L'encadrement des technologies de surveillance des foules

Caroline Lequesne

Chapitre 6.
L'encadrement des technologies de surveillance des foules : réflexions sur la démocratie numérique dans l'espace public

Caroline Lequesne[1]

> « Quelles sont les politiques de reconnaissance, les politiques de construction de toutes sortes de taxonomies ? Il y a toujours des jugements de valeur. Quand vous apprenez à une machine à reconnaître des choses, vous lui apprenez aussi toujours à ne pas reconnaître d'autres choses. Une des grandes questions est donc de savoir comment cela se passe en termes de société » (T. Paglen, entretien avec Br. Boucher, artnews net, 11 juin 2018).

Le présent chapitre dresse un bilan de quatre années de recherche sur les terres sinueuses de la surveillance algorithmique. Celles-ci sont vastes et dessinent des paysages très contrastés d'un État de droit à l'autre. Nous retiendrons qu'elles convergent dans une même dynamique de conquête. Des logiciels espions dans les smartphones de nos dirigeants, à la reconnaissance faciale dans le métro de Rio de Janeiro, en passant par l'automatisation de la lutte contre les fraudeurs ou le ciblage de nos pensées intimes à des fins marchandes, la surveillance technologique s'impose aujourd'hui comme l'un des modes d'existence du commun, de l'État à l'éthos capitaliste. Nous nous intéresserons ici, plus spécifiquement, à celle qui colonise l'espace public ou « les espaces accessibles aux publics » pour reprendre la vulgate européenne qui tente de lui conférer un premier cadre : les espaces de partage,

1. Maître de conférences HDR en droit public à l'Université Côte d'Azur.

où l'on fait société pour se distraire, se cultiver, consommer, ou se déplacer indépendamment de la nature intrinsèque des lieux (publique ou privée). La focale se portera sur les technologies répondant à un double critère, cumulatif : celles qui, *matériellement*, mobilisent un réseau de vidéosurveillance ; celles qui, *fonctionnellement*, identifient (de manière catégorielle ou individuelle) les personnes en vue de l'adoption de mesures préventives ou coercitives par les forces de l'ordre. Nous soutenons à ce titre qu'il existe un continuum technologique de la reconnaissance faciale à la reconnaissance émotionnelle ou comportementale, que nous avons qualifié, non sans susciter quelques débats, de « physiognomoniques »[2]. Indépendamment de conflits formels que l'espace de cette réflexion ne parviendrait à résoudre, cette vaste catégorie d'outils est aisément identifiable et invite, au regard de la mécanique commune qu'ils engagent, à une réflexion commune. Force est de constater que la surveillance technologique des foules a suscité, ces trois dernières années, des prises de position fortement polarisées. Une actualité mouvementée y a fortement contribué : les attentats, la pandémie et aujourd'hui un durcissement des oppositions – et les tensions qu'elles suscitent dans nos sociétés – autour des grands enjeux globaux. Une demande sécuritaire accrue en est résultée, se traduisant par des projets (ou expérimentations) tout aussi divers que l'équipement des stades de foot de systèmes de reconnaissance faciale pour prévenir les débordements de supporters violents, l'adoption de la reconnaissance émotionnelle pour repérer les comportements « anormaux » lors des événements sportifs et culturels, l'équipement des transports en commun de logiciels de vidéosurveillance dite « intelligente » contre les pickpockets ou pour assurer la fluidité du trafic. Plus récemment, ont vu le jour des demandes plus « exotiques », mais non moins préoccupantes, nous y reviendrons : l'adoption de systèmes visant à repérer, au départ des traits du visage des individus, les personnes LGBTQIA+, les criminels ou encore les opposants politiques. Empressons-nous de souligner que cette demande globale n'est pas unanime et travaille les corps sociaux de vives oppositions. En Europe, particulièrement, leur accueil est très contrasté : si les forces de l'ordre plaident en faveur d'une large adoption des technologies de surveillance pour faire face à la sophistication supposée grandissante de la criminalité, elle suscite des oppositions fermes de la part des associations et autres organisations non gouvernementales

2. C. Lequesne-Roth (dir.) et J. Keller, « Surveiller les foules – Pour un encadrement des IA physiognomoniques », *Rapport pour l'Observatoire de l'Éthique Publique*, 2023, 92 p.

qui relaient une opinion publique méfiante. De l'autre côté, l'offre n'est pas en reste. L'industrie des technologies de surveillance compose dans une large mesure celle de l'intelligence artificielle, dont les promesses mirobolantes en termes de croissance alimentent la plus vive attention des milieux économiques et politiques. La course à l'équipement et la conquête des terres d'expérimentation – voire déjà de déploiement – ne sont pas étrangères à la course économico-industrielle pour l'IA que mènent en tête la Chine et les États-Unis.

Nos deux premiers rapports sur la question (2020[3], 2021[4]) traduisaient ces lignes de partage que les volontés politiques nationales et européennes ne sont pas parvenues à surmonter. Il ressortait des recensements européens l'existence de nombreuses expérimentations à l'échelon local, concernant en premier lieu la reconnaissance faciale, souvent non pérennisées ou dont les conclusions n'ont pas été pas rendues publiques. Les interviews conduites auprès des principaux acteurs concernés (autorités locales, polices municipales) traduisaient en outre un malaise tenant à l'absence de « mode d'emploi », générant au mieux une insécurité juridique peu propice à l'innovation, au pire une absence totale de transparence quant aux dispositifs adoptés, considérant qu'ils s'inscrivaient dans les marchés d'équipement ordinaires. La démocratisation des débats autour de ces questions, notamment par la voie des « biais » dans l'espace médiatique, a eu raison de cet état de fait. L'adoption d'un système de reconnaissance faciale ou émotionnelle dans les espaces accessibles au public ne saurait en aucune manière être assimilée à l'achat « d'une nouvelle imprimante » pour reprendre la formule d'Élise Degrave. Il est aujourd'hui largement admis que les risques soulevés par l'adoption de ces différents systèmes en termes de libertés fondamentales – et de (cyber)sécurité – invitent à la mobilisation de fondements légaux solides au soutien de leur déploiement (1.). Dressant les constats d'une absence de dispositions idoines aux technologies de surveillance, le législateur européen a entrepris d'y répondre en posant les premiers jalons d'un cadre qui laissera (en toute vraisemblance) de larges marges de mains-d'œuvre nationales ; le législateur français s'en est d'ores et déjà saisi par le truchement d'une loi expérimentale et d'une proposition de loi actuellement en discussion (2.). Nous examinerons ces récentes

3. C. Lequesne-Roth (dir.), « La reconnaissance faciale dans l'espace public – Une cartographie juridique européenne », *Fablex DL4T*, 2020, 128 p.

4. C. Lequesne-Roth, « New Surveillance Technologies in Public Spaces Challenges and Perspectives for European Law at the Example of Facial Recognition », *Report for The Urban Agenda*, European Commission, 2021, 96 p.

initiatives à la lumière des exigences fondamentales de la démocratie technologique qui se dessinent dans la jurisprudence des juridictions supérieures. Nous conclurons en pointant les lacunes, les failles et les espoirs que soulèvent leurs approches.

1. Risques pour l'ordre public et risques pour l'État de droit[5]

Schématiquement, les technologies de surveillance des foules présentent deux types de risques : un premier « technique », lequel, mal maîtrisé, peut par ricochet aisément se mouvoir en risque sécuritaire (1.1.) ; un second type de nature juridique et politique : mal encadrées, les technologies de surveillance peuvent présenter une menace pour l'exercice des droits fondamentaux (1.2.).

