EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

TROISIÈME SECTION

AFFAIRE GLUKHIN c. RUSSIE

(Requête nº 11519/20)

ARRÊT

Art. 10 • Liberté d'expression • Condamnation injustifiée pour infraction administrative – à savoir pour défaut de notification préalable de la manifestation – d'une personne qui avait manifesté individuellement et pacifiquement en s'étant munie d'une silhouette en carton, grandeur nature, d'un militant politique, représenté brandissant une banderole • Autorités n'ayant pas fait preuve du degré de tolérance requis • Manquement à l'obligation de fournir des motifs pertinents et suffisants

Art. 8 • Vie privée •Traitement injustifié des données personnelles biométriques du requérant à raison de l'utilisation, dans le cadre d'une procédure pour infraction administrative, d'une technologie de reconnaissance faciale, très intrusive, en vue de l'identification, de la localisation et de l'arrestation de l'intéressé • Risque que le recours à de telles technologies aux fins de l'identification et de l'arrestation de manifestants pacifiques ait un effet dissuasif sur l'exercice des droits à la liberté d'expression et à la liberté de réunion • Nécessité d'établir, dans le cadre de la mise en place de technologies de reconnaissance faciale, des règles détaillées quant à la portée et à l'application des mesures, ainsi que des garanties fortes contre les risques d'abus et d'arbitraire • Nécessité de garanties accrues en cas d'utilisation de technologies de reconnaissance faciale à la volée • Ingérence ne répondant pas à un « besoin social impérieux »

STRASBOURG

4 juillet 2023

DÉFINITIF

4/10/2023

Cet arrêt est devenu définitif dans les conditions définies à l'article 44 § 2 de la Convention. Il peut subir des retouches de forme.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

En l'affaire Glukhin c. Russie,

La Cour européenne des droits de l'homme (troisième section), siégeant en une chambre composée de :

Pere Pastor Vilanova*, président*,
Jolien Schukking,
Yonko Grozev,
Georgios A. Serghides,
Peeter Roosma,
Andreas Zünd,
Oddný Mjöll Arnardóttir*, juges*,

et de Milan Blaško, *greffier de section*,

Vu :

la requête (n° 11519/20) dirigée contre la Fédération de Russie et dont un ressortissant russe, M. Nikolay Sergeyevich Glukhin (« le requérant ») a saisi la Cour en vertu de l'article 34 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (« la Convention ») le 31 janvier 2020,

la décision de porter à la connaissance du gouvernement russe (« le Gouvernement ») les griefs formulés sur le terrain des articles 6 § 1, 8 et 10 de la Convention, et de déclarer la requête irrecevable pour le surplus,

les observations communiquées par le Gouvernement et celles communiquées en réplique par le requérant,

les commentaires reçus de l'organisation non-gouvernementale ARTICLE 19, que le président de la section avait autorisée à se porter tierce intervenante,

le fait que le Gouvernement n'a pas communiqué d'observations en réplique aux observations de la tierce intervenante et l'absence de toute communication de la part du Gouvernement depuis le mois de mars 2022,

la décision du président de la section, appliquant par analogie l'article 29 § 2 du règlement de la Cour (« le règlement »), de désigner l'un des juges siégeant à la Cour pour faire office de juge *ad hoc* (pour une explication du contexte dans lequel s'inscrit cette pratique, voir *Kutayev c. Russie*, n° 17912/15, §§ 5-8, 24 janvier 2023),

Après en avoir délibéré en chambre du conseil le 23 mai et le 13 juin 2023,

Rend l'arrêt que voici, adopté à cette dernière date :

INTRODUCTION

1. L'affaire concerne la condamnation du requérant pour infraction administrative au motif qu'il n'avait pas notifié aux autorités son intention de manifester individuellement muni d'un « objet rapidement (dé)montable ». Au cours de l'enquête, les services de police eurent recours à une technologie de reconnaissance faciale pour traiter les données personnelles du requérant.

EN FAIT

2. Le requérant est né en 1985 et réside à Moscou. Il a été représenté par Mes N. Zboroshenko et A. Rossius, avocats à Moscou.

3. Le Gouvernement a été représenté par le représentant de la Fédération de Russie auprès de la Cour européenne des droits de l'homme, à savoir d'abord M. A. Fedorov, puis M. M. Vinogradov, qui a succédé à celui-ci.

4. Les faits de la cause peuvent se résumer comme suit.

5. En mai 2017, il fut annoncé sur le site officiel du maire de Moscou que plus de 3 500 caméras de vidéosurveillance avaient été installées dans la ville. Au mois de septembre de la même année, plus de 3 000 caméras de vidéosurveillance furent équipées d'un système de reconnaissance faciale à la volée. Au printemps 2018, des caméras de vidéosurveillance permettant la reconnaissance faciale furent installées dans le métro de Moscou. Selon le maire de la ville, un système de reconnaissance faciale à la volée fut testé en 2019. Au 1er septembre 2020, toutes les caméras de vidéosurveillance de Moscou – il y en avait environ 175 000 à l'époque, et plus de 220 000 en 2022 – étaient équipées d'une technologie de reconnaissance faciale à la volée.

6. Le 12 août 2019, un militant politique, M. Konstantin Kostov, fut arrêté et inculpé, au titre de l'article 212.1 du code pénal russe, d'infractions répétées à la réglementation relative aux « événements publics ». La détention de M. Kostov et la procédure pénale dirigée contre lui eurent un grand retentissement dans les médias et au sein de l'opinion publique, et elles suscitèrent un tollé général.

7. Le 23 août 2019, le requérant prit le métro moscovite en s'étant muni d'une silhouette en carton, grandeur nature, de M. Kotov, lequel était représenté en train de brandir une banderole sur laquelle était inscrit le message suivant : « Vous vous f***ez de moi. Je suis Konstantin Kotov. Je risque jusqu'à cinq ans [de prison] au titre [de l'article] 212.1 pour des manifestations pacifiques. »

8. Il ressort d'un rapport des services de police daté du 24 août 2019 que dans le cadre de sa « surveillance d'Internet », l'unité anti-extrémisme de la police du métro de Moscou (« l'unité anti-extrémisme de la police ») avait découvert une photographie montrant, dans une station de métro, un homme qui se tenait debout aux côtés d'une silhouette représentant une personne munie d'une banderole.

9. L'unité anti-extrémisme de la police prit alors des captures d'écran d'une chaîne Telegram publique où figuraient des photographies et une vidéo montrant le requérant qui tenait la silhouette en carton de M. Kotov dans une station de métro et à bord d'une rame de métro. Le message inscrit sur la banderole (paragraphe 7 ci-dessus) était clairement lisible sur les captures d'écran. L'unité anti-extrémisme de la police imprima les captures d'écran et

les conserva « conformément au chapitre 26 du code des infractions administratives » (« le CIA » – paragraphes 26-27 ci-dessous).

10. Il ressort d'un autre rapport des services de police daté du 24 août 2019 que l'unité anti-extrémisme de la police se procura les enregistrements vidéo réalisés par les caméras de vidéosurveillance installées dans les stations de métro Chistye Prudy et Sretenskiy Bulvar. L'unité anti-extrémisme de la police visionna ces enregistrements le 27 août 2019, prit des captures d'écran d'images où figurait le requérant, les imprima et les versa au dossier de l'affaire.

11. Il ressort d'un rapport des services de police en date du 26 août 2019 que l'unité anti-extrémisme de la police prit des « mesures opérationnelles d'investigation » dans le but d'identifier l'homme qui apparaissait sur les photographies et dans la vidéo publiées sur Telegram, qu'elle conclut qu'il s'agissait du requérant et qu'elle découvrit son adresse.

12. Le requérant affirme que des agents de l'unité anti-extrémisme de la police se sont rendus chez lui en son absence le 30 août 2019, vers 10 heures du matin. Vers 11 heures du matin le même jour, il fut arrêté par la police dans une station de métro. Le requérant allègue que les agents de police lui ont dit qu'il avait été identifié au moyen des caméras de vidéosurveillance équipées d'un système de reconnaissance faciale installées dans le métro de Moscou.

13. Le requérant fut ensuite conduit à un poste de police, où il fut inculpé, sur le fondement de l'article 20.2 § 5 du CIA, de l'infraction administrative de non-respect de la procédure établie pour la conduite d'événements publics. Le procès-verbal d'infraction mentionnait que le 23 août 2019, le requérant avait manifesté individuellement en utilisant un « objet rapidement (dé)montable » dans la station de métro Chistye Prudy et à bord d'une rame de métro, et qu'il aurait donc dû informer au préalable les autorités locales de cette manifestation.

14. Le 2 septembre 2019, le chef par intérim de l'unité anti-extrémisme de la police adressa au chef de la sécurité du métro de Moscou une lettre dans laquelle il lui demandait de lui transmettre des copies des enregistrements vidéo réalisés le 23 août 2019 entre 20 h 15 et 20 h 35 par 22 caméras de vidéosurveillance installées dans la station de métro Okruzhnaya. Il fondait cette demande sur les articles 6-3, 7-2 § 1 et 15-1 de la loi sur les mesures opérationnelles d'investigation (paragraphes 22-23 et 25 ci-dessous) ainsi que sur l'article 13-1 § 4 de la loi sur les services de police (paragraphe 29 ci-dessous). Il ajoutait que sa demande concernait une enquête menée aux fins de la lutte contre l'extrémisme dans le cadre des manifestations publiques de masse autorisées à Moscou. L'unité anti-extrémisme de la police visionna les enregistrements en question le 5 septembre 2019, prit des captures d'écran d'images où figurait le requérant, les imprima et les versa au dossier de l'affaire.

15. Le 23 septembre 2019, le tribunal du district Meshchanskiy de Moscou jugea le requérant coupable des faits qui lui étaient reprochés. Notant que le requérant avait présenté des observations orales et avait plaidé non coupable, il s'appuya entre autres sur les captures d'écran de la chaîne Telegram et celles des enregistrements vidéo provenant des caméras de vidéosurveillance du métro pour conclure que l'intéressé avait manifesté individuellement en utilisant un « objet rapidement (dé)montable ». Il jugea que, contrairement à ce que soutenait le requérant, la silhouette en carton de M. Kotov pouvait être considérée comme un « objet rapidement (dé)montable » car elle était dotée d'un support. Il condamna le requérant à payer une amende de 20 000 roubles russes (RUB ; environ 283 euros).

16. Le requérant fit appel cette décision. Il alléguait en particulier que les mesures opérationnelles d'investigation qui avaient été mises en œuvre aux fins de son identification étaient illégales, la loi sur les mesures opérationnelles d'investigation ne permettant pas, selon lui, la prise de telles mesures dans le cadre d'une enquête sur une infraction administrative. Il soutenait que les éléments que ces mesures avaient permis de recueillir étaient donc irrecevables. Par ailleurs, il se plaignait de l'absence de partie poursuivante, situation qui selon lui portait atteinte au principe d'impartialité. Enfin, il soutenait que sa condamnation pour une manifestation individuelle pacifique s'analysait en une atteinte à son droit à la liberté d'expression, et qu'il n'avait jamais été prétendu que sa manifestation eût présenté le moindre risque pour l'ordre public ou pour la vie ou la santé d'autrui.

17. Le 30 octobre 2019, le tribunal de Moscou confirma, en appel, la condamnation du requérant. Le requérant était présent à l'audience, durant laquelle il formula des observations orales. Constatant que le requérant avait été condamné pour une infraction à la procédure établie pour la conduite d'événements publics, à savoir un manquement à l'obligation de notification préalable, le tribunal jugea que le caractère pacifique de la manifestation était dépourvu de pertinence. Il considéra que le transfert du requérant au poste de police et son arrestation administrative étaient légaux, et que, lors de la découverte de l'infraction et de la collecte de preuves, les services de police avaient agi conformément à la loi sur les services de police.

