Privacy International

Personne de contact :
M. Kirill Koroteev,
Responsable du contentieux international,
Groupe international des droits humains Agora
(kirill.koroteev@gmail.com)

ANNEXE : Présentation des organisations intervenantes

Association canadienne des libertés civiles (*Canadian Civil Liberties Association*, CCLA)

La CCLA est une organisation non-gouvernementale non-partisane, nationale et à but non lucratif qui est à l'avant-garde de la protection des libertés fondamentales et de la vie démocratique au Canada depuis 1964. La CCLA a été constituée pour promouvoir le respect des droits fondamentaux et des libertés publiques, défendre et favoriser la reconnaissance de ces droits et libertés. Les principaux objectifs de la CCLA comprennent la promotion et la protection juridique de la liberté individuelle et de la dignité humaine contre l'invasion déraisonnable de l'autorité publique, et la mise en œuvre des obligations constitutionnelles et internationales du Canada dans les juridictions canadiennes.

Centre des ressources juridiques (*Legal Resources Centre*, LRC, Afrique du Sud)

Le LRC est une clinique juridique d'intérêt public et à but non lucratif qui utilise le droit comme instrument de justice. Il a été créé en 1979 et est la plus grande clinique du droit des droits de l'homme d'intérêt public en Afrique du Sud. En plus de son bureau national et de son unité de contentieux constitutionnel, le LRC dispose de quatre bureaux régionaux, au Cap, Durban, Grahamstown et Johannesbourg. Le LRC fournit des services juridiques aux personnes vulnérables et marginalisées, y compris les personnes et les communautés pauvres, sans abri et sans terre d'Afrique du Sud qui souffrent de discrimination en raison de leur race, de leur classe, de leur sexe, de leur handicap ou en raison de circonstances sociales, économiques et historiques.

Centre européen du droit du secteur non-lucratif (*European Center for Not-for-Profit Law Stichting*)

Le Centre européen du droit du secteur non-lucratif (*European Center for Not-for-Profit Law Stichting*), avec le siège à La Haye, aux Pays Bas, a plus de 20 ans d'expérience dans la défense des libertés civiques pour les groupes, mouvements et activistes. Notamment, ECNL s'engage dans le plaidoyer lié aux lois et politiques mondiales, régionales et nationales concernant l'intelligence artificielle et technologies émergeantes, y compris le règlement de l'UE sur l'IA et la Convention-cadre du Conseil de l'Europe sur l'IA.

Conseil irlandais pour les libertés publiques (*Irish Council for Civil Liberties*, ICCL)

L'ICCL a été fondée en 1976 par l'ancienne Présidente de l'Irlande Mary Robinson et des militants, des avocats et des universitaires. Depuis 40 ans, l'ICCL travaille à la protection et à la promotion des droits de l'homme pour toutes les personnes vivant en Irlande, il a

participé à certaines des plus grandes campagnes de l'histoire irlandaise, aboutissant à une Irlande plus tolérante et plus égalitaire. Le travail d'ICCL a impliqué la promotion du mariage des personnes du même sexe avant le référendum de 2015, l'établissement d'une commission des médiateurs indépendants de la *Garda Síochána* (force de police irlandaise), la campagne pour la légalisation du droit au divorce, une protection plus efficace des droits des enfants, la dépénalisation de l'homosexualité et l'introduction d'une législation renforcée sur l'égalité.

Groupe international des droits humains Agora (Russie)

Agora est une association de plus de 100 avocats et autres professionnels du droit engagés dans le contentieux des droits de l'homme au niveau national et international. Les équipes juridiques permanentes d'Agora travaillent dans plusieurs villes de Russie et à l'étranger. Une unité d'intervention qui traite les incidents impliquant des violations des droits de l'homme opère dans toute la partie européenne de la Russie. Agora représente actuellement des requérants dans plusieurs centaines des affaires introduites devant la Cour européenne des droits de l'homme et les comités de l'ONU. Agora apporte également un soutien aux émigrés politiques, aux exilés et aux demandeurs d'asile. Elle est également active dans les États post-soviétiques où l'impact négatif des pratiques russes sur la situation des droits de l'homme se fait fortement sentir.

Initiative égyptienne pour les droits individuels (*Egyptian Initiative for Personal Rights*, EIPR)

L'EIPR est une organisation de défense des droits de l'homme indépendante à but non lucratif qui a été créée en 2002 pour promouvoir et défendre les droits et libertés individuels en Égypte. L'EIPR s'efforce d'obtenir un impact mesurable au niveau national et de soutenir la constitution d'un groupe autour de ses priorités thématiques, tout en participant activement au plaidoyer régional et international et en contribuant au mouvement international des droits de l'homme à la fois en établissant des partenariats stratégiques et en fournissant contribution aux processus de normalisation et de recherche de consensus.

Privacy International

Privacy International est une organisation non-gouvernementale basée à Londres (Charity No. 1147471), qui plaide pour des solutions juridiques et technologiques pour protéger les personnes et leurs données. PI a notamment conseillé des organisations internationales telles que le Conseil d'Europe ou l'Agence des Nations Unies pour les réfugiés. Elle intervient aussi régulièrement dans des affaires liées aux droits humains et à la technologie devant les tribunaux nationaux, régionaux et internationaux.

