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.