LE CADRE JURIDIQUE PERTINENT

I. LA PROCÉDURE PRÉVUE POUR LA CONDUITE D'ÉVÉNEMENTS PUBLICS

18. La loi sur les événements publics (loi n° 54-FZ du 19 juin 2004) prévoit qu'aucune notification n'est requise pour les manifestations individuelles, à l'exception des cas où le manifestant a l'intention d'utiliser un « objet rapidement (dé)montable » (« *быстровозводимая сборно-разборная конструкция* ») (article 7 § 1 point 1). Une manifestation

individuelle accompagnée de l'usage d'un tel objet, susceptible de faire obstacle à la circulation des piétons ou des véhicules, doit être notifiée aux autorités trois à quatre jours à l'avance (article 7 § 1).

19. Il est interdit d'organiser un événement public n'ayant pas été notifié dans les délais prévus par la loi (article 5 § 5).

20. L'article 20.2 § 5 du code des infractions administratives (« le CIA ») prévoit que le non-respect, par un participant à un événement public, de la procédure établie pour la conduite de tels événements est passible, s'il n'a pas porté atteinte à la santé d'autrui ou à des biens, d'une amende d'un montant compris entre 10 000 RUB et 20 000 RUB ou de travaux d'intérêt général d'une durée maximale de quarante heures.

II. LES MESURES OPÉRATIONNELLES D'INVESTIGATION

21. La loi sur les mesures opérationnelles d'investigation (loi n° 144-FZ du 12 août 1995 – « la LMOI ») prévoit que les mesures opérationnelles d'investigation visent les buts suivants : a) la détection, la prévention, la répression des infractions pénales et les investigations sur celles-ci, ainsi que l'identification des personnes qui se préparent à commettre une infraction pénale, qui en commettent ou qui en ont commis une ; b) la recherche des personnes qui tentent de se soustraire à la justice et des personnes portées disparues ; c) l'obtention d'informations sur des faits ou activités qui mettent en péril la sécurité nationale, militaire, économique ou écologique de la Fédération de Russie ; d) l'obtention d'informations sur des biens faisant l'objet d'une mesure de confiscation (article 2 de la LMOI).

22. Il est autorisé, dans le cadre de telles mesures, de procéder à des enregistrements audio et vidéo, de photographier, de filmer et de recourir à d'autres moyens techniques, sous réserve que cela ne soit pas préjudiciable à la vie ou à la santé des personnes concernées ou à l'environnement (article 6-3 de la LMOI).

23. Des mesures opérationnelles d'investigation peuvent être mises en œuvre après réception d'informations selon lesquelles une infraction pénale a été commise, est en train d'être commise ou est en préparation, ou d'informations sur des personnes qui se préparent à commettre une infraction pénale, qui en commettent ou qui en ont commis une, s'il n'y a pas d'éléments suffisants pour justifier l'ouverture d'une procédure pénale (article 7-2 § 1 de la LMOI).

24. Dans son arrêt n° 86-O du 14 juillet 1998, la Cour constitutionnelle a jugé que l'article 7-2 § 1 de la LMOI devait être lu à la lumière de l'article 2 de cette loi. Elle en a déduit que le terme « infraction » figurant à l'article 7-2 § 1 devait être interprété comme signifiant « infraction pénale » et que s'il apparaissait, au cours de l'exécution de mesures opérationnelles d'investigation, que l'infraction visée par une enquête ne revêtait pas la

qualification d'infraction pénale, elles devaient être immédiatement abandonnées.

25. Les organes habilités à mettre en œuvre des mesures opérationnelles d'investigation peuvent procéder à la saisie de documents, d'objets, de pièces et de communications (article 15-1 de la LMOI).

III. LA COLLECTE DE PREUVES DANS LE CADRE DES PROCÉDURES POUR INFRACTION ADMINISTRATIVE

26. Le chapitre 26 du CIA prévoit que dans le cadre d'une affaire portant sur une infraction administrative, des documents, des photographies, des enregistrements audio ou vidéo, des bases de données et d'autres formes de données peuvent être utilisés comme preuves s'ils contiennent des informations pertinentes pour l'affaire en question. La personne chargée de l'affaire, qu'il s'agisse d'un juge ou d'un autre fonctionnaire, doit prendre toutes les mesures nécessaires pour assurer la conservation des éléments de preuve jusqu'à l'issue de l'affaire, puis décider du sort de ces éléments (article 26.7).

27. Le juge ou autre fonctionnaire chargé d'une affaire portant sur une infraction administrative peut demander toute information nécessaire à la résolution de l'affaire. L'information demandée doit lui être communiquée dans un délai de trois jours à compter de la réception de la demande. Si l'information ne peut être communiquée, l'organe auquel elle a été demandée doit en informer par écrit, dans un délai de trois jours, le juge ou autre fonctionnaire à l'origine de la demande (article 26.10).

IV. LES POUVOIRS DES SERVICES DE POLICE

28. En vertu de la loi sur les services de police (loi n° 3-FZ du 7 février 2011), les services de police doivent prendre des mesures aux fins de la recherche et de la répression des infractions administratives relevant de leur compétence et aux fins de la réalisation d'enquêtes sur ces infractions (article 12-1 § 11). Ils doivent également prendre des mesures visant à prévenir, déceler et réprimer les activités à caractère extrémiste (article 12-1 § 16).

29. Lorsqu'ils enquêtent sur des infractions pénales ou administratives ou examinent des plaintes portant sur des infractions pénales ou administratives ou sur des accidents, les services de police sont habilités à obtenir gratuitement, sur demande motivée de leur part, la communication, par les autorités étatiques et municipales, les associations publiques, les organisations, les fonctionnaires et les citoyens, d'informations, de documents, de copies de documents ou de toute autre donnée nécessaire, y compris des données personnelles, à l'exception des informations auxquelles

l'accès est régi par une procédure spéciale en vertu du droit fédéral (article 13-1 § 4).

V. LE TRAITEMENT DES DONNÉES PERSONNELLES

30. Dans sa version en vigueur à l'époque pertinente, la loi n° 152-FZ du 27 juillet 2006 sur la protection des données personnelles autorisait le traitement de données personnelles notamment dans le cadre de la participation d'une personne à une procédure menée devant les juridictions administratives, mais aussi si la personne concernée avait rendu publiques ces données personnelles (article 6 §§ 1, 3 et 10).

31. L'article 11 § 1 de cette loi définissait les données personnelles biométriques comme étant des informations révélant des caractéristiques physiologiques et biologiques d'une personne susceptibles de permettre l'identification de celle-ci. Il précisait que de telles données ne pouvaient être traitées que si la personne concernée y consentait par écrit, sauf dans les cas prévus par l'article 11 § 2. L'article 11 § 2 disposait que ces données pouvaient être traitées sans le consentement de la personne concernée notamment pour les besoins de l'administration de la justice et dans les cas prévus par la législation relative à la défense, à la sécurité, à la lutte contre le terrorisme, à la sécurité des transports, à la lutte contre la corruption ou aux mesures opérationnelles d'investigation (article 11 § 2).

32. L'article 10 § 1 interdisait de manière générale le traitement de catégories particulières de données personnelles, à savoir celles susceptibles de révéler la race, la nationalité, les opinions politiques, les croyances religieuses ou philosophiques, l'état de santé ou la vie intime de la personne concernée, sauf dans les cas les cas prévus par l'article 10 § 2. Les alinéas 2, 6 et 7 de l'article 10 § 2 prévoyaient respectivement que les données personnelles relevant de ces catégories particulières pouvaient faire l'objet d'un traitement entre autres si elles avaient été rendues publiques par la personne concernée, ou pour les besoins de l'administration de la justice ainsi que dans les cas prévus par la législation relative à la défense, à la sécurité, à la lutte contre le terrorisme, à la sécurité des transports, à la lutte contre la corruption, aux mesures opérationnelles d'investigation ou à l'exécution des décisions de justice en matières civile et pénale.

VI. LA VIDÉOSURVEILLANCE DANS LE MÉTRO DE MOSCOU

33. Dans sa version en vigueur à l'époque pertinente, le décret gouvernemental n° 410 du 5 avril 2017 sur les exigences en matière de sécurité des transports imposait l'installation de différents équipements techniques dans les stations de métro, en fonction de leur profil sur le plan de la sécurité. En particulier, les stations de métro de la première catégorie (le

niveau de sécurité le plus élevé) devaient être équipées de systèmes de sécurité des transports propres à assurer :

– l'identification de personnes et véhicules cibles au moyen de systèmes de vidéosurveillance au niveau de points de contrôle situés aux limites de la zone de sécurité et de ses sous-parties ainsi qu'au niveau des parties du réseau du métro essentielles au fonctionnement de celui-ci ;

– la détection et l'identification d'événements cibles au moyen de systèmes de vidéosurveillance à tout moment et à n'importe quel endroit du réseau du métro, notamment dans les sous-parties de la zone auxquelles l'accès n'était pas limité, dans celles auxquelles l'accès était réservé aux personnes munies d'un ticket, et au niveau des parties du réseau essentielles au fonctionnement du métro ;

– la détection de personnes et véhicules cibles au moyen de systèmes de vidéosurveillance à tout moment et à n'importe quel endroit dans les sous-parties « réservées au personnel » du réseau du métro ;

– la détection de personnes et véhicules cibles au moyen de systèmes de vidéosurveillance à un moment précis en un emplacement donné du périmètre de la zone de sécurité ;

– la transmission des données en temps réel ;

– la conservation des données sur des appareils électroniques pendant au moins trente jours ;

– la détection en temps réel des personnes tentant d'accéder au métro sans passer par les points de contrôle situés sur le périmètre de la zone de sécurité et au niveau des parties du réseau du métro essentielles au fonctionnement de celui-ci ;

– l'enregistrement et la transmission en temps réel de données relatives aux membres du personnel et aux usagers qui franchissaient les limites des sous-parties de la zone auxquelles l'accès était réservé aux personnes munies d'un ticket ou des sous-parties « réservées au personnel », ou qui accédaient aux parties du réseau essentielles au fonctionnement du métro (article 6 § 1).

34. Les organes compétents du Service fédéral de sécurité, des services de police et du Service fédéral de supervision des transports devaient avoir accès aux données recueillies par les systèmes de sécurité des transports (article 5 § 10).