1.1. (Cyber)sécurité menacée

Pour être efficace, le déploiement des technologies de surveillance suppose solidité et fiabilité d'un réseau de vidéo-caméras d'une part, une sécurisation des données biométriques de l'autre. Il est également nécessaire que le programme informatique soit suffisamment robuste face aux diverses formes d'attaques dont il peut faire l'objet[6]. En l'absence de garanties suffisantes à ces différents niveaux, les autorités/entités qui recourent à ces outils s'exposent à des risques majeurs susceptibles d'affecter les personnes ciblées par les systèmes, la sécurité publique et dans certains cas la puissance publique.

Premièrement, lorsque les autorités/entités qui utilisent ces systèmes ne disposent pas de systèmes *hardware* capables de capturer des images de qualité optimale, la fiabilité des résultats est d'autant plus incertaine. Dans ce cas, la menace concerne tant les individus ciblés[7] que la sécurité

5. Ces développements reprennent les références du rapport établi pour l'OEP, *Surveiller les foules – Pour un encadrement des IA physiognomoniques*, précédemment cité.

6. Laboratoire d'innovation numérique de la CNIL (LINC), *Dossier : Sécurité des systèmes d'IA*, 2022, en ligne : https://linc.cnil.fr/sites/linc/files/atoms/files/linc_cnil_dossier-securite-systemes-ia.pdf, qui répertorie trois catégories d'attaques des modèles d'intelligence artificielle : les attaques par manipulation, par infection ou par exfiltration. Voy. égal. pour les attaques en temps réel sur les modèles d'intelligence artificielle pour la vision, A. Guesmi, K. N. Khasawneh, N. Abu-Ghazaleh et I. Alouani, « ROOM: Adversarial Machine Learning Attacks Under Real-Time Constraints », *International Joint Conference on Neural Networks (IJCNN)*, 2022, Padoue, pp. 1-10.

7. Et renvoie ainsi à nos précédentes analyses sur les systèmes dysfonctionnels.

publique elle-même : d'une part, des personnes peuvent être injustement ciblées ; de l'autre, en tant que partie prenante du dispositif sécuritaire, elle peut affaiblir la garde des forces humaines, qui nourrissent une confiance dans ces dispositifs.

Deuxièmement, les périphériques informatiques – en l'occurrence, les caméras connectées – constituent des points d'entrée pour des attaques informatiques. Dans son panorama de la cybermenace 2022, l'Agence Française de la Sécurité Informatique (ANSSI) rappelle en effet que ces « équipements connectés en permanence […] fournissent aux attaquants un accès discret et persistant aux réseaux de leurs victimes »[8]. Les conséquences de ces attaques sont potentiellement multiples. Ces équipements exposent les autorités/entités qui les adoptent, comme les personnes concernées par les traitements. Des vols de données biométriques ont déjà été perpétrés en août 2019. Une faille de sécurité dans une base de données utilisée par des banques, des entrepreneurs de la défense et la police métropolitaine britannique a permis d'accéder aux données biométriques de plus d'un million de personnes[9]. La base de données appartenait à la société sud-coréenne Suprema, leader du marché de l'identification biométrique en Europe[10], au Moyen-Orient et sur le continent africain. En 2020, la base de données controversée Clearview AI, constituée de milliards de données biométriques mises au rebut sur les médias sociaux, a également connu une importante faille de sécurité. Le code source et certaines de ses clés privées sont devenus publiquement accessibles, permettant à quiconque d'accéder à la base de données[11]. Des études ont parallèlement démontré que de nombreux systèmes sont vulnérables aux techniques d'usurpation d'identité : des photos, des vidéos, des modèles 3D ou des « *deep fakes* »[12] d'un visage peuvent permettre une usurpation[13]. Des réseaux neuronaux profonds (DNN) peuvent éga-

8. Agence nationale de la sécurité des systèmes d'information (ANSSI), *Panorama de la cybermenace*, 2022, en ligne : www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-001.pdf, p. 10.

9. J. Taylor, « Major breach found in biometrics system used by banks, UK police and defence firms », *The Guardian*, 14 août 2019.

10. La société fournissait notamment l'Allemagne, la Belgique et la Finlande.

11. Z. Whittaker, « Security lapse exposed Clearview AI source code », *TechCrunch*, 16 avril 2020.

12. S. Tariq, S. Jeon et S. S. Woo, *Am I a Real or Fake Celebrity? Measuring Commercial Face Recognition Web APIs under Deepfake Impersonation Attack*, 2 mars 2021.

13. J. K. Khan et D. Upadhyay, « Security issues in face recognition », *5th International Conference – Confluence The Next Generation Information Technology*

lement être trompés par des exemples adverses[14]. Ajoutons plus globalement que le recours à l'intelligence artificielle est fondamentalement vulnérable à certains types d'attaques, ce qui questionne la fiabilité des systèmes[15].

Ces violations sont particulièrement préoccupantes, ces données étant immuables[16]. La Commission nationale de l'informatique et des libertés (CNIL) rappelle en ce sens que « toute compromission peut avoir des conséquences graves sur leur vie quotidienne »[17]. De même, le Conseil de l'Europe considère que « [t]oute faille dans la sécurité des données peut avoir des conséquences particulièrement graves pour les personnes concernées puisqu'une divulgation non autorisée de données sensibles ne peut être corrigée »[18]. Les attaques peuvent enfin engager les rapports entre États, et menacer la souveraineté nationale. Cela se vérifie particulièrement dans l'hypothèse où les autorités exploitent du matériel informatique étranger.

Summit, Inde, Noida, 2014, pp. 719-725. S.V.N.V.S. Sudeep, S. Venkata Kiran, D. Nandan et S. Kumar, « An Overview of Biometrics and Face Spoofing Detection », in A. Kumar et S. Mozar (eds), *ICCCE 2020. Lecture Notes in Electrical Engineering*, X, Springer, 2021.

14. Y. Alparslan, K. Alparslan, J. Keim-Shenk, S. Khade et R. Greenstadt, *Adversarial Attacks on Convolutional Neural Networks in Facial Recognition Domain*, 2021. Voy. aussi : I. Evtimov *et al.*, « What if a facial recognition system is too easy to fool? Is Tricking a Robot Hacking? », *Berkeley Technology Law Journal*, 34, 2019, p. 891.

15. Plusieurs cas d'études ont permis de l'établir. Concernant les plateformes et les enjeux de sécurité : S. Dave *et al.*, « Special Session: Towards an Agile Design Methodology for Efficient, Reliable, and Secure ML Systems », IEEE 40th VLSI Test Symposium (VTS), San Diego, CA, USA, 2022, pp. 1-14 ; les attaques en temps réel sur les modèles d'IA pour la vision : A. Guesmi, K. N. Khasawneh, N. Abu-Ghazaleh et I. Alouani, « ROOM: Adversarial Machine Learning Attacks Under Real-Time Constraints », *op. cit.* ; la vulnérabilité dans le cas de radars intelligents : A. Guesmi et I. Alouani, « Adversarial Attack on Radar-based Environment Perception Systems », arXiv:2211.01112v2 [cs.CR], 28 novembre 2022 ; la vulnérabilité de l'IA dans le cas de conduite autonome : A. Guesmi, M.A. Hanif, I. Alouani et M. Shafique, « APARATE: Adaptive Adversarial Patch for CNN-based MonocularDepth Estimation for Autonomous Navigation », arXiv:2303.01351v1 [cs.CV], 2 mars 2023.

16. « *If a hacker succeeds in seizing the 35,000 points that make up your face and sells it on the darkweb, it will be almost impossible to recover your digital identity* » (D. Dechaux, « La vérité sur les failles de la biométrie faciale », *Challenges*, 23 janvier 2021).

17. CNIL, *Reconnaissance faciale, pour un débat à la hauteur des enjeux*, 2019, en ligne : www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf, p. 10.

18. Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Lignes directrices pour la reconnaissance faciale, 28 janvier 2021, en ligne : https://rm.coe.int/lignes-direectrices-sur-la-reconnaissance-faciale/1680a134f4, p. 12.

Il est ainsi notoire que les matériels informatiques étasunien[19] et chinois[20] comportent des « portes dérobées » facilitant l'espionnage par des puissances étrangères. Cet état des lieux se retrouve, malheureusement, également dans les logiciels fournis sous code exécutable. En dehors de l'accès aux serveurs de l'État, ces portes dérobées peuvent surtout influer les résultats du système de reconnaissance faciale. Elles peuvent injecter ou soustraire des données, et entraîner soit l'identification de fausses menaces, soit la mise à l'écart de menaces réelles. Ainsi, l'utilisation de matériel étranger est susceptible de neutraliser la finalité même des systèmes physiognomoniques pour des fins de sécurité de l'État ou de la lutte contre le terrorisme. Dans la première hypothèse, la pratique démontre l'utilisation des systèmes de reconnaissance faciale pour détecter des agents étrangers[21]. Si les services de renseignement d'États tiers disposent des moyens techniques d'infiltrer les systèmes de reconnaissance faciale déployés par l'État français, ceux-ci peuvent constituer une arme se retournant contre leurs utilisateurs en traquant par exemple des agents français pour déterminer leurs intérêts ou des responsables politiques pour découvrir leur(s) secret(s) et les réemployer à des fins de chantage.

Mentionnons, en dernier lieu, le recours à la sous-traitance privée pour les traitements biométriques. Les ramifications de l'affaire *Clearview AI*[22] ont mis en évidence les risques soulevés par les usages de son logiciel de reconnaissance en termes de souveraineté. Dans le monde entier, de nombreuses polices ont – ou avaient – sollicité ses services qui offraient un accès à l'une des plus vastes bases de données biométriques jamais constituées[23]. L'enquête de l'Organe de contrôle de l'information policière belge, qui fut l'une des plus exhaustives quant aux pratiques policières liées à Clearview, a alerté les autorités belges sur les risques liés à l'extraterritorialité de la société :

19. En 2016, « Processeur x86 d'Intel, un Backdoor secret et intouchable », *GinFO*, en ligne : www.ginjfo.com/actualites/politique-et-economie/processeur-x86-dintel-backdoor-secret-intouchable-20160617, puis de nouveau en 2022 : « Une backdoor cachée dans les derniers processus Intel », *Silicon*, en ligne : www.silicon.fr/une-puce-secrete-dans-les-derniers-processeurs-intel-150663.html.

20. « Huawei à nouveau accusé d'installer des backdoors », *Frandoid*, 2021, en ligne : www.frandroid.com/marques/huawei/1027557_huawei-a-nouveau-accuse-dinstaller-des-backdoors.

21. Voy. la controverse relative aux usages de la reconnaissance faciale en Ukraine, P. Dave et J. Dastin, « Exclusive: Ukraine has started using Clearview AI's facial recognition during war », *Reuters*, 14 mars 2022 ; « Facial Recognition Goes to War », *New York Times*, 7 avril 2022.

22. C. Lequesne-Roth, « Mise en demeure de Clearview AI par la CNIL : les jalons d'un combat pour le droit à l'anonymat », *Dalloz IP/IT*, 2022.

23. *Ibid*. Selon la presse, la police française est également concernée, bien que nous ne disposions pas d'éléments tangibles permettant de l'établir.

> « [L]'utilisateur de l'application Clearview n'exerce aucun contrôle sur le traitement des données biométriques. Les photos et les images sont en effet chargées par le biais d'une URL, de sorte que la disponibilité des photos et des images est entièrement confiée à l'entreprise américaine Clearview. Les photos et les images, y compris le traitement biométrique (le *template* qui contient les données à caractère personnel unique), *sont envoyées en dehors de l'environnement policier* (et en dehors de l'ordre judiciaire de l'UE) et sont ensuite traitées. L'entité de police qui transmet les photos et les images n'a donc (plus) aucune emprise sur le traitement des données biométriques, ni sur la suite du processus de traitement appliqué par le destinataire. Il est donc clair, et dès lors hautement problématique, *que le service de police qui transmet les photos et les images n'a aucune influence notamment sur le délai de conservation des photos et images, ni sur l'usage commercial qui pourrait potentiellement en être fait par Clearview* »[24].

En d'autres termes, la collaboration entretenue par les forces de l'ordre avec certains acteurs du secteur privé génère un risque certain de diffusion et de réutilisation incontrôlées des données à caractère personnel collectées lors d'une tâche régalienne.

L'étude que nous avions conduite en 2021 montrait que la plupart des outils de reconnaissance faciale expérimentés ou déployés dans les espaces accessibles au public étaient européens[25], et qu'un effort de déploiement interne était à l'œuvre[26]. Toutefois, le secteur de la surveillance, très concurrentiel, se déploie activement sur d'autres continents et les sociétés américaines, chinoises ou encore israéliennes sont parmi les plus compétitives : leur offre fait partie des plus performantes du marché. Cela est en partie lié au fait qu'elles disposent d'importants terrains d'expérimentations à la base de la performance des systèmes. Cette force de frappe étrangère, attractive, appelle à prendre les risques de menace étrangère très au sérieux. Outre une dépendance technologique de prérogatives régaliennes à des technologies étrangères, ces risques constituent indéniablement des menaces aux droits et libertés des citoyens.

24. Organe de contrôle de l'information policière, Rapport de contrôle de l'Organe de contrôle de l'information policière relatif à l'utilisation de l'application Clearview AI par la police intégrée, Contrôle thématique, 4 février 2022, en ligne : www.organedecontrole.be/files/DIO21006_Rapport_Contr%C3%B4le_Clearview_F_00050441.pdf.

25. C. Lequesne-Roth, *New Surveillance Technologies in Public Spaces, op. cit.*, p. 39.

26. *Ibid.*

1.2. Libertés fondamentales sous tension

Nos réflexions relatives aux potentielles menaces que les technologies de surveillance présentent pour l'exercice des droits fondamentaux nous ont conduits, au fil des lectures et des échanges, à distinguer deux configurations : l'hypothèse d'une technologie fonctionnelle, c'est-à-dire dépourvue d'erreurs voire « de biais » (bien que cela semble peu probable[27]) et, à l'inverse, l'hypothèse dysfonctionnelle. La seconde a initié et concentre encore aujourd'hui, dans une large mesure, les débats : peut-on prétendre s'inscrire dans un régime de libertés alors que des outils conduisent la police à des arrestations erronées récurrentes ? Il va sans dire que ce point est hautement problématique et la question principalement rhétorique. Toutefois, nous souhaiterions déporter le débat sur l'hypothèse première en ce qu'elle permet de contourner un certain nombre d'arguments industriels consistant à voir dans les projets technologiques la solution à tous problèmes juridico-éthiques. Les développements qui suivent se concentrent aussi sur l'hypothèse où ces technologies « fonctionneraient » techniquement, en remplissant les missions qui ont justifié leur acquisition. Il apparaît que leur usage fait peser une menace sur le droit à la vie privée d'une part, sur les libertés d'expression, de croyance et d'assemblée, notamment au travers du *chilling effect*, d'autre part.

Les juridictions européennes n'ont pas encore eu l'occasion de se prononcer sur la légalité des systèmes de surveillance dans les espaces accessibles au public. La Cour de justice de l'Union européenne a toutefois été saisie de questions ayant trait à la surveillance de masse des citoyens. Dans l'affaire *Tele2 Sverige*, elle a ainsi considéré que la conservation générale et indiscriminée des communications électroniques entraînait une ingérence « particulièrement grave » dans les droits à la vie privée et à la protection des données consacrés par les articles 7 et 8 de la Charte des droits fondamentaux. La surveillance électronique donne à l'individu « le sentiment que sa vie privée fait l'objet d'une surveillance constante »[28]. Elle en conclut ainsi que la conservation générale des données relatives au trafic et à la localisation devait demeurer une exception à la règle[29], et invite les États à limiter la surveillance à ce qui est « strictement nécessaire ».

