L'instauration d'une "technopolice" administrative en milieu urbain : les droits et libertés sur un fil

Robin Medard Inghilterra

La Revue des droits de l'homme
Revue du Centre de recherches et d'études sur les droits fondamentaux

26 | 2024
Revue des droits de l'homme - N°26

L'instauration d'une « technopolice » administrative en milieu urbain : les droits et libertés sur un fil

Robin Medard Inghilterra

Electronic version
URL: https://journals.openedition.org/revdh/20912
ISSN: 2264-119X

Publisher
Centre de recherches et d'études sur les droits fondamentaux

Electronic reference
Robin Medard Inghilterra, "L'instauration d'une « technopolice » administrative en milieu urbain : les droits et libertés sur un fil", *La Revue des droits de l'homme* [Online], 26 | 2024, Online since 09 October 2024, connection on 15 October 2024. URL: http://journals.openedition.org/revdh/20912

L'instauration d'une « technopolice » administrative en milieu urbain : les droits et libertés sur un fil

Robin Medard Inghilterra

AUTHOR'S NOTE

La présente contribution s'inscrit dans le cadre d'une série d'études relatives à la « technopolice » administrative. Elle en constitue le deuxième volet, consacré aux risques en matière de droits et libertés. Le premier volet, dédié à la définition du phénomène et à de grands enjeux qu'il soulève en droit administratif, est en accès libre au sein du numéro 25 de la *Revue des droits de l'homme*. Un troisième article – à paraître – complétera cette série. Il portera sur les arrêtés de police édictés à l'occasion des Jeux olympiques et paralympiques 2024.

> *« Pour déterminer l'étendue du pouvoir de police dans un cas particulier, il faut tout de suite se rappeler que les pouvoirs de police sont toujours des restrictions aux libertés des particuliers, que le point de départ de notre droit public est dans l'ensemble des libertés des citoyens, que la Déclaration des droits de l'homme est, implicitement ou explicitement, au frontispice des constitutions républicaines, et que toute controverse de droit public doit, pour se calquer sur les principes généraux, partir de ce point de vue que la liberté est la règle, et la restriction de police l'exception »*[1]

1 Souvent précaire, toujours discutable, parfois introuvable, l'équilibre entre sécurité et libertés anime les controverses[2]. Du côté des juristes, les conclusions du commissaire du

gouvernement Corneille sous l'arrêt *Baldy,* rendu le 10 août 1917, continuent de résonner avec force un siècle plus tard et sont régulièrement exhumées par les publicistes. L'écho leur est offert, il est vrai, par une rhétorique politique désormais commune qui clame haut et fort que « la sécurité est la première des libertés ! », sans que le locuteur ne soit la plupart du temps troublé par l'oxymore[3]. Pourtant, si relation il y a bien entre sécurité et liberté, elle prend avant tout la forme de l'opposition. À l'inverse du droit à la sûreté[4], la sécurité ne figure pas dans le catalogue des droits fondamentaux[5]. Elle ne saurait par ailleurs être érigée en liberté, comprise comme un « pouvoir faire » qui « ne nuit pas à autrui »[6]. Lorsque la notion de sécurité est évoquée dans les instruments nationaux et internationaux de protection des droits, elle l'est sous les traits de la sécurité « nationale » ou sécurité « publique », et non individuelle. Elle est alors appréhendée comme motif de restriction – et non de garantie – des droits et libertés consacrés[7].