LES TEXTES INTERNATIONAUX PERTINENTS

I. LES NATIONS UNIES

35. En ses parties pertinentes, le rapport du 24 juin 2020 de la Haute-Commissaire des Nations unies aux droits de l'homme, intitulé *Incidence des nouvelles technologies sur la promotion et la protection des droits de l'homme dans le contexte des rassemblements, y compris des manifestations*

pacifiques (document des Nations unies A/HRC/44/24) est libellé comme suit (notes de bas de page omises) :

> « 33. L'utilisation de la reconnaissance faciale pour identifier des personnes dans le cadre de rassemblements porte gravement atteinte au droit à la vie privée, à la liberté d'expression et au droit de réunion pacifique lorsqu'elle n'est pas assortie de garanties effectives. L'image d'un individu est l'un des attributs principaux de sa personnalité, du fait qu'elle traduit son originalité et lui permet de se différencier de ses semblables. Enregistrer, analyser et conserver les images faciales d'un individu sans son consentement revient à s'ingérer dans l'exercice de son droit à la vie privée. Lorsque la reconnaissance faciale est utilisée lors de rassemblements, cette immixtion s'opère à grande échelle et de manière non ciblée, vu qu'il s'agit de capturer et de traiter les images faciales de toutes les personnes saisies par une caméra couplée ou connectée à un système de reconnaissance faciale.
>
> 34. Depuis toujours, les rassemblements offrent une certaine protection aux participants contre le risque d'être visés individuellement ou identifiés. Cette protection se trouve déjà considérablement amoindrie du fait d'États, nombreux, qui font systématiquement capturer sur support audiovisuel ceux qui prennent part à des rassemblements. La reconnaissance faciale, qui est en plein essor, marque un basculement de paradigme par rapport à l'enregistrement audiovisuel, en ce qu'elle décuple la capacité d'identifier de manière automatique tous les participants à un rassemblement ou bon nombre d'entre eux. Cela pose particulièrement problème dans le cas de la reconnaissance faciale en direct, qui permet d'identifier en temps réel les participants, ainsi que de les surveiller de manière ciblée et de les localiser. Les identifications erronées ainsi effectuées peuvent entraîner des interventions indues de la part des forces de sécurité dans des rassemblements pacifiques. Les effets négatifs de l'utilisation de la reconnaissance faciale sur le droit de réunion pacifique peuvent être considérables, comme l'ont fait observer plusieurs experts onusiens des droits de l'homme. Nombreuses sont les personnes qui renoncent à manifester dans l'espace public et à exprimer librement leurs opinions, de peur de pouvoir être identifiées et de s'exposer à des conséquences négatives.
>
> 35. Toute technique d'enregistrement audiovisuel ou de reconnaissance faciale ne devrait être employée que si elle satisfait aux critères de légalité, de nécessité et de proportionnalité. D'aucuns doutent que l'utilisation de la reconnaissance faciale lors de manifestations pacifiques puisse répondre aux critères de nécessité et de proportionnalité, vu son caractère intrusif et fortement dissuasif. De manière générale, les pouvoirs publics devraient s'abstenir d'enregistrer les participants aux rassemblements. Conformément à la nécessité de faire preuve de proportionnalité, il ne faudrait envisager de déroger à ce principe que lorsqu'il y a des éléments concrets indiquant que de graves infractions pénales sont de fait en train d'être commises, ou des motifs de soupçonner la manifestation imminente d'un comportement hautement délictueux, notamment par la violence ou l'usage d'armes à feu. Les enregistrements disponibles devraient servir uniquement à identifier les participants à un rassemblement qui sont suspectés d'infractions graves.
>
> 36. L'utilisation de la reconnaissance faciale dans le contexte des rassemblements pacifiques n'est pas recommandée, et les gouvernements qui ont encore recours à cette technique devraient veiller à le faire selon une base légale claire, constituée notamment d'un cadre réglementaire solide, conforme aux droits de l'homme. De plus, les gouvernements qui continuent d'utiliser l'enregistrement audiovisuel et la reconnaissance faciale devraient mettre en place une réglementation assortie de dispositions propres à garantir la protection effective des données à caractère personnel,

y compris des images faciales et des données tirées de celles-ci. Des mesures devraient prévoir la suppression immédiate de toutes les données, à l'exception de celles qui pourraient être indispensables à la conduite d'enquêtes pénales et à l'engagement de poursuites contre les auteurs de faits de délinquance violente. Chacun devrait avoir le droit d'accéder aux données conservées sans raison valable ni base légale, ainsi que d'en demander la rectification et la suppression, sauf si cela ferait obstacle à une enquête pénale ou à une procédure de poursuites tributaire de ces données.

37. En outre, toute utilisation de l'enregistrement audiovisuel ou de la reconnaissance faciale doit être subordonnée à des mécanismes de surveillance robustes et dotés de ressources suffisantes. Cette surveillance peut être assurée en partie par des organismes de protection des données indépendants et impartiaux. Cependant, les États devraient envisager des mesures supplémentaires, notamment l'intervention d'une entité indépendante, de préférence à caractère judiciaire, qui serait chargée d'autoriser le recours à la reconnaissance faciale lors d'un rassemblement. Quoi qu'il en soit, toute utilisation de dispositifs d'enregistrement ou de reconnaissance faciale devrait pouvoir être contestée devant les tribunaux. Les autorités devraient en toutes circonstances faire preuve de transparence concernant l'usage de tels dispositifs et devraient toujours informer les citoyens lorsqu'ils sont ou pourraient être enregistrés ou lorsque leur image pourrait être traitée par un système de reconnaissance faciale.

(...)

53. Compte tenu de ce qui précède, la Haute-Commissaire formule les recommandations ci-après à l'intention des États :

(...)

h) S'abstenir en tout temps d'utiliser la reconnaissance faciale pour identifier les personnes qui participent pacifiquement à un rassemblement ;

i) S'abstenir de faire des enregistrements vidéo des participants aux rassemblements, à moins qu'il n'y ait des éléments concrets indiquant que des participants se livrent ou vont se livrer à des activités criminelles graves et que la loi n'autorise pareils enregistrements, sous réserve des garanties solides qui s'imposent ;

(...) »

II. LE CONSEIL DE L'EUROPE

36. La Recommandation n° R (87) 15 du Comité des Ministres du Conseil de l'Europe aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police (adoptée le 17 septembre 1987) prévoit entre autres ce qui suit :

Principe 2 – Collecte des données

« 2.1. La collecte de données à caractère personnel à des fins de police devrait se limiter à ce qui est nécessaire à la prévention d'un danger concret ou à la répression d'une infraction pénale déterminée. Toute exception à cette disposition devrait faire l'objet d'une législation nationale spécifique.

(...)

2.4 La collecte de données sur des individus pour l'unique motif qu'ils ont telle origine raciale, telles convictions religieuses, tel comportement sexuel ou telles

opinions politiques ou qu'ils appartiennent à tels mouvements ou organisations qui ne sont pas interdits par la loi devrait être prohibée. La collecte de données concernant ces facteurs ne peut être effectuée que si elle est absolument nécessaire pour les besoins d'une enquête déterminée. »

37. Les Lignes directrices sur la reconnaissance faciale (2021) du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) se lisent ainsi (notes de bas de page omises) :

« La reconnaissance faciale est une technologie de traitement automatique d'images numériques contenant les visages de personnes afin de les identifier ou de les authentifier à partir de modèles de visages.

La sensibilité des informations de nature biométrique a été reconnue explicitement avec l'inclusion des données identifiant une personne de façon unique au titre des catégories particulières de données de l'article 6 de la Convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après « Convention 108+ »).

Le contexte du traitement d'images est pertinent pour qualifier la nature sensible des données. Le traitement d'images n'implique pas, en général, un traitement de données sensibles, les images n'étant couvertes par la définition des données biométriques que lorsqu'elles sont traitées par un moyen technologique spécifique permettant l'identification ou l'authentification unique d'un individu.

Ces lignes directrices traitent de l'utilisation des technologies de reconnaissance faciale, y compris les technologies de reconnaissance faciale à la volée (...)

L'intégration de technologies de reconnaissance faciale dans les systèmes de surveillance existants fait courir des risques sérieux aux droits au respect de la vie privée et à la protection des données à caractère personnel, ainsi qu'à d'autres droits fondamentaux puisque leur utilisation n'impose pas toujours que les personnes dont les données biométriques sont ainsi traitées en soient informées ou y coopèrent. C'est le cas par exemple avec la possibilité d'accéder à des images numériques de personnes sur internet.

Afin de prévenir de telles atteintes, les Parties à la Convention 108+ s'assureront que le développement et l'utilisation de la reconnaissance faciale respectent le droit à la vie privée et le droit à la protection des données personnelles, renforçant ainsi les droits de l'homme et les libertés fondamentales par la mise en œuvre des principes consacrés par la convention dans le contexte particulier des technologies de reconnaissance faciale.

(...)

Licéité

Comme le prévoit l'article 6 de la Convention 108+, le traitement de catégories particulières de données, telles que les données biométriques, n'est autorisé que s'il repose sur une base juridique appropriée et si des garanties complémentaires et appropriées sont inscrites dans la loi nationale. Ces garanties doivent être adaptées aux risques encourus et aux intérêts, droits et libertés à protéger.

Dans certaines législations, l'interdiction de ce traitement est une règle et sa mise en œuvre n'est autorisée qu'à titre exceptionnel, dans des cas spécifiques (par exemple, avec le consentement explicite des personnes, pour protéger leurs intérêts vitaux ou

lorsque le traitement est nécessaire en raison d'un intérêt public prépondérant) et sous réserve de garanties correspondant aux risques encourus.

La nécessité d'utiliser des technologies de reconnaissance faciale doit être évaluée en même temps que la proportionnalité à la finalité visée et son impact sur les droits des personnes concernées.

Les différents cas d'utilisation doivent être classés par catégorie et un cadre juridique applicable au traitement de données biométriques par le biais de la reconnaissance faciale devrait être mis en place. Un tel cadre juridique devrait, en fonction de chaque utilisation différente, notamment traiter :

– de l'explication détaillée de l'utilisation spécifique et de la finalité poursuivie ;

– de la fiabilité minimale et de la précision de l'algorithme employé ;

– de la durée de conservation des photos utilisées ;

– de la possibilité de contrôler ces critères ;

– de la traçabilité du processus ;

– des garanties.

Limitation stricte de certaines utilisations par la loi

Le niveau d'intrusion de la reconnaissance faciale et l'atteinte aux droits à la vie privée et à la protection des données qui en découle vont varier en fonction de l'utilisation particulière qui en sera faite et il y aura des cas où la législation nationale devra limiter strictement son utilisation, voire l'interdire complètement, lorsque la décision aura été prise dans le cadre d'un processus démocratique.

Dans les environnements non contrôlés [la notion d'« environnement non contrôlé » couvre les lieux librement accessibles aux personnes, qu'elles peuvent aussi traverser, y compris les espaces publics et quasi publics tels que les centres commerciaux, les hôpitaux ou les écoles], le recours aux technologies de reconnaissance faciale à la volée devrait être soumis à un débat démocratique comprenant la possibilité d'un moratoire en attendant une analyse complète du fait de son caractère intrusif pour la vie privée et la dignité des personnes, associé à un risque d'impact préjudiciable sur d'autres droits de l'homme et libertés fondamentales.

(...)

Intégration des images numériques aux technologies de reconnaissance faciale

Les législateurs et les décideurs veilleront à ce que les images disponibles en format numérique ne puissent pas être traitées pour en extraire des modèles biométriques, ou pour être intégrées dans des systèmes biométriques, afin de reconnaître la personne figurant sur les images numériques, sans base juridique spécifique pour le nouveau traitement lorsque ces images ont été capturées à d'autres fins (à partir de médias sociaux par exemple).

Comme l'extraction de modèles biométriques à partir d'images numériques implique le traitement de données sensibles, il convient de sécuriser la base juridique éventuelle envisagée ci-dessous qui varie selon les secteurs et les situations.

Plus précisément, utiliser des images numériques qui ont été téléchargées à partir d'internet, y compris sur les médias sociaux ou sur des sites de gestion de photos en ligne, ou qui ont été capturées via des caméras de vidéosurveillance, ne peut être

considéré comme licite au seul motif que ces données personnelles ont été rendues manifestement disponibles par les personnes concernées.

(...)

Utilisation des technologies de reconnaissance faciale dans le secteur public

En règle générale, le consentement ne devrait pas être le fondement juridique utilisé pour la reconnaissance faciale effectuée par les autorités publiques compte tenu du déséquilibre des pouvoirs entre les personnes concernées et ces autorités (...)

Législateurs et décideurs doivent fixer des règles spécifiques pour le traitement biométrique par le biais des technologies de reconnaissance faciale pour des finalités d'application de la loi. Elles garantiront que ces utilisations soient absolument nécessaires et proportionnées à ces finalités et prescriront les garanties nécessaires à fournir.