27. Les biais sont, dans une large mesure, inhérents aux systèmes. Nous envisageons ici l'hypothèse où les bases de données sont plus représentatives et mieux entraînées de sorte à ne pas commettre d'erreurs systématiques sur certains publics cibles.

28. C.J.U.E. (gde ch.), 21 décembre 2016, *Tele2 Sverige AB contre Postoch telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a.*, aff. jtes C-203/15 et C-698/15, ECLI:EU:C:2016:970, § 100.

29. *Ibid*., § 104.

La jurisprudence postérieure n'a pas remis en cause ces principes, mais en a précisé les exceptions. Les ingérences graves doivent être limitées à des crimes graves et des situations présentant une menace sérieuse et présente (ou prévisible) pour la sécurité nationale. La mesure doit en outre être strictement limitée dans le temps et faire l'objet d'un contrôle de la part des autorités compétentes[30]. De surcroît, l'État membre de l'Union européenne ne peut pas invoquer la sécurité nationale, compétence exclusive, pour déroger aux règles fixées dans un domaine de compétence partagée par un règlement européen. Cela signifie donc que l'invocation de la lutte contre le terrorisme ne peut pas déroger au Règlement général sur la protection des données ou à la directive ePrivacy[31].

La Cour européenne des droits de l'homme (Cour eur. D.H.) est parvenue à une conclusion sensiblement similaire concernant l'interception en masse des données de communication (métadonnées)[32] : de solides garanties contre les abus doivent être fournies par la loi de l'État membre[33] par l'inscription d'assurances procédurales[34] et judiciaires[35].

Aussi, même dans l'hypothèse improbable du développement de systèmes fonctionnels, leur déploiement à des fins de surveillance dans les espaces accessibles au public ne pourrait être que restreint au risque de méconnaître les droits à la vie privée. Le recours généralisé à de tels systèmes serait vraisemblablement considéré comme attentatoire aux droits fondamentaux par les juridictions européennes[36].

30. C.J.U.E. (gde ch.), 2 octobre 2018, *Ministerio Fiscal*, aff. C-207/16, ECLI:EU:C:2018:788 ; C.J.U.E. (gde ch.), 6 octobre 2020, *La Quadrature du Net e.a. contre Premier ministre e.a.*, aff. C-511/18, C-512/18 et C-520/18, ECLI:EU:C:2020:6 ; C.J.U.E. (gde ch.), 20 septembre 2022, *V.D. et S.R.*, aff. C-339/20 et C-397/20, ECLI:EU:C:2022:703 ; C.J.U.E. (gde ch.), 20 septembre 2022, *Bundesrepublik Deutschland contre SpaceNet AG et Telekom Deutschland GmbH*, aff. C-793/19 et C-794/19, ECLI:EU:C:2022:702.

31. C.J.U.E. (gde ch.), *La Quadrature du Net e.a. contre Premier ministre e.a.*, préc., rappelé par C.J.U.E. (gde ch.), 2 mars 2021, *H.K. contre Prokuratuur*, aff. C-746/18, ECLI:EU:C:2021:152.

32. Cour eur. D.H. (gde ch.), 25 mai 2021, *Big Brother Watch c. Royaume-Uni*, req. n^{os} 58170/13, 62322/14 et 24960/15, § 424.

33. *Ibid.* Voy. aussi : Cour eur. D.H. (gde ch.), 25 mai 2021, *Centrum för Rättvisa c. Suède*, req. n° 35252/08.

34. En précisant les motifs d'autorisation d'une interception, la procédure d'octroi de cette autorisation, les circonstances d'interception d'un individu, les procédures à suivre pour la sélection/examen et utilisation des éléments interceptés, les précautions pour la communication, la durée de l'interception et de la conservation de ces données.

35. Les procédures et modalités de supervision par une autorité indépendante et les procédures de contrôle indépendant *a posteriori* du respect des garanties.

36. C. Lequesne-Roth, « De la fin de l'anonymat : reconnaissance faciale et droit à la vie privée », *Dalloz IP/IT*, 2021, pp. 308-313.

Utilisées pour surveiller les espaces accessibles au public, les technologies de surveillance peuvent parallèlement entraver l'exercice de la liberté d'expression, de croyance ou d'assemblée. Dès lors que ces libertés sont conventionnellement consacrées, la menace a fait l'objet de plusieurs mises en garde de la part des Nations Unies[37]. Le fait d'être reconnu ou catégorisé dans les espaces accessibles au public expose potentiellement les croyances, appartenances ou oppositions des individus. Rappelons que l'une des fonctionnalités de la reconnaissance faciale est l'identification et le traçage de personnes d'intérêt, susceptibles de troubler la tranquillité publique. Les opposants politiques peuvent, à ce titre, figurer sur les listes. Il s'agit d'une pratique répandue à l'échelon global, l'histoire récente l'illustrant tristement. Mentionnons à ce titre le recours à cette technologie en Afghanistan contre les citoyens ayant collaboré avec les anciennes puissances occupantes[38], en Birmanie contre les Rohingyas[39], à Hong Kong pour réprimer la révolution des parapluies[40], en Inde contre les populations musulmanes[41], en Russie[42] contre les opposants au régime ou à l'encontre des populations ouïgoures en Chine.

37. Conseil des droits de l'homme, *Droit à la liberté de réunion pacifique et à la liberté d'association, Rapport du Rapporteur spécial sur les droits à la liberté de réunion pacifique et à la liberté d'association*, 17 mai 2019, A/HRC/41/41 ; Conseil des droits de l'homme, *Surveillance et droits de l'homme, Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression*, 28 mai 2019, A/HRC/41/35 ; Conseil des droits de l'homme, *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, Rapport de la Haute-Commissaire des Nations Unies aux droits de l'homme*, 24 juin 2020, A/HRC/44/24 ; International Network of Civil Liberties Organizations (INCLO), *Facial Recognition Tech Stories and Rights Harms from around the World*, 2021, pp. 5-8 ; pp. 13-17.

38. Human Rights Watch, *Afghanistan : les systèmes de données biométriques mettent en danger de nombreux Afghans*, 30 mars 2022, en ligne : www.hrw.org/fr/news/2022/03/30/afghanistan-les-systemes-de-donnees-biometriques-mettent-en-danger-de-nombreux.

39. R. Chandran, « They tried to erase us': Rohingya IDs deny citizenship », *Thomson Reuters report*, 18 novembre 2022, en ligne : www.context.news/surveillance/they-tried-to-erase-us-rohingya-ids-deny-citizenship.

40. « In Hong Kong protests, faces become weapons », *New York Times*, 26 juillet 2019.

41. S. Santoshini, « Indian police use facial recognition to persecute Muslims and other marginalized communities », *Coda*, 11 octobre 2022 ; E. Trujilo, « En Inde, la reconnaissance faciale utilisée pour surveiller les manifestants », *BFMTV*, 30 décembre 2019.

42. Human Rights Watch, Russia uses facial recognition to hunt down draft evaders, 27 août 2021, en ligne : www.hrw.org/news/2022/10/26/russia-uses-facial-recognition-hunt-down-draft-evaders.