Philippe Latombe
Député de la Vendée
Commissaire aux Lois
Commissaire à la CNIL

Paris le 21 avril 2023,

Monsieur le Président,
Mesdames et Messieurs le Membres du Conseil Constitutionnel,

Alors que j'étais corapporteur d'une mission sur les images de sécurité, dont le rapport vient d'ailleurs d'être publié, j'ai tout naturellement été sollicité par mon groupe parlementaire, le Groupe démocrate, afin de suivre le parcours législatif du Projet de loi sur les Jeux Olympiques et Paralympiques, et ce, jusqu'à la CMP. Je suis, par ailleurs, vice-président du groupe d'études Economie, sécurité et souveraineté numériques.

Le Groupe LFI a souhaité vous interroger sur la constitutionnalité du texte, mais je ne suis pas inquiet, car je pense que nous avons produit un dispositif équilibré et proportionné, notamment pour ce qui est de son article 7 si discuté. J'ai bon espoir qu'il passera sans encombre par les fourches caudines de votre examen.

En revanche, je souhaite attirer votre attention sur un amendement transpartisan du Groupe d'études Economie, sécurité et souveraineté numériques, (n°757), déposé à l'Article 7 alinéa 13, et qui a été voté par l'Assemblée Nationale.

Cet amendement se référait à l'article 19.6 du référentiel d'exigences dit « SecNumCloud » intitulé Protection vis-à-vis du droit extra-européen, appliqué par l'Agence nationale de la sécurité des systèmes d'information et qui vise à assurer des garanties de sécurité aux systèmes d'information labellisés.

Le texte issu du vote à l'Assemblée était ainsi libellé : « L'État assure le développement du traitement ainsi autorisé, en confie le développement à un tiers ou l'acquiert. Dans ces deux derniers cas, **il veille à ce que le tiers qui va développer ou développe cette solution soit prioritairement une entreprise qui répond à l'ensemble des règles de l'article 19.6 du référentiel d'exigences dit « SecNumCloud** ».

Le point abordé portait précisément sur la protection contre l'extraterritorialité de droits extra européens. Le but consistait à faire en sorte que les entreprises des tiers qui vont développer ou qui développent la solution d'intelligence artificielle envisagée soient établies dans l'Union européenne, les critères retenus étant le siège statutaire, l'administration centrale et le principal établissement du tiers en question.

ASSEMBLÉE NATIONALE

Or, à la sortie de la CMP, le texte était ainsi modifié : « ...**il veille à ce que le tiers qui va développer ou développe cette solution soit prioritairement une entreprise qui répond aux règles de sécurité définies par l'Agence nationale de la sécurité des systèmes d'information s'agissant du respect des exigences relatives à la cybersécurité.** », soit une formulation qui n'intègre pas les conditions d'immunité aux lois d'extra-territorialité étrangères, ce qui me paraît fortement dommageable.

Il semble que mes collègues du Sénat aient été induits en erreur par un courrier, qui leur a été adressé par un cabinet de lobbying, et les a amenés à croire qu'aucune entreprise française ne serait en mesure de fournir le service attendu (ce qui est faux) et qu'il ne fallait donc pas introduire des conditions restrictives qui rendraient impossible le recours à des sociétés étrangères. Cette hypothèse était déjà prise en compte dans l'amendement voté à l'Assemblée avec l'adverbe « prioritairement » et ne nécessitait donc pas d'être récrit.

L'immunité aux lois extraterritoriales constitue un prérequis de la souveraineté numérique que ne prend pas en compte la récriture de ce passage. Ainsi affaibli, le texte ne protège pas les données personnelles, sensibles par nature, et ce en contradiction avec le rapport du Conseil d'Etat du 31 août 2022 sur l'Intelligence artificielle (Intelligence artificielle et action publique : construire la confiance, servir la performance).

Le texte ne s'inscrit pas non plus dans une cohérence avec les décisions prises par la CJUE depuis l'arrêt dit « Schrems II », qui a invalidé le régime des transferts de données entre l'Union européenne et les États-Unis (Privacy shield), ni dans la tendance clairement affirmée par cette même cour d'élargir le périmètre des données personnelles considérées comme sensibles, et donc de protéger de plus en plus de données. Pour toutes ces raisons, je souhaiterais de votre part une réserve d'interprétation.

Alors que les députés insoumis et écologistes ont annoncé ce lundi 17 avril qu'ils déposaient un recours, estimant notamment que certaines mesures sécuritaires contreviennent et au « droit au respect de la vie privée », il m'a semblé important d'attirer votre attention sur ce point particulier du dispositif.

Je me tiens bien évidemment à votre disposition pour échanger sur ce sujet et vous prie de croire, Monsieur le Président, Mesdames et Messieurs les Membres du Conseil Constitutionnel, à l'assurance de ma respectueuse considération.