Autorités chargées de l'application de la loi

Le traitement des données biométriques par le biais des technologies de reconnaissance faciale à des fins d'identification dans un environnement contrôlé ou non contrôlé devrait, en règle générale, être limité à des finalités d'application de la loi. Il devrait être effectué uniquement par les autorités compétentes en matière de sécurité.

Les lois peuvent prévoir différents tests de nécessité et de proportionnalité selon que l'objectif est la vérification ou l'identification, compte tenu des risques potentiels pour les droits fondamentaux et pour autant que les images des personnes soient légalement collectées.

Aux fins d'identification, l'absolue nécessité et la proportionnalité doivent être respectées tant dans la création de la base de données (liste de surveillance) que dans le déploiement des technologies de reconnaissance faciale (à la volée) dans un environnement non contrôlé.

Les lois devraient prévoir des paramètres et des critères clairs auxquels les autorités chargées de l'application de la loi devraient adhérer lors de la création de bases de données (listes de surveillance) dans le cadre de finalités d'application de la loi spécifiques, légitimes et explicites (par exemple, soupçon d'infraction grave ou risque pour la sécurité publique).

Compte tenu du caractère intrusif de ces technologies, dans la phase de déploiement de technologies de reconnaissance faciale à la volée dans des environnements non contrôlés, la loi doit garantir que les autorités chargées de l'application de la loi démontrent que divers facteurs, notamment le lieu et le moment du déploiement de ces technologies, justifient l'absolue nécessité et la proportionnalité des utilisations.

(...) »

III. L'UNION EUROPÉENNE

38. La directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre

circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO 2016 L 119, p. 89) prévoit notamment ce qui suit :

Article 10
Traitement portant sur des catégories particulières de données à caractère personnel

« Le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, et le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique [sont] autorisé[s] uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et uniquement :

a) lorsqu'ils sont autorisés par le droit de l'Union ou le droit d'un État membre ;

b) pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique ;

c) lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée. »

39. Les passages pertinents des lignes directrices 05/2022 sur l'utilisation de la technologie de reconnaissance faciale dans le domaine répressif, publiées le 26 avril 2023 par le Comité européen de la protection des données (EDPB), se lisent ainsi[1] (notes de bas de page omises) :

« 36. Le traitement de données biométriques en toutes circonstances constitue une atteinte grave en soi, et ce, quel que soit le résultat, par exemple une concordance positive. Le traitement constitue une atteinte même si le modèle biométrique est immédiatement supprimé après que la comparaison avec une base de données de la police a abouti à un résultat négatif.

(...)

43. L'article 52, paragraphe 1, de la charte fixe l'exigence d'une base juridique spécifique. Elle doit être libellée de manière suffisamment claire pour permettre aux citoyens de savoir précisément à quelles conditions et dans quelles circonstances les autorités sont habilitées à recourir à toute mesure de collecte de données et de surveillance secrète. Elle doit indiquer, avec une clarté raisonnable, la portée et les modalités d'exercice du pouvoir discrétionnaire pertinent conféré aux autorités publiques afin d'assurer aux personnes le niveau minimal de protection garanti par l'état de droit dans une société démocratique. En outre, la licéité exige des garanties suffisantes pour garantir, en particulier, le respect du droit d'une personne au titre de l'article 8 de la charte. Ces principes s'appliquent également au traitement de données à caractère personnel effectué à des fins d'évaluation, d'entraînement et de développement des systèmes de technologie de reconnaissance faciale.

44. Étant donné que les données biométriques, lorsqu'elles sont traitées dans le but d'identifier une personne physique de manière unique, constituent des catégories particulières de données énumérées à l'article 10 de [la directive (UE) 2016/680, citée au paragraphe 38 ci-dessus], les différentes applications de la technologie de

[1] Note du traducteur : traduction française non encore relue par les membres de l'EDPB consultée le 4 juillet 2024 sur le site de l'EDPB.

reconnaissance faciale nécessiteraient, dans la plupart des cas, une loi spécifique décrivant précisément l'application et les conditions de son utilisation. Cette description englobe notamment les types d'infractions et, le cas échéant, le seuil de gravité approprié de ces infractions, afin, entre autres, d'exclure effectivement les infractions mineures.

(...)

51. Selon la jurisprudence constante de la Cour de justice de l'Union européenne, les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire. Il en découle également qu'il n'existe pas de moyens moins intrusifs pour atteindre l'objectif visé. En fonction de celui-ci, il convient de déterminer et d'évaluer minutieusement d'autres solutions possibles, notamment du personnel supplémentaire, des contrôles plus fréquents ou un éclairage public supplémentaire. Les mesures législatives devraient différencier et cibler les personnes couvertes par ces mesures à la lumière de l'objectif poursuivi, par exemple la lutte contre les formes graves de criminalité. Si elles couvrent toutes les personnes d'une manière générale sans une telle différenciation, limitation ou exception, elles accentuent l'atteinte. Il en va de même si le traitement des données porte sur une partie importante de la population.

52. La protection des données à caractère personnel résultant de l'obligation explicite prévue à l'article 8, paragraphe 1, de la charte est particulièrement importante pour le droit au respect de la vie privée consacré à l'article 7 de la charte. La réglementation doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences de sorte que les personnes dont les données ont été traitées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données. Le besoin de telles garanties est d'autant plus grand lorsque des données à caractère personnel font l'objet d'un traitement automatique et lorsqu'il existe un risque important d'accès illicite aux données. En outre, l'autorisation interne ou externe, par exemple judiciaire, du déploiement de la technologie de reconnaissance faciale peut également servir de garanties et peut s'avérer nécessaire dans certains cas d'atteinte grave.

53. Il convient d'adapter les règles prévues à la situation spécifique, par exemple en ce qui concerne la quantité de données traitées, la nature des données et le risque d'accès illicite aux données. Il s'agirait alors de mettre en œuvre des règles qui serviraient, en particulier, à régir la protection et la sécurité des données en question de manière claire et stricte en vue de garantir leur intégrité et leur confidentialité totales.

54. En ce qui concerne la relation entre le responsable du traitement et le sous-traitant, il ne devrait pas être permis à ce dernier de ne tenir compte que de considérations économiques au moment de déterminer le niveau de sécurité à appliquer aux données à caractère personnel, sous peine de compromettre un niveau de protection suffisamment élevé.

55. Un acte de droit doit fixer des conditions de fond et de procédure ainsi que des critères objectifs permettant de déterminer les limites de l'accès accordé aux autorités compétentes aux données et de leur utilisation ultérieure. Aux fins de la prévention, de la détection ou des poursuites pénales, les infractions concernées devraient être considérées comme suffisamment graves pour justifier l'étendue et la gravité de ces atteintes aux droits fondamentaux consacrés, par exemple, par les articles 7 et 8 de la charte.

56. Les données doivent être traitées en garantissant l'applicabilité et l'effet des règles de l'Union en matière de protection des données, en particulier celles prévues à l'article 8 de la charte, qui dispose que le respect des exigences en matière de protection et de sécurité est soumis au contrôle d'une autorité indépendante. Le lieu géographique du traitement peut, dans ce cas, être pertinent.

57. Eu égard aux différentes étapes du traitement des données à caractère personnel, il convient d'établir une distinction entre les catégories de données en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées. La détermination des conditions du traitement, par exemple la détermination de la durée de conservation, doit être fondée sur des critères objectifs en vue de garantir que l'atteinte est limitée à ce qui est strictement nécessaire.

58. L'évaluation de la nécessité et de la proportionnalité doit, en fonction de chaque situation, identifier et examiner toutes les incidences qui relèvent du champ d'application d'autres droits fondamentaux, tels que la dignité humaine au sens de l'article 1er de la charte, la liberté de pensée, de conscience et de religion au sens de l'article 10 de la charte, la liberté d'expression au sens de l'article 11 de la charte ainsi que la liberté de réunion et d'association au sens de l'article 12 de la charte.

59. En outre, il convient d'envisager avec gravité que si les données sont systématiquement traitées à l'insu des personnes concernées, l'idée générale d'une surveillance constante pourrait apparaître. Il peut en résulter des effets dissuasifs sur certains droits fondamentaux concernés, ou sur l'ensemble d'entre eux.

(...)

73. Le traitement ne peut être considéré comme « strictement nécessaire » que si l'ingérence dans la protection des données à caractère personnel et ses restrictions sont limitées à ce qui est absolument nécessaire. L'ajout du terme « strictement » traduit l'intention du législateur de ne traiter des catégories particulières de données que dans des conditions encore plus strictes que les conditions de nécessité (...). Il convient d'interpréter cette exigence comme étant indispensable. Elle limite la marge d'appréciation laissée à l'autorité répressive lors du test de nécessité à un minimum absolu. Conformément à la jurisprudence constante de la Cour de justice de l'Union européenne, la condition de la « stricte nécessité » est également étroitement liée à l'exigence de critères objectifs afin de définir les circonstances et les conditions dans lesquelles le traitement peut être effectué, excluant ainsi tout traitement de nature générale ou systématique.

(...)

104. L'utilisation des technologies de reconnaissance faciale est intrinsèquement liée au traitement de quantités importantes de données à caractère personnel, y compris de catégories particulières de données. Le visage et, plus généralement, les données biométriques sont liés de manière permanente et irrévocable à l'identité d'une personne. Par conséquent, l'utilisation de la reconnaissance faciale a une incidence directe ou indirecte sur un certain nombre de libertés et droits fondamentaux inscrits dans la charte des droits fondamentaux de l'Union européenne, qui peuvent aller au-delà du respect de la vie privée et de la protection des données, comme la dignité humaine, la liberté de circulation, la liberté de réunion, etc. Ce point est particulièrement pertinent dans le domaine de l'application de la loi et de la justice pénale.

105. Le comité européen de la protection des données comprend qu'il est essentiel que les autorités répressives aient à leur disposition les meilleurs outils possible pour identifier rapidement les auteurs d'actes terroristes ou d'autres infractions pénales graves. Toutefois, ces outils devraient être utilisés dans le strict respect du cadre

juridique applicable et uniquement dans les cas où ils satisfont aux exigences de nécessité et de proportionnalité, comme le prévoit l'article 52, paragraphe 1, de la charte. En outre, si les technologies modernes peuvent faire partie de la solution, elles ne constituent en aucun cas une « solution miracle ».