2 La *technopolice administrative*[8] illustre cette relation. Son déploiement restreint la portée des droits et libertés au nom de la poursuite d'un impératif de sécurité publique. Les mesures de police envisagées doivent dès lors être soumises à un « triple test » pour vérifier tour à tour leur caractère *adapté*, *nécessaire* et *proportionné*[9]. Leur constitutionnalité, leur conventionnalité et leur légalité en dépendent. Que le législateur confère aux outils de la technopolice une base légale ou que l'administration autorise par arrêtés leur mise en œuvre sur le territoire, ce triple test constituera quoi qu'il en soit le référentiel d'un contrôle opéré tantôt par le Conseil constitutionnel, tantôt par les juridictions administratives, voire par la Cour européenne des droits de l'homme (ci-après Cour EDH). La pertinence du triple test, solidement établie pour les activités de police administrative traditionnelles[10], n'est pas remise en cause par l'emploi moderne de moyens numériques. Au contraire, en agissant par l'intermédiaire de traitements de données (*e.g.* captation, enregistrement et diffusion d'images aux moyens de caméras installés sur des aéronefs, emploi d'un traitement algorithmique des images issues d'un système de vidéoprotection), la technopolice administrative est – au surplus – soumise aux grands principes du droit des données à caractère personnel. Parmi eux, figure le principe de minimisation des données qui impose que les données traitées soient adéquates et pertinentes (pour un traitement *adapté*, propre à atteindre la finalité poursuivie) mais également limitées ou non excessives (pour un traitement *proportionné*)[11]. D'autres principes, tels que la limitation de la durée de conservation des données ou la limitation des finalités du traitement au strict *nécessaire*, contribuent aussi à asseoir l'emprise des standards évoqués[12]. *A fortiori*, le traitement de données biométriques n'est envisageable en France qu'en cas de « nécessité absolue » et « sous réserve de garanties appropriées pour les droits et libertés de la personne concernée »[13].

3 Il n'est dès lors guère surprenant que le développement de la technopolice administrative ait pu être entravé dans les prétoires en raison du non-respect des standards du triple test. Le Conseil constitutionnel a censuré par deux fois des dispositions législatives autorisant le recours à des drones équipés de caméras, car le législateur n'avait pas opéré une « conciliation équilibrée » entre, d'une part, les objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions et, d'autre part, le droit au respect de la vie privée[14]. Le tribunal administratif d'Orléans a annulé la convention d'expérimentation conclue entre la ville d'Orléans et l'entreprise Sensivic car l'implantation de capteurs

de son, « à la supposer utile pour l'exercice des pouvoirs de police confiés au maire », ne pouvait « être [regardée] comme nécessaire à l'exercice de ces pouvoirs »[15]. Quant au tribunal administratif de Marseille, il a prononcé l'annulation de la délibération du conseil régional de Provence-Alpes-Côte d'Azur annonçant l'expérimentation d'un dispositif d'authentification par reconnaissance faciale à l'entrée de deux lycées de la région. La proportionnalité n'était cette fois pas établie car l'administration ne démontrait pas que la fluidification et la sécurisation des contrôles « ne pourraient être atteintes de manière suffisamment efficace par des contrôles par badge » ou par d'autres mesures alternatives moins attentatoires aux droits et libertés[16].

4 Si la technopolice administrative a ponctuellement buté sur le triple test[17], son principal outil semble, en revanche, exonéré du respect de ces standards. Le caractère *adapté* de la vidéoprotection peine en effet à être démontré. Les études empiriques réalisées ont, à l'inverse, documenté une incapacité du dispositif à satisfaire les principaux objectifs qui lui sont assignés. L'utilisation de la vidéoprotection se révèle d'abord « considérablement moins simple, naturelle et fluide que la culture populaire le laisse croire »[18] en raison de nombreuses difficultés techniques[19]. Surtout, son efficacité en vue de prévenir la délinquance est frontalement mise en cause[20]. Seule une exception est régulièrement relevée, à savoir la sécurisation de lieux précis pour prévenir notamment des vols de véhicules stationnés dans des parkings et des cambriolages. Mais un « effet plumeau » tend alors à déplacer la délinquance. Guillaume Gormand, spécialiste de l'évaluation des dispositifs de vidéoprotection, estime en conséquence que « la mise à l'épreuve rigoureuse de ce bénéfice supposé révèle que l'intérêt dissuasif de la vidéosurveillance demeure parfaitement illusoire lorsqu'elle est installée sur des espaces publics ouverts »[21]. Quant à la capacité de la vidéoprotection à servir le traitement judiciaire des affaires de délinquance et à élucider les enquêtes, elle est, certes, davantage établie. Elle ne l'est toutefois que dans des proportions relativement faibles (les caméras seraient en moyenne mobilisées dans une enquête sur dix, fournissant un indice ou une preuve issue de la vidéo dans 1,1 % des enquêtes au total et dans 5,8 % des enquêtes élucidées[22]). Le maniement judiciaire de la preuve vidéo s'avère par ailleurs hautement délicat[23]. Aux côtés des chercheurs, la Cour des comptes, sceptique, pointe le fait qu'« aucune corrélation globale n'a été relevée entre l'existence de dispositifs de vidéoprotection et le niveau de la délinquance commise sur la voie publique, ou encore les taux d'élucidation », cela, « malgré l'ampleur des sommes engagées »[24]. Les chambres régionales des comptes[25] et la CNIL manifestent elles aussi leurs réserves[26] quand les députés Philippe Gosselin et Philippe Latombe, partisans de la vidéoprotection, concèdent : « il apparaît difficile d'affirmer avec certitude que les caméras fixes ont réellement un effet dissuasif sur la délinquance »[27].