L'identification de catégories d'individus, sans même établir leur identité civile, peut s'avérer tout aussi menaçante. Le régime iranien recourt ainsi à la vidéosurveillance intelligente pour repérer et sanctionner les femmes qui ne portent pas le hijab[43]. De la même manière, les autorités serbes l'utilisent pour repérer les populations Roms[44]. Demain, ces technologies pourraient, comme elles en font la promesse[45], être mises au service de la pseudo-identification des personnes homosexuelles ou des personnes adeptes d'un culte en se fondant sur leur tenue vestimentaire.

Il est intéressant de relever que l'atteinte opère de deux manières. Dans les cas évoqués, les technologies de surveillance exercent une atteinte directe : l'identification technologique à une appartenance ou de l'organisation d'un rassemblement emporte une immédiate sanction. Dans nos régimes démocratiques, la menace s'exerce également, de manière indirecte, au travers de ce que l'on désigne communément comme le « *chilling effect* »[46]. Celui-ci décrit communément le fait, pour une personne redoutant une sanction juridique ou une atteinte à son intimité, de s'autocensurer ou de ne pas exercer un droit qui lui est légitimement accordé. Pour paraphraser la Cour de justice de l'Union européenne, la technologie exerce dans cette seconde hypothèse « un effet stigmatisant entraînant à son tour un effet dissuasif » des « opposants politiques » à rejoindre ou à soutenir des actions associatives[47].

43. « Iran Says Face Recognition Will ID Women Breaking Hijab Laws », *Wired*, 18 janvier 2023, en ligne : www.wired.com/story/iran-says-face-recognition-will-id-women-breaking-hijab-laws.

44. Amnesty International, *Serbia: Social Card law could harm marginalized members of society – legal opinion*, 28 novembre 2022, en ligne : www.amnesty.org/en/latest/news/2022/11/serbia-social-card-law-could-harm-marginalized-members-of-society-legal-opinion.

45. Y. Wang et M. Kosinski, « Deep Neural Networks Are More Accurate Than Humans at Detecting Sexual Orientation From Facial Images », *J. Personality, & Soc. Psych*., 2018, vol. 114, p. 246 cité par L. Stark et J. Hutson, « Physiognomic Artificial Intelligence », *Fordham Intell. Prop. Media & Ent*., 2022, vol. 32, p. 922.

46. Notons qu'en matière doctrinale, le *chilling effect* a principalement été conceptualisé par la doctrine anglophone. L'article « fondateur » est celui de Fr. Schauer, « Fear, Risk, and the First Amendment: Unraveling, the "Chilling Effect" », *B.U. L. REV.*, 1978, vol. 58, p. 685 cité par Open Society, *The Concept of Chilling Effect*, 2021, en ligne : www.opensocietyfoundations.org/publications/the-concept-of-chilling-effect. On trouve la création de cette notion dans l'arrêt de la Cour eur. D.H., 5 avril 1973, *Donnelly et autres c. Royaume-Uni*. Nous invitons la/le lectrice/lecteur intéressé(e) à consulter la note de bas de page n° 6 de J. W. Penney, « Understanding chilling effects », *Minnesota Law Review*, 2022, vol. 106, pp. 1451 et s., qui fait état d'une bibliographie importante.

47. C.J.U.E. (gde ch.), 18 juin 2020, *Commission c. Hongrie*, aff. C-78/18, EU:C:2020:476. Les commentateurs de cet arrêt soulignent que « les mesures

Certains auteurs ajoutent qu'elle opère un effet de « conformité » ou « d'obéissance anticipée » au mépris des croyances individuelles[48]. L'identification de ce risque induit est corroborée par les enquêtes sociologiques. Deux phénomènes ont été observés : le comportement des individus évolue en présence de caméras[49] et les lieux équipés de caméras sont tendanciellement désertés[50]. À l'inverse, le droit d'aller et venir librement a pour condition celui de s'assurer que les individus puissent le réaliser anonymement[51]. Plusieurs autorités, à l'instar du Contrôleur européen des données[52], de la Commission nationale consultative des droits de l'homme (CNCDH)[53] ou de l'Agence européenne

contestées ne sont pas des exemples singuliers de mauvaise loi, mais plutôt représentatives d'un schéma plus large qui a vu des "autocrates légalistes" utiliser délibérément une réglementation juridique visant à réduire ou à supprimer tout degré de dissidence ou de désaccord dans l'espace public et politique ». P. Bard, J. Grogan et L. Pech, « The Democratic and Pluralist Society and its Enemies: The Court of Justice to the Rescue of Civil Society in the Member States », *Reconnect blog*, 23 juin 2020.

48. M. Buchi, N. Festic et M. Latzer, « The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda », *Big Data society*, 2022, vol. 9, p. 14, spéc. p. 4.

49. B. Knijnenburg, X. Page, P. Wisniewski, H. Richter-Lipford, N. Proferes et J. Romano, *Modern Socio-Technical Perspectives on Privacy*, Cham, Springer, 2022, pp. 459, spéc. p. 245 : « *In the public domain, security cameras cause people to change their behavior when they perceive they are being watched. In public, CCTVs can result in less anti-social behavior and reduce crime. Yet, as smart cameras move into more private spaces, constantly being watched may have a chilling effect on behavior, particularly for those who lack control over the cameras* ».

50. F. Castagnino, « Rendre "intelligentes" les caméras : déplacement du travail des opérateurs de vidéosurveillance et redéfinition du soupçon », 2019, en ligne : www.sciencespo.fr/centre-etudes-europeennes/sites/sciencespo.fr.centre-etudes-europeennes/files/2019_05%20-%20Castagnino.pdf.

51. P. Kelly, Facial recognition technology and the growing power of artificial intelligence – Report of the Standing Committee on Access to Information, Privacy and Ethics pour le compte du parlement canadien, p. 84, spéc. p. 32, sur l'audition de Mme C. Khoo, en ligne : www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/report-6.

52. CEPD, *Vers une nouvelle éthique numérique – Données, dignité et technologie*, avis n° 4/2015, 11 septembre 2015, en ligne : https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_fr.pdf, p. 8 : « *Drones, or semi-autonomous aircraft, currently serve mainly military purposes, but are increasingly used for purposes of surveillance, mapping, transportation, logistics and public security, such as containing wildfires. Photographs, videos and other personal data collected by drones can be exchanged over telecommunications networks. Their use risks serious interference with privacy and a chilling effect on freedom of expression* ».

53. CNCDH, avis sur la proposition de loi relative à la sécurité globale (Ass. plén.), 26 novembre 2020, *J.O.R.F.*, n° 0290 du 1er décembre 2020, texte n° 83.

des droits fondamentaux (FRA)[54], ont ainsi, d'ores et déjà, alerté sur ce risque d'entrave technologique. En tout état de cause, tous insistent sur le fait que les usages présentent un risque de surveillance de masse qui constituerait une atteinte majeure aux libertés. Pour être conformes aux impératifs démocratiques, les régimes d'encadrement devront nécessairement prévoir des usages très restreints, déclinés de l'interdiction ferme au régime de redevabilité renforcée. C'est précisément sur ces questions que planchent aujourd'hui parallèlement le législateur européen et le législateur français.

2. Les premiers jalons d'un encadrement : la dynamique européenne

L'offre, la demande (même contrastée) et les risques : convergence et congruence de facteurs qui invitent le législateur à descendre dans l'arène. Cette entrée en scène ne relève pas, précisons-le, d'une forme de « naturalité » juridique ou de sens de l'histoire, mais bien de la nécessité face à ce que nous analysons comme un défaut de garanties juridiques. En effet, il ressort de nos travaux que la législation en vigueur s'accorde mal aux contextes technologiques. Nous relevons notamment l'inadéquation des fondements légaux pour le déploiement des traitements biométriques à la base de nombre de systèmes de surveillance dans les espaces accessibles au public[55]. L'Union européenne a fait de la réglementation du numérique et son (escompté ou réel) « *Brussel effect* » la marque de fabrique de ses politiques contemporaines. Il n'est dès lors pas surprenant que la Commission fasse figure de pionnière en proposant un premier cadre relatif aux technologies de surveillance[56]. L'*Artificial Intelligence Act*, en discussion depuis le printemps 2021, trace les contours et grandes lignes des usages, et pose une conditionnalité marchande en soumettant les dispositifs à un système de certification (2.1.). Alors que la France s'apprête à accueillir des évènements sportifs et culturels d'ampleur, le législateur français s'est parallèlement saisi, anticipant les interstices européens, de l'aménagement des règles

54. FRA, Facial recognition technology: fundamental rights considerations in the context of law enforcement, 27 novembre 2019, en ligne : https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law.