106. Certains cas d'utilisation de la technologie de reconnaissance faciale présentent des risques inacceptables pour les personnes et la société (« lignes rouges »). C'est pourquoi le comité européen de la protection des données et le contrôleur européen de la protection des données ont demandé leur interdiction générale

107. Ainsi, l'identification biométrique des personnes effectuée à distance dans des espaces accessibles au public présente un risque élevé d'intrusion dans la vie privée des personnes et n'a pas sa place dans une société démocratique, étant donné que, par nature, elle se traduit par une surveillance de masse. Dans le même ordre d'idées, le comité européen de la protection des données estime que les systèmes de reconnaissance faciale fondés sur l'IA qui classent les personnes à partir de leurs données biométriques dans des groupes en fonction de l'origine ethnique, du genre, ainsi que des opinions politiques ou de l'orientation sexuelle, ne sont pas compatibles avec la charte. En outre, le comité européen de la protection des données est convaincu que l'utilisation de la reconnaissance faciale ou de technologies similaires pour déduire les émotions d'une personne physique est hautement indésirable et devrait être interdite, éventuellement avec peu d'exceptions dûment justifiées. Le comité européen de la protection des données estime également que le traitement de données à caractère personnel dans un contexte répressif qui s'appuierait sur une base de données alimentée par la collecte de données à caractère personnel à grande échelle et de manière indifférenciée, par exemple en « extrayant » des photographies et des images faciales accessibles en ligne, en particulier celles mises à disposition par l'intermédiaire des réseaux sociaux, ne satisferait pas, en tant que telle, à l'exigence de stricte nécessité prévue par le droit de l'Union. »

IV. AUTRES ÉLÉMENTS PERTINENTS

40. En ses parties pertinentes, le rapport *How the Russian State uses cameras against protesters* (« Comment l'État russe utilise des caméras contre les manifestants »), publié le 17 janvier 2022 par OVD-Info, un projet médiatique indépendant de défense des droits de l'homme, se lit ainsi :

« Des interpellations de manifestants après la fin de l'événement – ce que nous appelons des « interpellations *a posteriori* » – ont déjà eu lieu avant 2021. En 2018, OVD-Info en avait recensé 219, survenues dans 39 régions de Russie ; pour l'essentiel, il s'agissait de mesures isolées : une ou deux personnes étaient interpellées pour un événement donné, jusqu'à dix personnes dans des cas exceptionnels. Les interpellations *a posteriori* ont commencé à être largement utilisées en 2020 (...)

Nous estimons que l'augmentation du nombre d'interpellations *a posteriori* découle des progrès des technologies de surveillance des réseaux sociaux et de reconnaissance faciale (...)

Notre rapport a pour objet l'usage de systèmes de reconnaissance faciale à des fins de restriction de la liberté de réunion. Même si nos recherches portent essentiellement sur Moscou, il s'avère, selon les données dont nous disposons, que ce phénomène s'étend bien au-delà de la capitale (...)

L'usage de technologies de reconnaissance faciale est attesté, en premier lieu, par les interpellations *a posteriori* réalisées à grande échelle et les poursuites visant des

individus qui ne sont pas des personnages publics, ainsi que par les propos tenus par des agents des services de police (...)

Quoique l'usage d'un système de reconnaissance faciale pour l'identification des manifestants ait fait l'objet d'une large couverture médiatique après les manifestations de janvier 2021, cette technologie est rarement mentionnée dans les documents officiels (...)

La rareté, dans les rapports de police, les dossiers d'affaires et les décisions de justice, des éléments prouvant directement l'usage d'une technologie de reconnaissance faciale pourrait indiquer une réticence des services de police et des cours et tribunaux à consigner officiellement cette information. Il existe néanmoins dans certains documents des indices d'un recours à [cette] technologie (...)

Des personnes soupçonnées par les services de police d'avoir participé aux manifestations ont été interpellées sur leur lieu de travail ou forcées de quitter leur salle de classe à l'université ; une personne a été emmenée au beau milieu d'un cours à l'école. On recense des interpellations survenues dans des cafés, dans la rue, dans le métro, sur des quais de gare et dans le train (...)

Les interpellations pratiquées sur des quais, dans des cafés et dans des appartements de location pourraient indiquer que des systèmes de suivi des déplacements dans l'ensemble de la ville sont utilisés contre des participants aux manifestations qui sont persécutés. Les images enregistrées par les caméras de vidéosurveillance placées à l'entrée de bâtiments résidentiels peuvent être utilisées pour les recherches en question (...)

Le fait qu'un procès-verbal d'infraction soit dressé *a posteriori*, et non à la suite de l'interpellation de la personne concernée au cours d'un événement, implique souvent que l'identité de cette personne n'a pas été établie au moment des faits en question (...) En conséquence, les agents des forces de l'ordre doivent expliquer le processus de comparaison par lequel ils ont identifié la personne filmée comme étant celle qu'ils tentent de mettre en cause pour participation à un événement non autorisé.

Ayant examiné les éléments disponibles, OVD-Info est parvenue à la conclusion que les services de police emploient principalement deux méthodes pour ce faire :

1. indiquer que les personnes ont été identifiées au cours de « mesures opérationnelles d'investigation » ;

2. faire établir par l'un de leurs agents un rapport dans lequel celui-ci déclare, sans davantage d'explications, avoir « identifié » telle ou telle personne sur des photos et des vidéos.

Dans aucun de ces deux cas les services de police n'admettent « sur le papier » avoir eu recours de quelque manière que ce soit à une technologie de reconnaissance faciale à des fins de détermination de l'identité d'une personne. Il est possible que les agents des forces de l'ordre préfèrent ne pas laisser de trace écrite de l'usage de la reconnaissance faciale précisément parce que cette pratique relève de la « zone grise » de la législation russe (...)

En même temps, dans de telles affaires, il n'est fait aucune référence à des mesures d'enquête, et aucune réponse n'est apportée à la question de savoir précisément comment on a réussi à identifier telle ou telle personne (...)

Pour identifier les manifestants, des images enregistrées par des caméras de vidéosurveillance (...), des images enregistrées sur le terrain par des agents des forces de l'ordre, des photos et des vidéos provenant d'Internet (chaînes Telegram, discussions

par messagerie instantanée, pages personnelles sur les réseaux sociaux, YouTube) ont été utilisées.

Dans certains cas, des caméras, par exemple celles installées dans l'entrée de bâtiments résidentiels ou dans le métro, ont également été utilisées pour déterminer l'endroit où se trouvait une personne, aux fins de l'ouverture contre celle-ci d'une procédure pour infraction administrative.

Aux fins de l'identification, les services de police utilisent des bases de données où figurent des photos qui proviennent de documents (passeports internes et externes, cartes de sécurité sociale) et des réseaux sociaux (...)

Par rapport à une interpellation au cours d'un événement, les poursuites à retardement pour participation à une manifestation impliquent des difficultés supplémentaires et de graves inconvénients. Elles s'accompagnent entre autres d'une grave atteinte à la vie privée et elles ont aussi une incidence sur d'autres aspects de la vie humaine.

La pratique des interpellations *a posteriori* a une visée clairement punitive, et elle a pour effet d'intimider et de marginaliser les participants potentiels à des rassemblements. Le délai de prescription applicable à l'article 20.2 du code des infractions administratives – la disposition la plus fréquemment invoquée dans les affaires liées à des rassemblements – ayant été porté à un an, les participants aux manifestations demeurent longtemps exposés au risque d'une interpellation. Il a déjà été rapporté que des procès-verbaux avaient été dressés plus de six mois après les événements sur lesquels ils portaient. Enfin, la mise en cause *a posteriori* de la responsabilité administrative des personnes concernées permet aux organes chargés de l'application de la loi de manipuler le calendrier des audiences judiciaires de manière à inventer des raisons d'accuser ces personnes d'infractions « répétées » et « multiples » (partie 8 de l'article 20.2 du code des infractions administratives et article 212.1 du code pénal) sévèrement réprimées (...)

Il arrive que les juridictions saisies de procédures dirigées contre des manifestants approuvent le recours à la reconnaissance faciale en invoquant la protection des intérêts publics. Cependant, le fait que cette technologie ne soit pas utilisée massivement à l'égard des auteurs de nombreuses autres infractions (par exemple les personnes qui traversent la chaussée hors des passages protégés ou les passagers clandestins) révèle que l'objectif principal n'est pas la protection des intérêts publics, mais la persécution de ceux qui s'opposent aux autorités sur le plan politique.

Un certain nombre de questions relatives, d'une part, à la création et au fonctionnement de l'infrastructure nécessaire à l'utilisation d'un système de reconnaissance faciale dans le but de limiter les manifestations (la prise de vues au moyen d'appareils photographiques et de caméras dans la rue, la conservation des données reçues, la constitution de bases de données de photographies de personnes identifiées) et, d'autre part, à l'accès des agents des services de police aux bases de données ainsi qu'à la protection des données personnelles sont insuffisamment réglementées. Cette situation, combinée avec l'absence de transparence quant à l'utilisation de la technologie de reconnaissance faciale et avec l'absence de contrôle public, pourrait conduire à la transformation de cette technologie en un instrument de persécution politique. »

EN DROIT

I. SUR LA COMPÉTENCE DE LA COUR ET SA CORRESPONDANCE AVEC LE GOUVERNEMENT

41. La Cour observe que les faits sur lesquels le requérant fonde ses allégations de violation de la Convention se sont produits avant le 16 septembre 2022, date à laquelle la Fédération de Russie a cessé d'être Partie à la Convention. En conséquence, elle est compétente pour connaître de la présente requête (*Fedotova et autres c. Russie* [GC], nos 40792/10 et 2 autres, §§ 68-73, 17 janvier 2023).

42. L'article 58 de la Convention prévoyant la continuation de la compétence de la Cour, les articles 38, 41 et 46 en particulier, ainsi que les dispositions correspondantes du règlement de la Cour demeurent applicables à la présente requête après le 16 septembre 2022. Le fait que le Gouvernement ait cessé de participer à la procédure ne le délie pas de son devoir de coopérer avec la Cour et n'empêche pas la Cour de poursuivre l'examen des requêtes qui demeurent de sa compétence (*Ukraine et Pays-Bas c. Russie* (déc.) [GC], nos 8019/16 et 2 autres, §§ 435-439, 30 novembre 2022, et *Svetova et autres c. Russie*, no 54714/17, §§ 29-31, 24 janvier 2023). La Cour peut tirer les conclusions qu'elle juge appropriées d'un refus de participation effective à la procédure (article 44C du règlement).

43. La Cour précise qu'elle continue d'utiliser le site Internet sécurisé pour les gouvernements, à la fois comme moyen de communication avec les autorités de la Fédération de Russie (voir l'instruction pratique sur l'envoi électronique sécurisé de documents par le gouvernement, édictée par le président de la Cour au titre de l'article 32 du règlement le 22 septembre 2008, modifiée le 29 septembre 2014 et le 5 juillet 2018) et afin de respecter le caractère contradictoire de la procédure menée devant elle. Ce site demeure sécurisé et accessible aux autorités de l'État défendeur .

II. SUR L'ÉPUISEMENT DES VOIES DE RECOURS INTERNES

44. S'appuyant sur la décision *Chigirinova c. Russie* ((déc.), no 28448/16, 13 décembre 2016), le Gouvernement soutient que le requérant n'a pas épuisé les voies de recours internes, faute d'avoir saisi la Cour suprême d'un pourvoi en cassation.

45. La Cour note que l'affaire *Chigirinova* (décision précitée) portait sur une procédure fondée sur le code de procédure administrative, tandis que la présente affaire concerne une procédure engagée sur le fondement du code des infractions administratives (« le CIA »). La procédure de contrôle juridictionnel/de pourvoi en cassation prévue par le CIA n'est pas un recours effectif à épuiser (*Smadikov c. Russie* (déc.), no 10810/15, § 49,

31 janvier 2017, et *Ecodefence et autres c. Russie*, nos 9988/13 et 60 autres, § 75, 14 juin 2022).

46. L'exception de non-épuisement des voies de recours internes soulevée par le Gouvernement doit donc être rejetée.

III. SUR LA VIOLATION ALLÉGUÉE DE L'ARTICLE 10 DE LA CONVENTION

47. Le requérant allègue que la procédure pour infraction administrative dont il a fait l'objet a porté atteinte à ses droits tels que garantis par les articles 10 et 11 de la Convention. La Cour examinera ce grief sous l'angle de l'article 10 de la Convention, en tenant compte des principes généraux qu'elle a établis sur le terrain de l'article 11 (*Novikova et autres c. Russie*, nos 25501/07 et 4 autres, § 91, 26 avril 2016). L'article 10 de la Convention est libellé comme suit :

> « 1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. Le présent article n'empêche pas les États de soumettre les entreprises de radiodiffusion, de cinéma ou de télévision à un régime d'autorisations.
>
> 2. L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire. »

A. Sur la recevabilité

48. Constatant que ce grief n'est pas manifestement mal fondé ni irrecevable pour un autre motif visé à l'article 35 de la Convention, la Cour le déclare recevable.