5 Le caractère *nécessaire* de la vidéoprotection est, lui aussi, généralement présumé, rarement démontré, notamment lorsqu'il est question d'acquérir de nouvelles caméras[28]. Le défaut de nécessité[29] peut alors fonder une requête en annulation intentée à l'encontre de l'arrêté préfectoral autorisant l'implantation des nouvelles caméras. Tel fut le cas dans la commune de Ploërmel. La cour administrative d'appel de Nantes a sanctionné le dispositif autorisé, qui s'étendait « sans justification légale à presque tous les principaux lieux de vie de la commune », dès lors qu'il n'était pas établi « par les statistiques relatives à la délinquance dans la commune, que ces lieux seraient particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants »[30]. Mais de telles requêtes sont extrêmement rares, et le maillage

territorial de la vidéoprotection s'étend le plus souvent sans fin et sans frein. En juin 2024, la Commission nationale consultative pour les droits de l'homme (ci-après CNCDH) élargissait le constat en dénonçant une soustraction généralisée de la vidéoprotection à la démonstration d'une réelle nécessité aux fins de prévention des troubles à la sécurité publique[31].

6 Face aux standards juridiques clairs attachés au triple test, la pratique offre en définitive un contraste saisissant en l'absence – pour l'essentiel – de contrôles effectifs des outils de la technopolice administrative, imputable à plusieurs facteurs (*e.g.* rares actions en justice, massification du recours à ces outils, déficience et internalisation des procédures autorisant leur déploiement)[32]. Ce contexte renforce l'intérêt d'une réflexion sur la nature et la proportionnalité des atteintes aux droits et libertés qu'engendrent ces outils. D'autant que les atteintes en question sont considérables. D'un point de vue quantitatif, la captation et le traitement massifs de données ouvrent la voie à une surveillance tout aussi massive en l'absence de garde-fous. D'un point de vue qualitatif, la technopolice présente des caractéristiques spécifiques, et implique en particulier une distance entre les sujets de droit et les technologies de surveillance, qui sont parfois mobiles et souvent discrètes. Il s'agit en d'autres termes d'une police administrative « sans contact » qui laisse place à un sentiment ou à une crainte de surveillance constante, totale[33].