55. Nous renvoyons notre aimable lecteur à nos précédents développements : C. Lequesne-Roth (dir.) et J. Keller, « Surveiller les foules – Pour un encadrement des IA physiognomoniques », *op. cit*.

56. Voy. le chapitre 3 de l'ouvrage.

de déploiement et autres règles de redevabilité (2.2.). Nous analyserons celle-ci à l'aune de ce que nous appréhendons comme les exigences de la démocratie technologique.

2.1. Les jalons de l'Artificial Intelligence Act (AIA)

À titre liminaire, rappelons que le processus législatif européen est, à l'heure où nous écrivons, toujours en cours. Les débats de ces deux dernières années, jalonnés par des prises de position institutionnelles très marquées – et souvent opposées –, ont assurément fait évoluer les lignes tracées par la proposition initiale. Pour les besoins de la présente démonstration, nous nous appuierons sur cette dernière[57], en signalant les points de cristallisation des débats avant le trilogue sur la base des travaux du Conseil de novembre 2022 et du Parlement européen de mai 2023.

Le premier apport du texte tient dans le périmètre d'exploitation des technologies qu'il établit. Il se concentre prioritairement sur ce qui est désigné comme « systèmes d'identification biométrique à distance ». Ces systèmes doivent permettre l'identification des personnes physiques « sans leur participation active », par la comparaison des données biométriques captées avec celles contenues dans un référentiel donné[58]. L'article 5 interdit, par principe, leur utilisation « "en temps réel" dans des espaces accessibles au public par les autorités répressives ou en leur nom à des fins répressives ». Les exceptions demeurent toutefois nombreuses. D'une part, l'article 5(d) prévoit que le recours à ces systèmes est admis pour :

(i) la recherche ciblée de victimes potentielles spécifiques de la criminalité ;

(ii) la prévention d'une menace spécifique, substantielle et imminente pour la vie ou la sécurité physique des personnes physiques ou la prévention d'une attaque terroriste ;

(iii) la détection, la localisation, l'identification ou les poursuites à l'encontre de l'auteur ou du suspect d'une infraction pénale visée à l'article 2, § 2, de la décision-cadre 2002/584/JAI du Conseil 62 et punissable dans l'État membre concerné d'une

57. Proposition de Règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, COM(2021) 206 final (« AIA » par la suite).

58. Art. 3 (36) de l'AIA.

peine ou d'une mesure de sûreté privatives de liberté d'une durée maximale d'au moins trois ans, déterminées par le droit de cet État membre.

D'autre part, au titre de l'article 5(4), un État membre pourrait décider d'autoriser totalement ou partiellement l'utilisation de ces systèmes dans les espaces accessibles au public à des fins répressives. Dans ces hypothèses, le législateur devra préciser les conditions de déploiement des systèmes et les garanties qui l'entourent.

Il est intéressant d'observer que l'interdiction établie par principe a fait l'objet d'une très vive médiatisation dès lors qu'elle conduit à catégoriser cet usage de la reconnaissance faciale – en temps réel dans les espaces accessibles au public – au rang d'IA « inacceptable ». Le Parlement européen s'est particulièrement fait l'écho de cette position. Pour autant, l'étude de ses aménagements met en exergue une bien faible digue face à son déploiement : les exceptions sont si larges, qu'elle ne contient nullement son déploiement à des fins sécuritaires. L'exception nationale opère en outre un renvoi de balle substantiel aux législateurs nationaux, dont la France a su parfaitement se saisir comme nous l'étudierons ci-après.

Parallèlement, l'AIA définit les « systèmes de reconnaissance des émotions », comme « système d'IA permettant la reconnaissance ou la déduction des émotions ou des intentions de personnes physiques sur la base de leurs données biométriques »[59]. Il se réfère également aux systèmes de « catégorisation biométrique » destinés à « affecter des personnes physiques à des catégories spécifiques sur la base de leurs données biométriques »[60] ; la proposition initiale mentionnait, au titre des catégories, « le sexe, l'âge, la couleur des cheveux, la couleur des yeux, les tatouages, l'origine ethnique ou l'orientation sexuelle ou politique ». Ces systèmes sont également susceptibles de composer l'arsenal de surveillance des foules en ce qu'ils font écho aux dispositifs de vidéo-surveillance dite intelligente, lesquelles promettent d'identifier les comportements « anormaux »[61]. Aux termes de l'AIA, ils sont considérés comme des systèmes dits « à haut risque », à savoir des systèmes autorisés sous réserve du respect d'un certain nombre d'obligations.

59. Art. 3(34) de l'AIA.
60. Art. 3(35) de l'AIA.
61. Précisons toutefois que le déploiement de technologies de surveillance sur la base d'une telle catégorisation paraît totalement contraire à nos droits fondamentaux, et inconcevable dans un régime démocratique.

Celles-ci sont à la fois d'ordre industriel et fonctionnel. Mentionnons, de manière non exhaustive, trois d'entre elles qui façonneront tout particulièrement l'économie générale du déploiement.

Premièrement, l'AIA établit en son article 13, § 3 (ii) une obligation de transparence du fournisseur du système sur « le niveau d'exactitude, de robustesse et de cybersécurité ». Ce dernier élément est plus précisément décrit à l'article 15, qui prévoit que l'IA doit faire l'objet d'une sécurité informatique renforcée, dès la conception et par défaut, en fonction de sa fonction. Le premier paragraphe précise que cette exigence doit être maintenue pendant toute la durée d'utilisation de l'IA. Ce même article prévoit un paragraphe spécifiquement dédié aux attaques de tiers en imposant une équivalence entre les circonstances dans lequel s'inscrivent le système d'IA et les mesures de sécurité requises. Enfin, dans l'hypothèse où l'IA continue son apprentissage pendant son déploiement, le fournisseur devra prévoir les moyens de prévention sur l'empoisonnement de données[62] pour éviter, par exemple, la création de discrimination algorithmique. Il est intéressant de relever que les prescriptions de l'AIA sont plus techniques que le RGPD ; ces garanties offriraient ainsi un niveau de sécurité accru par rapport au niveau actuel offert.

Deuxièmement, l'AIA consacre à l'article 14 l'obligation d'un contrôle humain, qui rejoint, comme nous le verrons, les exigences constitutionnelles françaises. Ce contrôle visera à « prévenir ou à réduire au minimum les risques pour la santé, la sécurité ou les droits fondamentaux qui peuvent apparaître lorsqu'un système d'IA à haut risque est utilisé conformément à sa destination ou dans des conditions de mauvaise utilisation raisonnablement prévisible, en particulier lorsque de tels risques persistent ». Le texte prévoit à cet égard deux garanties essentielles. D'une part, l'exigence d'un contrôle « effectif », « par des personnes physiques », pendant la période d'utilisation d'un système d'IA à haut risque. Ce contrôle doit permettre de s'assurer de son adéquate destination, voire de le reconfigurer en cas de mauvaise utilisation voire de l'arrêter. D'autre part, l'exigence d'un niveau de compétence suffisant pour assurer ce contrôle. En effet, les « personnes chargées d'effectuer un contrôle humain » devront être capables « d'appréhender totalement les capacités et les limites du système d'IA », « d'avoir conscience d'une éventuelle tendance à se fier automatiquement ou excessivement

62. C'est-à-dire la « manipulation (du) jeu de données d'entraînement » (voy. art. 15, § 6 du Règlement général sur la protection des données).

aux résultats produits », « d'interpréter correctement les résultats du système d'IA » et « de décider, dans une situation particulière, de ne pas utiliser le système d'IA à haut risque ». Le texte prévoit en outre, pour les systèmes d'identification biométrique à distance, qu'aucune mesure ou décision ne pourra être prise par l'utilisateur « sur la base de l'identification résultant du système sans vérification et confirmation par au moins deux personnes physiques ».