B. Sur le fond

49. Le requérant soutient que sa condamnation pour défaut de notification préalable de sa manifestation individuelle était contraire à la loi. Il argue qu'étant constituée d'un seul morceau de carton, la silhouette de M. Kotov ne pouvait être considérée comme un « objet rapidement (dé)montable », et qu'en conséquence il n'était pas tenu d'adresser aux autorités une notification de sa manifestation individuelle. Il déclare qu'en tout état de cause les dispositions légales applicables ne répondaient pas à l'exigence de « qualité de la loi ». Il ajoute que les autorités internes n'ont fait preuve d'aucune tolérance à l'égard de sa manifestation individuelle pacifique, et qu'aucun besoin social impérieux ne justifiait qu'on l'arrêtât plusieurs jours après la

manifestation. Il affirme que les autorités internes n'ont procédé à aucune appréciation des risques que sa manifestation individuelle était susceptible de présenter, et qu'elles n'ont pas vérifié s'il était nécessaire de l'arrêter et de le condamner.

50. Le Gouvernement soutient que le droit interne imposait la notification préalable des événements publics. Il argue que c'est conformément à la loi que le requérant a été condamné pour manquement à cette obligation. Il ajoute que le transfert au poste de police et l'arrestation de l'intéressé étaient eux aussi conformes à la loi.

51. La Cour rappelle que la protection offerte par l'article 10 ne se limite pas aux paroles ou écrits, les idées et les opinions pouvant également être communiquées par des moyens d'expression non verbaux ou par la conduite d'une personne (*Karuyev c. Russie*, n° 4161/13, § 18, 18 janvier 2022). Compte tenu de la nature de la conduite du requérant ainsi que du contexte dans lequel celle-ci s'inscrivait, la Cour considère que, par ses actions, l'intéressé cherchait à exprimer son opinion sur un sujet d'intérêt public, domaine dans lequel l'article 10 § 2 de la Convention ne laisse guère de place aux restrictions à la liberté d'expression.

52. Le transfert du requérant au poste de police, son arrestation administrative et sa condamnation pour infraction administrative s'analysent en une ingérence dans l'exercice par lui de son droit à la liberté d'expression (*Novikova et autres*, précité, § 106).

53. Les principes généraux pertinents ont été résumés dans les arrêts *Novikova et autres* (précité, §§ 190-201) et *Kudrevičius et autres c. Lituanie* ([GC], n° 37553/05, §§ 108-110, 150-151 et 155, CEDH 2015).

54. En ce qui concerne le critère selon lequel l'ingérence doit être « prévue par la loi », la Cour note que la disposition relative aux « objets rapidement (dé)montables » ne comportait aucun critère propre à permettre de prévoir quels types d'objets pouvaient en relever. Eu égard à la nature de la manifestation individuelle du requérant, et étant donné qu'elle ne dispose ni d'explications complémentaires concernant la portée et les modalités de l'application des dispositions pertinentes par les juridictions supérieures russes ni d'une analyse détaillée de l'affaire du requérant par les juridictions internes, la Cour doute que la manière dont les dispositions légales litigieuses ont été appliquées ait été suffisamment prévisible pour satisfaire en l'espèce à l'exigence de qualité de la loi (*Navalnyy c. Russie* [GC], n°s 29580/12 et 4 autres, § 118, 15 novembre 2018).

55. Cela étant, à supposer même que l'ingérence ait été prévue par la loi et qu'elle ait visé les buts légitimes que sont la « défense de l'ordre » et la « protection des droits d'autrui », elle n'était pas « nécessaire dans une société démocratique », pour la raison indiquée ci-après.

56. Le requérant a manifesté individuellement d'une manière incontestablement pacifique et dénuée de tout caractère perturbateur. L'infraction dont il a été jugé coupable consistait simplement en un défaut de

notification aux autorités de sa manifestation individuelle et n'était assortie d'aucune circonstance aggravante telle qu'une entrave à la circulation, des dégâts ou des actes de violence (voir, *a contrario*, *Kudrevičius et autres*, précité, §§ 164-175). Il n'a pas été établi que les actes du requérant eussent perturbé la vie quotidienne et d'autres activités à un degré excédant le niveau de désagrément normal ou inévitable dans ces circonstances. Il n'a pas non plus été allégué que les actes de l'intéressé eussent présenté un quelconque risque pour l'ordre public ou la sécurité des transports. Les autorités n'ont pourtant pas fait preuve du degré de tolérance requis à l'égard de la manifestation individuelle pacifique du requérant. Elles n'ont pas tenu compte des éléments pertinents susmentionnés ni cherché à déterminer si l'usage par le requérant de la silhouette en carton d'une personne brandissant une banderole était une manifestation de ses opinions. La seule considération pertinente à leurs yeux était la nécessité de réprimer une conduite illégale. Or, dans le contexte de l'espèce, cette considération, en l'absence de toute circonstance aggravante, n'est pas suffisante au regard de l'article 10 de la Convention (*Novikova et autres*, précité, § 199). Il s'ensuit que les juridictions internes n'ont pas justifié par des motifs pertinents et suffisants l'ingérence commise dans l'exercice par le requérant de son droit à la liberté d'expression.

57. Partant, il y a eu violation de l'article 10 de la Convention.

IV. SUR LA VIOLATION ALLÉGUÉE DE L'ARTICLE 8 DE LA CONVENTION

58. Le requérant allègue que le traitement appliqué à ses données personnelles – notamment le recours à une technologie de reconnaissance faciale – dans le cadre de la procédure pour infraction administrative dont il a fait l'objet a porté atteinte à son droit au respect de sa vie privée. Il invoque l'article 8 de la Convention, ainsi libellé :

> « 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
>
> 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

A. Sur la recevabilité

59. Constatant que ce grief n'est pas manifestement mal fondé ni irrecevable pour un autre motif visé à l'article 35 de la Convention, la Cour le déclare recevable.

B. Sur le fond

1. Thèses des parties

60. Le requérant soutient qu'il a été filmé par des caméras de vidéosurveillance installées dans le métro de Moscou, qu'il a été identifié au moyen d'une technologie de reconnaissance faciale et qu'il a par la suite été jugé coupable d'une infraction administrative sur la base des éléments ainsi obtenus. Il argue que la collecte, la conservation et l'utilisation de vidéos de lui n'avaient été autorisées par aucune décision de justice. Selon lui, la loi sur les services de police et le décret n° 410, qui constituaient la base légale de l'ingérence, ne répondaient pas à l'exigence de « qualité de la loi » en ce qu'ils étaient trop vagues, qu'ils n'exigeaient pas la délivrance d'une autorisation judiciaire préalable et ne prévoyaient pas la possibilité d'un contrôle juridictionnel *a posteriori*.

61. Le requérant soutient en outre que l'ingérence commise dans l'exercice par lui de son droit au respect de sa vie privée ne visait aucun but légitime et qu'elle n'était pas « nécessaire dans une société démocratique ». Il affirme qu'il a été porté atteinte à sa vie privée au seul motif qu'il avait manifesté individuellement de manière pacifique.

62. Le Gouvernement soutient que le requérant a commis une infraction administrative et que toutes les mesures que les services de police ont adoptées à son égard étaient légales et justifiées. Il affirme que le nom de l'intéressé ne figurait sur aucune liste de personnes recherchées. Il argue en outre que les mesures adoptées à l'égard du requérant avaient toutes une base légale (voir le résumé de la législation qui figure aux paragraphes 33-34 ci-dessus).

63. L'organisation ARTICLE 19, tierce intervenante, soutient que les technologies de reconnaissance faciale doivent être utilisées avec la plus grande prudence et que leur emploi doit s'accompagner de garanties juridiques adéquates. Elle argue que la surveillance biométrique de masse, en particulier lorsqu'elle repose sur des technologies de reconnaissance faciale, représente l'une des plus graves menaces qui soient pour les droits fondamentaux à l'ère du numérique. Selon elle, cette surveillance constitue une menace pour le droit à la vie privée et à l'anonymat et a un fort effet dissuasif sur l'exercice du droit à la liberté d'expression et du droit à la liberté de réunion. Le fait de se savoir surveillées et suivies pourrait dissuader les personnes d'exercer leur droit de manifester et d'exprimer librement leur opinion dans l'espace public.

2. Appréciation de la Cour

a) Quant à l'existence d'une ingérence

i. Les principes généraux

64. La Cour rappelle que la notion de « vie privée » est une notion large, qui ne se prête pas à une définition exhaustive. Cette notion recouvre de multiples aspects de l'identité physique et sociale de la personne. Elle ne se limite pas à un « cercle intime », où chacun peut mener sa vie personnelle sans intervention extérieure, mais englobe également le droit de mener une « vie privée sociale », à savoir la possibilité pour l'individu de nouer et de développer des relations avec ses semblables et le monde extérieur. Elle n'exclut pas les activités qui ont lieu dans un contexte public. Il existe en effet une zone d'interaction entre l'individu et autrui qui, même dans un contexte public, peut relever de la « vie privée » (*López Ribalda et autres c. Espagne* [GC], nos 1874/13 et 8567/13, §§ 87-88, 17 octobre 2019).

65. Le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8. Peu importe que les informations mémorisées soient ou non utilisées par la suite. Toutefois, pour déterminer si les informations à caractère personnel conservées par les autorités font entrer en jeu l'un des aspects de la vie privée précités, la Cour tiendra dûment compte du contexte particulier dans lequel ces informations ont été recueillies et conservées, de la nature des données consignées, de la manière dont elles sont utilisées et traitées et des résultats qui peuvent en être tirés (*S. et Marper c. Royaume-Uni* [GC], nos 30562/04 et 30566/04, § 67, CEDH 2008).

66. Puisqu'à certaines occasions les gens se livrent sciemment ou intentionnellement à des activités qui sont ou peuvent être enregistrées ou rapportées publiquement, ce qu'un individu est raisonnablement en droit d'attendre quant au respect de sa vie privée peut constituer un facteur significatif, quoique pas nécessairement décisif. S'agissant de la surveillance des actions d'un individu au moyen de matériel photo ou vidéo, les organes de la Convention ont ainsi estimé que la surveillance des faits et gestes d'une personne dans un lieu public au moyen d'un dispositif photographique ne mémorisant pas les données visuelles ne constituait pas en elle-même une forme d'ingérence dans la vie privée. En revanche, des considérations tenant à la vie privée peuvent surgir dès lors que des données à caractère personnel, notamment les images d'une personne identifiée, sont recueillies et enregistrées de manière systématique ou permanente. L'image d'un individu est l'un des attributs principaux de sa personnalité, parce qu'elle exprime son originalité et lui permet de se différencier de ses pairs. Le droit de chaque personne à la protection de son image constitue ainsi l'une des conditions essentielles de son épanouissement personnel et présuppose principalement la maîtrise par l'individu de son image. Si pareille maîtrise implique dans la plupart des cas la possibilité pour l'individu de refuser la diffusion de son

image, elle comprend en même temps le droit pour lui de s'opposer à la captation, la conservation et la reproduction de celle-ci par autrui (*López Ribalda et autres*, précité, § 89, avec les références qui y sont citées).