7 Pour être problématisée plus avant, la recherche sur la nature et la proportionnalité des atteintes aux droits et libertés qu'engendre la technopolice administrative ne peut faire l'économie du contexte spatial dans lequel elle est déployée, à savoir l'espace public. Central pour l'exercice des droits et libertés par les citoyens, l'espace public a alternativement été envisagé en tant que concept[34] et en tant que catégorie juridique[35]. En tant que notion, il désigne les voies publiques, les lieux accessibles au public – que l'accès à ces lieux soit libre (*e.g.* plages, parcs, gares) ou conditionné (*e.g.* commerces, lieux de spectacles, voies et véhicules de transports en commun) –, ainsi que les lieux affectés à un service public (*e.g.* mairies, hôpitaux, tribunaux, établissements d'enseignement, musées, bibliothèques)[36]. Plusieurs auteurs se sont récemment interrogés sur la transformation de l'espace public face aux pouvoirs de police administrative mis en œuvre pour réagir à la pandémie de covid-19[37]. Stéphanie Hennette-Vauchez a quant à elle mis en lumière une privatisation fonctionnelle croissante de l'espace public, pour ensuite interroger les conséquences de ce « brouillage des frontières entre le "public" et le "privé" du point de vue du droit des libertés »[38]. En somme, une interrogation récurrente traverse la recherche en droit des libertés fondamentales : la portée des droits et libertés est-elle affectée par les transformations que subit l'espace public, en particulier ces dernières années ? Cette interrogation gagne à être prolongée, et c'est sous cet angle[39] que nous souhaitons saisir les implications de *l'instauration d'une technopolice administrative en milieu urbain*, après en avoir posé le cadre, matériel et juridique, et après avoir envisagé ses effets sur les catégories habituelles du droit administratif[40]. Les transformations induites par la technopolice administrative sont-elles susceptibles de « mettre en sommeil »[41] les droits et libertés dans l'espace public ?

8 Pour saisir les principales dynamiques à l'œuvre, nous faisons le choix d'envisager l'hypothèse « fonctionnelle »[42] des technologies de surveillance, c'est-à-dire d'évacuer les atteintes aux droits et libertés qui résultent de leurs dysfonctionnements pourtant aussi réels que fréquents (*e.g.* faux positifs, effets discriminatoires provoqués par la

sélection des jeux de données, par leur étiquetage ou par les modalités d'entraînement algorithmique, obsolescence du support matériel ou logiciel, vol de données en raison d'un stockage en base centralisé)[43]. Ce choix est dicté par le souci de ne pas résumer l'effectivité des droits et libertés à l'enjeu du perfectionnement technologique. En dépit de cette concession d'ampleur, les droits et libertés semblent malgré tout sur un fil, suspendus à des arbitrages et à des clarifications juridiques qu'il conviendra d'effectuer dans un avenir proche. Parce que la technopolice administrative accroît considérablement la transparence au sein de l'espace public, d'une part, elle a pour effet de dissiper une sphère privée jusqu'alors protectrice des administrés (I). Parce qu'elle implique une surveillance accrue, d'autre part, elle entame la vitalité des libertés exercées par les citoyens dans – et grâce à – l'espace public (II).

I/ – Une sphère privée dissipée par la transparence de l'espace public

9 Le concept de *sphère privée* est ici employé de manière lâche et fonctionnelle afin d'englober deux appendices des sujets de droit que sont leur vie privée et leurs données à caractère personnel. Étroitement liées, elles font l'objet d'une protection juridique tantôt ancienne, via le droit au respect de la vie privée, tantôt moderne, par l'entremise du droit des données à caractère personnel[44]. Ce dernier est progressivement envisagé comme distinct et indépendant du premier[45]. Les deux droits s'avèrent pertinents pour saisir les implications de la technopolice administrative. La recherche constante d'une transparence de l'espace public conduit d'abord à une collecte massive de données, assimilable à une captation du « privé ». En la matière, le régime protecteur qui découle du droit des données à caractère personnel se trouve affaibli par la montée en puissance de l'impératif de sécurité publique (A). La recherche de transparence aboutit ensuite à la mobilisation croissante de traitements biométriques dans l'espace public, assimilable à une négation du « privé ». La perspective d'une neutralisation de l'anonymat questionne alors quant à la portée du droit au respect de la vie privée (B).

A/ La captation du privé : des données publiques, plus que personnelles ?

10 Peu importe le moyen (vidéoprotection, recours aux drones, vidéosurveillance automatisée, reconnaissance faciale, capteurs de son, géolocalisation…), les technologies de surveillance peuvent servir à la fois des missions de police judiciaire et de police administrative – le cas échéant de renseignement. Dans le cadre de la police administrative, il s'agit avant tout de réguler les flux, gérer les foules, analyser, prédire et anticiper les comportements afin d'éviter les atteintes aux biens et aux personnes. La nature des données (anonymisées, sensibles, biométriques) peut varier, tout comme les modalités de leur collecte (consentie ou non, avec ou sans information préalable) et les conditions de leur exploitation (avec ou sans déport des images, avec ou sans stockage, avec ou sans autorisation préalable, d'une autorité judiciaire ou administrative, indépendante ou déconcentrée). La finalité du traitement de données fluctue également (retransmission d'images, génération d'alertes, authentification, identification). Chacun de ces paramètres peut influencer l'appréciation portée sur la légalité du

traitement. Dans tous les cas, en revanche, les données collectées puis traitées sont érigées en ressource stratégique pour les pouvoirs publics.