Enfin, le texte met en place un système de certification. La procédure de mise en conformité des systèmes prévue à l'article 43-1 de l'AIA – dont relèveraient les systèmes d'identification faciale compris comme « systèmes à haut risque » – sera(it) dans une large mesure dévolue à des organismes de normalisation et de certification. Il appartiendra(it) à ces derniers d'établir la méthodologie et les normes d'évaluation. Le modèle privilégié confère(rait) un rôle d'importance majeure à des acteurs privés tant dans l'accès au marché que dans le respect des normes de conformité et par suite de l'État de droit.

Il apparaît ainsi que le texte européen offre un fondement légal relativement large à l'instauration des technologies de surveillance des foules dans les espaces accessibles au public. Leur déploiement est subordonné à des exigences de marché d'une part, qui procède d'un modèle corégulatoire conférant un rôle décisif aux organismes de normalisation et de certification ; à des exigences fonctionnelles de transparence et d'intervention humaine d'autre part, qui requièrent encore une « opérationnalisation » pour être effectives. L'aménagement des « modes d'emploi » nationaux apparaît à cet égard décisif.

2.2. Exceptions et redevabilité : exemple du mode d'emploi « à la française »

En Europe, la France fait figure de pionnière concernant la régulation des technologies de surveillance dans les espaces accessibles au public. Après la loi n° 2022-52 du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure encadrant l'usage des drones, la loi n° 2023-380 du 19 mai 2023 relative aux Jeux Olympiques et Paralympiques de 2024 (ci-après dite loi JO 2024), autorisant la vidéo-surveillance dite intelligente, une proposition de loi relative à la reconnaissance biométrique dans l'espace public est actuellement en débat au Parlement. Ces textes décrivent une approche incrémentale de la part du législateur français, qui a progressivement élargi le spectre technologique de la surveillance. On relève ainsi que l'identification

biométrique, fermement exclue des deux premiers textes, est aujourd'hui largement envisagée dans le dernier, qui propose d'en autoriser l'usage pour « des motifs d'une exceptionnelle gravité ». Autre manifestation de cette méthode, le caractère expérimental de deux des textes qui mettent (ou invitent à le faire pour la dernière proposition) un dispositif visant à « tester » la technologie sur une période donnée. Une « prudence » politique qui n'en cache pas moins une volonté ferme et une dynamique d'adoption relativement claire.

D'un point de vue technique, ces textes sont riches d'enseignement à deux égards : d'une part, l'adoption des premiers a permis au Conseil constitutionnel d'exprimer des exigences constitutionnelles en la matière ; de l'autre, ils offrent un premier effort d'opérationnalisation de ces exigences. Nous verrons que la jurisprudence, comme son modèle opératoire, ne va pas sans soulever quelques interrogations au regard des lacunes et contradictions qu'ils laissent apparaître.

En amont des décisions propres à la surveillance technologique des foules, il est intéressant de lire la position du Conseil constitutionnel concernant plus largement la surveillance, plus étroitement l'encadrement des traitements automatisés auxquels l'administration française recourt. Ce recueil jurisprudentiel établit les jalons de positions non démenties, dans la veine desquels s'inscrivent les décisions qui intéressent plus spécifiquement notre propos. L'analyse jurisprudentielle intéressant les lois sécuritaires post-11 septembre – de la lutte contre le terrorisme aux pouvoirs de police administrative – laisse entrevoir ce que Karine Roudier décrit comme « la mise à l'écart » du Conseil constitutionnel, ou le mouvement d'une Haute juridiction poussant au « point de rupture », « à son stade maximal », « la souplesse de la norme constitutionnelle »[63] . Elle relève ainsi qu'en dépit d'atteintes préoccupantes, la conciliation entre ordre public et droit au respect de la vie privée est « quasi systématiquement » jugée proportionnée. Il apparaît en outre que le Conseil a admis la constitutionnalité de la surveillance non individualisée de « groupes de personnes », d'organisations, de « zones géographiques »[64], ou l'extension du traitement des données de connexion dans le cadre de procédures de réquisition administrative[65], que la Cour de justice de l'Union européenne avait par ailleurs

63. Cons. const., déc. n° 2015-713 DC, 24 juillet 2015, cons. 10.

64. Légalisé par l'article 1er de la loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales, *J.O.R.F.*, n° 0278, 1er décembre 2015, p. 22185.

65. Cons. const., déc. n° 2015-478 QPC, 24 juillet 2015, cons. 17.

qualifiée d'« ingérence particulièrement grave »[66]. Cette position a en outre été confortée par la décision ayant avalisé la surveillance de masse sur les réseaux sociaux par l'administration fiscale[67]. Concernant les traitements automatisés n'impliquant pas nécessairement surveillance, le Conseil constitutionnel ne s'est pas davantage illustré dans l'opposition qu'il aurait pu incarner au mouvement législatif. Dans sa décision du 12 juin 2018, alors qu'il était appelé à s'interroger sur l'existence d'une potentielle délégation de l'homme à la machine dans le cadre des décisions administratives automatisées, il conclut que celle-ci faisait défaut eu égard aux garanties humaine et juridique établies par le législateur. L'élargissement du spectre des décisions automatisées ne contrevenait pas, selon lui, à l'article 21 de la constitution française dès lors qu'un humain était « dans la boucle », même *a posteriori* par la voie du juge[68].

La décision concernant la loi relative aux JO 2024[69] reflète ce double héritage. La conciliation entre droit au respect de la vie privée et ordre public, contestée par les requérants, est jugée satisfaisante[70] au regard des garanties législatives apportées. Le système de surveillance que la loi permet d'établir ne soulève pas d'opposition de principe particulière. En outre, le Conseil valide en creux le mode opératoire défini au titre des garanties : la mobilisation doit répondre aux critères de nécessité (« risques particuliers d'atteintes graves à l'ordre public » à l'exclusion des risques d'atteinte aux biens[71]) et de proportionnalité[72]. Notons que ce même critère de proportionnalité a conduit le Conseil à exclure l'usage des drones par les polices municipales, usage qui doit en outre répondre au critère de subsidiarité[73]. Dans le cadre de la loi d'expérimentation pour les JO 2024, ces premières exigences sont jugées satisfaites dès lors que l'autorisation préfectorale est motivée et qu'elle indique à ce titre : le responsable du traitement, les motifs de sa mise en œuvre, le périmètre géographique et la durée de l'autorisation. Celle-ci peut faire l'objet d'un recours administratif notamment devant le juge des référés positionné comme contre-pouvoirs. Le Conseil rappelle qu'il peut en effet « suspendre l'exécution de la mesure ou ordonner toutes mesures