67. La Cour a déjà jugé que la collecte et la conservation par les autorités de données relatives à une personne s'analysent en une atteinte à la vie privée de celle-ci, même lorsque les données recueillies concernent exclusivement ses activités publiques (*Amann c. Suisse* [GC], nº 27798/95, §§ 65-67, CEDH 2000-II, et *Rotaru c. Roumanie* [GC], nº 28341/95, §§ 43-44, CEDH 2000-V), par exemple sa participation à des manifestations contre le gouvernement (*Association « 21 Décembre 1989 » et autres c. Roumanie*, nºs 33810/07 et 18817/08, § 170, 24 mai 2011, et *Catt c. Royaume-Uni*, nº 43514/15, § 93, 24 janvier 2019). Elle a également jugé que les exemples suivants de collecte de données dans un lieu public étaient constitutifs d'une atteinte à la vie privée des personnes concernées : l'enregistrement d'un interrogatoire réalisé dans une zone publique d'un poste de police (*P.G. et J.H. c. Royaume-Uni*, nº 44787/98, §§ 56-60, CEDH 2001-IX), l'enregistrement par des caméras de vidéosurveillance des images qu'elles captaient, dans un lieu public, et la communication subséquente des images enregistrées aux médias (*Peck c. Royaume-Uni*, nº 44647/98, §§ 57-63, CEDH 2003-I), l'enregistrement de séquences vidéo captées dans un commissariat de police et l'utilisation subséquente des séquences enregistrées dans le cadre d'une procédure pénale (*Perry c. Royaume-Uni*, nº 63737/00, §§ 36-43, CEDH 2003-IX (extraits)), la collecte, au moyen d'un récepteur GPS placé dans la voiture d'une personne, de données indiquant le lieu où celle-ci se trouvait et ses déplacements dans l'espace public, ainsi que la conservation de ces données (*Uzun c. Allemagne*, nº 35623/05, §§ 51-53, CEDH 2010 (extraits), et *Ben Faiza c. France*, nº 31446/12, §§ 53-55, 8 février 2018), l'enregistrement du nom d'une personne dans une base de données de la police qui collectait et traitait automatiquement les informations relatives aux déplacements effectués par cette personne par voie ferroviaire ou aérienne (*Shimovolos c. Russie*, nº 30194/09, § 66, 21 juin 2011), ainsi que la vidéosurveillance des amphithéâtres dans une université publique (*Antović et Mirković c. Monténégro*, nº 70838/13, §§ 40-45 et 55, 28 novembre 2017).

ii. Application de ces principes en l'espèce

68. En l'espèce, au cours d'une surveillance de routine d'Internet, les services de police ont découvert des photographies et une vidéo publiées sur une chaîne Telegram publique montrant le requérant en train de manifester individuellement. Ils ont pris des captures d'écran de cette chaîne Telegram, les ont conservées et, selon le requérant, leur ont appliqué une technologie de reconnaissance faciale dans le but de l'identifier. Après avoir constaté que la vidéo avait été filmée dans une station du métro de Moscou, les services de police ont également recueilli les enregistrements vidéo réalisés par les caméras de vidéosurveillance installées dans cette station et dans deux autres

stations par lesquelles l'intéressé était passé. Ils ont pris des captures d'écran de ces enregistrements vidéo, qu'ils ont conservées. Ils auraient aussi, quelques jours plus tard, utilisé les caméras de vidéosurveillance équipées d'un système de reconnaissance faciale à la volée installées dans le métro de Moscou pour localiser le requérant afin de l'arrêter dans le but de l'inculper d'une infraction administrative. Les captures d'écran de la chaîne Telegram et des enregistrements vidéo des caméras de vidéosurveillance ont par la suite été versées au dossier de la procédure pour infraction administrative dirigée contre le requérant (paragraphes 7-15 ci-dessus).

69. Le Gouvernement ne conteste pas que les faits de l'espèce exposés ci-dessus s'analysent en une « ingérence » dans l'exercice par le requérant du droit au respect de la vie privée consacré à l'article 8 de la Convention. Il n'a pas répondu, bien que la Cour l'y eût expressément invité, aux allégations du requérant selon lesquelles la technologie de reconnaissance faciale a été utilisée d'abord pour l'identifier à partir des photographies et de la vidéo publiées sur Telegram puis pour le localiser en vue de l'arrêter alors qu'il effectuait un trajet en métro à Moscou. La Cour a conscience de la difficulté pour le requérant de prouver ses allégations. De fait, au vu des dispositions du droit interne dont elle a connaissance, les services de police n'ont pas l'obligation de consigner dans un procès-verbal l'utilisation qu'ils font des technologies de reconnaissance faciale, ni de donner accès à un tel procès-verbal à la personne concernée, d'office ou à la demande de celle-ci (voir, au paragraphe 40 ci-dessus, la description de la pratique consistant à avoir recours à la technologie de reconnaissance faciale sans en consigner officiellement l'utilisation).

70. En ce qui concerne l'identification du requérant à partir des photographies et de la vidéo qui avaient été publiées sur Telegram, la Cour note que bien que celles-ci ne continssent aucune information propre à permettre l'identification de l'intéressé, il a fallu moins de deux jours pour l'identifier. Dans leur rapport (paragraphe 11 ci-dessus), les services de police n'ont pas indiqué quelles mesures opérationnelles d'investigation avaient été mises en œuvre aux fins de l'identification du requérant. C'est en vain que le requérant a tenté de contester la légalité du recours à des mesures de cette sorte, ses griefs ayant été rejetés par des décisions sommaires (paragraphes 16-17 ci-dessus). Dans ces circonstances, il n'était pas déraisonnable de la part du requérant de supposer qu'une technologie de reconnaissance faciale avait été utilisée dans son affaire. Le Gouvernement ne le nie pas explicitement, et il ne précise pas non plus quelles mesures ont été prises aux fins de l'identification du requérant. Enfin, la Cour prend note des informations publiques faisant état de nombreux cas d'utilisation de technologies de reconnaissance faciale pour l'identification des participants à des manifestations en Russie (paragraphe 40 ci-dessus).

71. De plus, selon le requérant, les services de police ont reconnu avoir eu recours aux caméras de vidéosurveillance équipées d'un système de

reconnaissance faciale à la volée pour procéder à son arrestation alors qu'il effectuait un trajet en métro à Moscou (paragraphe 12 ci-dessus). Le fait que le Gouvernement mentionne, au titre des bases légales applicables, le décret prévoyant l'installation dans le métro de Moscou de caméras de vidéosurveillance propres à permettre de repérer et d'identifier des personnes cibles au moyen de systèmes de vidéosurveillance peut être interprété comme une reconnaissance implicite de l'usage d'une technologie de reconnaissance faciale à la volée dans la présente affaire (paragraphe 33 ci-dessus).

72. Dans ce contexte, et eu égard à la difficulté pour le requérant de prouver ses allégations dès lors que le droit interne n'imposait pas que le recours à une technologie de reconnaissance faciale fît l'objet d'un procès-verbal ou d'une notification officiels, à l'absence de toute autre explication à l'identification rapide du requérant et à la reconnaissance implicite, par le Gouvernement, de l'utilisation d'une technologie de reconnaissance faciale à la volée, la Cour admet, au vu des circonstances particulières de l'espèce, qu'une technologie de reconnaissance faciale a été employée. Or elle a déjà jugé que la conservation, par les services de police, de photographies susceptibles de se voir appliquer des techniques de reconnaissance faciale s'analysait en une ingérence dans l'exercice du droit au respect de la vie privée (*Gaughran c. Royaume-Uni*, n° 45245/15, §§ 69-70, 13 février 2020).

73. La Cour conclut que le traitement des données personnelles du requérant dans le cadre de la procédure pour infraction administrative dirigée contre lui, y compris au moyen d'une technologie de reconnaissance faciale – employée aux fins de l'identification de l'intéressé à partir des photographies et de la vidéo publiées sur Telegram et de sa localisation ultérieure en vue de son arrestation alors qu'il effectuait un trajet en métro à Moscou – s'analyse en une ingérence dans l'exercice par lui de son droit au respect de sa vie privée au sens de l'article 8 § 1 de la Convention.

b) Quant à la justification de l'ingérence

i. Principes généraux

74. La Cour réaffirme qu'une ingérence ne peut se justifier au regard de l'article 8 § 2 que si elle est prévue par la loi, vise un ou plusieurs des buts légitimes énumérés au paragraphe 2 de l'article 8 et est nécessaire, dans une société démocratique, pour atteindre ce ou ces buts (*Roman Zakharov c. Russie* [GC], n° 47143/06, § 227, CEDH 2015).

75. La protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article. La nécessité de disposer de telles garanties se fait d'autant plus sentir lorsqu'il s'agit de protéger les données à caractère

personnel soumises à un traitement automatique, en particulier lorsque ces données sont utilisées à des fins policières (*S. et Marper*, précité, § 103), ce d'autant que la technologie disponible devient de plus en plus sophistiquée (*Catt*, § 114, *Gaughran*, § 86, et *Uzun*, § 61, tous trois précités). La protection offerte par l'article 8 de la Convention serait affaiblie de manière inacceptable si l'usage des techniques scientifiques modernes dans le système de la justice pénale était autorisé à n'importe quel prix et sans une mise en balance attentive des avantages pouvant résulter d'un large recours à ces techniques, d'une part, et des intérêts essentiels s'attachant à la protection de la vie privée, d'autre part (*S. et Marper*, précité, § 112).

76. Les données à caractère personnel révélant les opinions politiques, telles que les informations relatives à la participation d'une personne à des manifestations pacifiques, sont l'une des catégories particulières de données qui appellent une protection accrue (*Catt*, précité, §§ 112 et 123).

77. Dans le contexte de la collecte et du traitement des données personnelles, il est donc essentiel de fixer des règles claires et détaillées régissant la portée et l'application des mesures et imposant un minimum d'exigences concernant, notamment, la durée, le stockage, l'utilisation, l'accès des tiers, les procédures destinées à préserver l'intégrité et la confidentialité des données et les procédures de destruction de celles-ci, de manière à ce que les justiciables disposent de garanties suffisantes contre les risques d'abus et d'arbitraire (*S. et Marper*, précité, § 99, et *P.N. c. Allemagne*, n° 74440/17, § 62, 11 juin 2020).

ii. Application de ces principes en l'espèce

78. La Cour considère qu'en l'espèce les questions de savoir si l'ingérence était prévue par la loi et si elle visait un but légitime ne peuvent être dissociées du point de savoir si elle était « nécessaire dans une société démocratique » (*S. et Marper*, précité, § 99, *Nemtsov c. Russie*, n° 1774/11, § 75, 31 juillet 2014, et *Elvira Dmitriyeva c. Russie*, n°s 60921/17 et 7202/18, § 77, 30 avril 2019). Partant, elle examinera ces questions conjointement ci-dessous.

79. Selon les autorités internes et le Gouvernement, les mesures qui ont été adoptées à l'égard du requérant trouvaient leur base légale dans le CIA, la LMOI, la loi sur les services de police et le décret n° 410.

80. La Cour note tout d'abord que seules les infractions qualifiées de « pénale » par le droit interne pouvaient donner lieu à des mesures opérationnelles d'investigation (paragraphe 24 ci-dessus). Dès lors que l'infraction ici en cause revêtait un caractère administratif, la LMOI ne pouvait servir de base légale aux mesures adoptées dans la présente affaire.

81. Le CIA et la loi sur les services de police conféraient aux services de police des pouvoirs d'enquête sur les infractions administratives et de collecte d'éléments de preuve, y compris des éléments contenant des données personnelles (paragraphes 26-29 ci-dessus). Le décret n° 410 prévoyait

l'installation dans le métro de Moscou de caméras de vidéosurveillance équipées d'un système de reconnaissance faciale à la volée, lesquelles étaient accessibles à la police (paragraphes 33-34 ci-dessus). La Cour admet donc que les mesures adoptées à l'égard du requérant avaient une base légale en droit interne.

82. Pour autant que le requérant allègue que le droit interne ne répondait pas à l'exigence de « qualité de la loi », la Cour considère qu'il est essentiel, dans le contexte de la mise en place de technologies de reconnaissance faciale, que soient établies des règles détaillées régissant la portée et l'application des mesures qui en découlent, ainsi que des garanties solides contre les risques d'abus et d'arbitraire. La nécessité de garanties est d'autant plus forte lorsqu'il est question du recours à une technologie de reconnaissance faciale à la volée.

83. La Cour doute fort que les dispositions du droit interne en vigueur à l'époque des faits répondaient à l'exigence de « qualité de la loi ». Elle note en particulier que celles-ci autorisaient le traitement des données personnelles biométriques notamment « pour les besoins de l'administration de la justice » (paragraphe 31 ci-dessus), texte formulé en termes généraux. Faute pour le Gouvernement d'avoir produit une interprétation authentique de ce texte par la Cour suprême ou par la Cour constitutionnelle ni même un exemple d'interprétation et d'application restrictives de celui-ci par la pratique administrative et judiciaire, force est à la Cour de constater que cette disposition permettait le traitement des données personnelles biométriques, y compris au moyen d'une technologie de reconnaissance faciale, dans le cadre de n'importe quelle procédure judiciaire. Le droit interne ne prévoyait aucune limite quant à la nature des situations susceptibles de donner lieu à l'usage d'une technologie de reconnaissance faciale, aux buts que pouvait viser l'utilisation d'une telle technologie, aux catégories de personnes qui pouvaient en faire l'objet, ni au traitement des données personnelles sensibles. En outre, le Gouvernement n'a mentionné aucune garantie procédurale afférente à l'utilisation des technologies de reconnaissance faciale en Russie, qu'il s'agisse de procédures d'autorisation, de procédures à suivre pour la consultation, l'utilisation et la conservation des données recueillies, d'éventuels mécanismes de contrôle ou de voies de recours.

84. Par ailleurs, la Cour partira de l'hypothèse que les mesures litigieuses visaient le but légitime qu'est la prévention des infractions.

85. Pour la Cour, il est hors de doute que la lutte contre la criminalité, et notamment contre le crime organisé et le terrorisme, qui constitue l'un des défis auxquels les sociétés européennes doivent faire face à l'heure actuelle, dépend dans une large mesure de l'utilisation des techniques scientifiques modernes d'enquête et d'investigation. Néanmoins, tout en reconnaissant le rôle important que jouent ces techniques dans la détection des infractions, la Cour doit délimiter la portée de son examen. La question n'est pas de déterminer si le traitement de données personnelles biométriques au moyen

d'une technologie de reconnaissance faciale en général peut passer pour justifié au regard de la Convention. Le seul point sur lequel la Cour doive se pencher est celui de savoir si le traitement des données personnelles du requérant se justifiait sous l'angle de l'article 8 § 2 de la Convention en l'espèce (comparer avec *S. et Marper*, précité, §§ 105-106).

86. Pour déterminer si le traitement des données personnelles du requérant était « nécessaire dans une société démocratique », la Cour examinera d'abord la gravité de l'atteinte effectivement portée au droit du requérant au respect de sa vie privée (*P.N. c. Allemagne*, précité, §§ 73 et 84). Elle note que les services de police ont recueilli et conservé des images numériques du requérant et qu'elles en ont extrait ses données personnelles biométriques pour les traiter au moyen d'une technologie de reconnaissance faciale, d'abord pour l'identifier à partir des photographies et de la vidéo publiées sur Telegram, puis pour le localiser en vue de l'arrêter alors qu'il effectuait un trajet en métro à Moscou. La Cour considère que les mesures en question étaient particulièrement intrusives, surtout celles qui faisaient appel à une technologie de reconnaissance faciale à la volée (paragraphe 37 ci-dessus). Le niveau de justification exigé pour qu'elles puissent passer pour « nécessaires dans une société démocratique » est donc élevé, et le recours à une technologie de reconnaissance faciale à la volée requiert pour sa part le niveau de justification le plus élevé. Par ailleurs, les données personnelles du requérant ainsi traitées révélaient ses opinions politiques en ce qu'elles contenaient des informations relatives à sa participation à une manifestation pacifique. Partant, elles relevaient de l'une des catégories particulières de données sensibles appelant une protection accrue (paragraphe 76 ci-dessus).

87. Aux fins de de l'appréciation de la « nécessité dans une société démocratique » du traitement de données personnelles dans le contexte d'une enquête, la nature et la gravité des infractions en cause font partie des éléments qui doivent être pris en considération (voir, *mutatis mutandis*, *P.N. c. Allemagne*, précité, § 72). En l'espèce, le droit interne autorisait le traitement de données personnelles biométriques dans le cadre d'enquêtes ou de poursuites relatives à n'importe quelle infraction, quelles que fussent la nature et la gravité de celle-ci.

88. La Cour observe que le requérant a été poursuivi pour une infraction mineure – à savoir la tenue d'une manifestation individuelle sans notification préalable – que le droit interne qualifie d'infraction administrative et non d'infraction pénale. L'intéressé n'a jamais été accusé d'avoir commis au cours de sa manifestation des actes répréhensibles, par exemple une entrave à la circulation, des dégâts ou des actes de violence. Nul n'a jamais prétendu que ses actions eussent présenté un risque quelconque pour l'ordre public ou la sécurité des transports. La Cour a déjà jugé que la procédure pour infraction administrative dirigée contre le requérant avait porté atteinte au droit de celui-ci à la liberté d'expression (paragraphe 57 ci-dessus). Elle considère que le recours à une technologie de reconnaissance faciale, extrêmement intrusive,

aux fins de l'identification et de l'arrestation des participants à des manifestations pacifiques pourrait avoir un effet dissuasif sur l'exercice des droits à la liberté d'expression et à la liberté de réunion.

89. Dans ces conditions, force est à la Cour de constater que le recours à une technologie de reconnaissance faciale pour l'identification du requérant à partir des photographies et de la vidéo publiées sur Telegram – et, *a fortiori*, à une technologie de reconnaissance faciale à la volée pour la localisation de l'intéressé en vue de son arrestation alors qu'il effectuait un trajet en métro à Moscou – ne répondait pas à un « besoin social impérieux ».

90. À la lumière de l'ensemble des considérations qui précèdent, la Cour conclut que l'utilisation d'une technologie de reconnaissance faciale très intrusive dans une situation où le requérant exerçait son droit à la liberté d'expression tel que garanti par la Convention est incompatible avec les idéaux et valeurs d'une société démocratique régie par la prééminence du droit, que la Convention est destinée à sauvegarder et à promouvoir. Le traitement des données personnelles du requérant au moyen d'une technologie de reconnaissance faciale dans le contexte d'une procédure pour infraction administrative – d'abord aux fins de l'identification de l'intéressé à partir des photographies et de la vidéo publiées sur Telegram, puis de sa localisation en vue de son arrestation alors qu'il effectuait un trajet en métro à Moscou – ne saurait être considéré comme « nécessaire dans une société démocratique ».

91. Partant, il y a eu violation de l'article 8 de la Convention.

V. SUR LA VIOLATION ALLÉGUÉE DE L'ARTICLE 6 DE LA CONVENTION

92. Invoquant l'article 6 de la Convention, le requérant se plaint d'un manque d'équité de la procédure pour infraction administrative dirigée contre lui, à raison de l'absence de partie poursuivante dans le cadre de cette procédure. Eu égard aux faits de l'espèce, aux thèses des parties et aux conclusions qu'elle a formulées sous l'angle des articles 8 et 10 de la Convention, la Cour estime qu'il n'y a pas lieu pour elle de statuer séparément sur la recevabilité et le fond du grief formulé sur le terrain de l'article 6 (*Centre de ressources juridiques au nom de Valentin Câmpeanu c. Roumanie* [GC], n° 47848/08, § 156, CEDH 2014).

VI. SUR L'APPLICATION DE L'ARTICLE 41 DE LA CONVENTION

93. Aux termes de l'article 41 de la Convention :

> « Si la Cour déclare qu'il y a eu violation de la Convention ou de ses Protocoles, et si le droit interne de la Haute Partie contractante ne permet d'effacer qu'imparfaitement les conséquences de cette violation, la Cour accorde à la partie lésée, s'il y a lieu, une satisfaction équitable. »

A. Dommage

94. Le requérant demande 15 000 euros (EUR) au titre du dommage moral qu'il dit avoir subi.

95. Le Gouvernement soutient que ces prétentions sont excessives.

96. La Cour octroie au requérant 9 800 EUR pour dommage moral, plus tout montant pouvant être dû à titre d'impôt sur cette somme.

B. Frais et dépens

97. S'appuyant sur les conventions d'honoraires et relevés d'heures de travail produits par ses avocats, le requérant réclame 6 400 EUR au titre des frais et dépens qu'il dit avoir engagés dans le cadre de la procédure menée devant les juridictions internes et de celle menée devant la Cour.

98. Le Gouvernement soutient que les prétentions du requérant au titre des honoraires de ses avocats doivent être rejetées, au motif, selon lui, que les accords de *quota litis* ne sont pas susceptibles d'exécution.

99. Selon la jurisprudence de la Cour, un requérant ne peut obtenir le remboursement de ses frais et dépens que dans la mesure où se trouvent établis leur réalité, leur nécessité et le caractère raisonnable de leur taux. La Cour note que les conventions d'honoraires signées par le requérant ne revêtent pas un caractère conditionnel. Compte tenu des documents en sa possession et des critères susmentionnés, la Cour juge raisonnable d'allouer au requérant la somme de 6 400 EUR, tous frais confondus, plus tout montant pouvant être dû par lui à titre d'impôt sur cette somme.

PAR CES MOTIFS, LA COUR, À L'UNANIMITÉ,

1. *Dit* qu'elle est compétente pour connaître des griefs du requérant, étant donné que ceux-ci portent sur des faits survenus avant le 16 septembre 2022 ;

2. *Déclare* recevables les griefs concernant les violations alléguées du droit au respect de la vie privée et du droit à la liberté d'expression ;

3. *Dit* qu'il y a eu violation de l'article 8 de la Convention ;

4. *Dit* qu'il y a eu violation de l'article 10 de la Convention ;

5. *Dit* qu'il n'y a pas lieu d'examiner séparément le grief formulé sur le terrain de l'article 6 de la Convention ;

6. *Dit*

a) que l'État défendeur doit verser au requérant, dans un délai de trois mois à compter de la date à laquelle l'arrêt sera devenu définitif conformément à l'article 44 § 2 de la Convention, les sommes suivantes, à convertir dans la monnaie de l'État défendeur au taux applicable à la date du règlement :
   i. 9 800 EUR (neuf mille huit cents euros), plus tout montant pouvant être dû à titre d'impôt sur cette somme, pour dommage moral ;
   ii. 6 400 EUR (six mille quatre cents euros), plus tout montant pouvant être dû par le requérant à titre d'impôt sur cette somme, pour frais et dépens ;

b) qu'à compter de l'expiration dudit délai et jusqu'au versement, ces montants seront à majorer d'un intérêt simple à un taux égal à celui de la facilité de prêt marginal de la Banque centrale européenne applicable pendant cette période, augmenté de trois points de pourcentage ;

7. *Rejette* le surplus de la demande de satisfaction équitable.

Fait en anglais, puis communiqué par écrit le 4 juillet 2023, en application de l'article 77 §§ 2 et 3 du règlement.

Milan Blaško Greffier	Pere Pastor Vilanova Président