66. C.J.U.E. (gde ch.), 8 avril 2014, *Digital Rights Ireland et Seitlinger e.a.*, aff. C-293/12 et C-594/12, ECLI:EU:C:2014:238, pt 27.
67. Cons. const., déc. n° 2019-796 DC, 27 décembre 2019.
68. Cons. const., déc. n° 2018-765 DC, 12 juin 2018.
69. Cons. const., déc. n° 2023-850 DC, 17 mai 2023.
70. À une réserve près, concernant l'autorisation préfectorale ; *ibid.*, cons. 39.
71. *Ibid.*, cons. 37.
72. *Ibid.*, cons. 38.
73. Cons. const., déc. n° 2021-834 DC, 20 janvier 2022, cons. 27.

nécessaires à la sauvegarde d'une liberté fondamentale ». Le Conseil admet, de la même manière, que la liste des événements prédéterminés justifiant la mobilisation des technologies puisse être établie par décret pris après avis de la Commission nationale de l'informatique et des libertés « sous le contrôle du juge ». Se joue, dans ces deux dispositions, la « garantie juridique » que le Conseil évoquait dès 2018 : celle du recours au juge. Parmi les autres exigences, l'information préalable du public est organisée « par tout moyen approprié », en sus d'une information « générale du public sur l'emploi de traitements algorithmiques sur les images collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs » par le ministre de l'Intérieur. Les dernières exigences relèvent de la garantie humaine. Le Conseil rappelle, d'une part, que « les traitements ne peuvent fonder, par eux-mêmes, aucune décision individuelle ni aucun acte de poursuite et demeurent en permanence sous le contrôle des personnes chargées de leur mise en œuvre »[74] ; de l'autre, que « les traitements algorithmiques employés doivent […] comporter des mesures de contrôle humain et un système de gestion des risques de nature à prévenir et à corriger la survenue de biais éventuels ou de mauvaises utilisations »[75]. Il souligne également l'importance de contrôles permettant *a priori* d'établir « l'objectivité des critères retenus et la nature des données traitées ». Il en conclut alors que « le législateur a veillé à ce que le développement, la mise en œuvre et les éventuelles évolutions des traitements algorithmiques demeurent en permanence sous le contrôle et la maîtrise de personnes humaines »[76].

Le protocole de déploiement des technologies de surveillance dans les espaces accessibles au public dessine ainsi en France, selon le législateur et conformément aux exigences constitutionnelles, un modèle à quatre faces : il est motivé par des circonstances exceptionnelles et est proportionné aux finalités poursuivies (1) ; présente des garanties juridiques par la voie des recours juridictionnels ouverts à l'encontre des décisions administratives le fondant (2) ; assure une information éclairée du public (3) et un contrôle humain, en amont comme en aval des usages (4).

Ces garanties, bien qu'essentielles, sont relativement modestes, notamment sur le terrain de la redevabilité algorithmique. Les exigences en termes de motivations demeurent tout d'abord très larges. Rien ne semble faire expressément obstacle, par exemple, à une surveillance

74. Cons. const., déc. n° 2023-850 DC, 17 mai 2023, cons. 43.
75. *Ibid.*, cons. 44.
76. *Ibid.*, cons. 45.

policière politique dès lors que des manifestations troubleraient l'ordre public. Il est par ailleurs regrettable que le seul contre-pouvoir soit le juge. Outre le caractère approprié du temps judiciaire et des moyens pour répondre à ce contentieux, on peut en effet s'interroger sur la faiblesse des pouvoirs de l'autorité de protection des données dont les avis ne sont ici pas contraignants. Au regard des risques identifiés, il est surprenant que le régime d'autorisation préalable par cette dernière n'ait pas été réintroduit. Soulignons encore la faiblesse des exigences posées concernant la garantie humaine. L'approche du Conseil constitutionnel se dévoile en forme de vœux pieux désincarnés. Que signifie *concrètement* un déploiement « sous contrôle » ? Qu'impose la qualité de « personne en charge » ? Quel(s) contrôle(s) *a posteriori* pour assurer l'effectivité de ces garanties ? Autant de questions qui seront déterminées, sous l'empire de la loi JO 2024, dans les décrets d'application et décisions d'autorisation sans que le Conseil n'y voie une incompétence négative de la part du législateur. Un nouveau point contestable quand l'on sait combien ces usages conditionneront l'exercice des droits fondamentaux. Le régime appellera de surcroît à l'adoption de garanties complémentaires s'il couvre plus largement les dispositifs de surveillance biométriques.

Il semblerait en effet que la biométrie suscite des positions plus prudentes de la part du Conseil constitutionnel. Rappelons qu'en 2012, la Haute juridiction avait censuré la loi instaurant une carte d'identité électronique au motif que certaines de ses dispositions portaient « au droit au respect de la vie privée une atteinte qui ne p[ouvait] être regardée comme proportionnée au but poursuivi »[77]. Bien qu'il ait admis en 2019 la constitutionnalité du recueil des données biométriques pour le fichage des mineurs étrangers non accompagnés[78], ses récentes décisions semblent mettre en cause une inflexion effective. Dans la décision portant sur la loi relative à la responsabilité pénale et à la sécurité intérieure déjà mentionnée, il indique que le recours aux drones par les services de l'État dans le cadre des missions de police judiciaire est jugé conforme à la Constitution, sous réserve du non-recours à la reconnaissance faciale : « [C]es dispositions ne sauraient, sans méconnaître le droit au respect de la vie privée, être interprétées comme autorisant les services compétents à procéder à l'analyse des images au moyen d'autres systèmes automatisés de reconnaissance faciale qui ne seraient

77. Cons. const., déc. n° 2012-652 DC, 22 mars 2012, cons. 11.
78. Cons. const., déc. n° 2019-797 QPC, 26 juillet 2019.

pas placés sur ces dispositifs aéroportés »[79]. De même, la décision concernant la loi relative aux JO 2024 subordonne la constitutionnalité de la loi au non-recours aux « techniques de reconnaissance faciale » ou aux « systèmes d'identification biométrique » ou l'usage de données biométriques[80]. Il apparaît aussi que la surveillance « biométrique » des foules s'inscrit dans un autre palier de surveillance, présentant un degré d'atteinte à la vie privée accru. Est-il pour autant indépassable ? Les précédents ont montré que non, mais tendent à indiquer que le niveau d'exigences sera proportionnellement renforcé. Or, la proposition de loi sur la surveillance biométrique déposée au Sénat ne semble pas établir de mesures de contrôle accru.

Aussi, les premiers éléments des protocoles de déploiement des technologies de surveillance sont encore très élémentaires. Premièrement, les modes d'emploi permettant le recours à la reconnaissance faciale pour la surveillance d'événements, plébiscitée par les sénateurs français, restent à inventer. Deuxièmement, bien que les expérimentations vaillent souvent aval, elles appellent à une évaluation *ex post* qui peut encore faire évoluer les lignes et mettre à jour les lacunes démocratiques mentionnées. Formons de nos vœux qu'elles soient l'occasion de renforcer le régime de redevabilité algorithmique. Enfin, comment imaginer une démocratie technologique sans assentiment citoyen ? Le grand débat n'a, à ce jour, pas eu lieu alors même qu'il engage un véritable choix de société : peut-on, veut-on, doit-on, et jusqu'où, concéder à l'argument sécuritaire nos libertés dont l'exercice requiert la garantie d'un certain degré anonymat dans les espaces du commun ? La nécessité de ce débat ne suscite pas l'unanimité, mais il nous semble indispensable, si ce n'est à la démocratie, à l'acceptabilité sociale de ces technologies sans laquelle elles seront inefficaces parce que détournées, brisées et génératrices *in fine* de tensions sociales. Qu'il nous soit ainsi permis de conclure que le cadre de la démocratie technologique dans les espaces accessibles au public en est encore à ses timides balbutiements.

79. Cons. const., déc. n° 2021-834 DC, 20 janvier 2022, cons. 30.
80. Cons. const., déc. n° 2023-850 DC, 17 mai 2023, cons. 42.