11 Dès lors que sont en cause des données à caractère personnel, c'est-à-dire des informations « se rapportant à une personne physique identifiée ou identifiable »[46], un régime juridique précis est applicable. Il découle principalement du Règlement général sur la protection des données à caractère personnel (ci-après RGPD) et de la Loi informatique et liberté (ci-après LIL), dont le titre III transpose la directive « police-justice »[47] applicable lorsque la finalité poursuivie est la prévention des menaces et des atteintes à la sécurité publique. Ce régime juridique est structuré autour de grands principes qui concourent à la protection des données[48], précisément parce que leur caractère *personnel* exige de les prémunir des accaparations et détournement abusifs, le cas échéant imputables aux pouvoirs publics. Or, dans un contexte de faibles contrôles, le développement de la technopolice administrative tend à affaiblir ce régime juridique et plusieurs digues jusqu'alors protectrices sautent.

12 Le sort réservé au droit d'opposition en fournit une première illustration. Défini par les articles 21 du RGPD et 110 de la LIL, il permet à toute personne concernée « de s'opposer à tout moment, pour des raisons tenant à sa situation particulière[49] [ou pour des motifs légitimes[50]], à un traitement des données à caractère personnel la concernant ». Cette opposition, une fois manifestée, contraint le responsable du traitement à cesser toute utilisation des données à caractère personnel. Le droit d'opposition, central pour le régime juridique de protection des données, incarne parfaitement leur dimension *personnelle* et la mainmise conservée du sujet du traitement sur ce qui lui est propre[51]. Des expérimentations de vidéosurveillance automatisée (ci-après VSA) dans l'espace public ont ainsi été bloquées en raison d'une impossibilité de garantir la prise en compte d'une opposition au traitement des données[52]. Rapidement, le droit d'opposition s'est révélé être un blocage décisif au bon développement de la technopolice ; un « problème » à « écarter » pour le secteur industriel. Les comptes-rendus des réunions de l'Association nationale de la vidéoprotection l'illustrent d'ailleurs sans détour : « Les personnes concernées par ces traitements ont des droits. Parmi ces droits, *il y en a un qui pose un problème*, c'est le droit d'opposition. Pourquoi ? Il doit pouvoir être exercé avant le traitement : cela est très difficile avec les caméras augmentées. Il y a eu beaucoup d'échanges avec les concepteurs, qui ont proposé des choses, mais qui restent trop contraignantes pour les personnes concernées. En conclusion, *il faudrait écarter le droit d'opposition* »[53].

13 Une dynamique nette émerge en réaction : celle d'une neutralisation du droit d'opposition par les pouvoirs publics. En ce sens, le décret du 10 mars 2021 a autorisé le recours à la VSA pour mesurer le taux de port du masque dans les transports publics. Son article 1er dut pour ce faire écarter plusieurs droits des sujets du traitement algorithmiques, parmi lesquels figure le droit d'opposition[54]. La loi du 19 mai 2023 relative aux Jeux olympiques et paralympiques 2024 (ci-après loi JOP) a quant à elle actualisé le Code de la sécurité intérieure (ci-après CSI) et soumis explicitement les traitements de données provenant des systèmes de vidéoprotection et des caméras installées sur des drones à la LIL et au RGPD[55]. Cette actualisation a immédiatement eu pour effet d'exposer le traitement des images au droit d'opposition prévu par les deux textes. Le pouvoir réglementaire en a tiré les conséquences. Par un décret du 27 novembre 2023, il a écarté ce droit pour les personnes filmées par les caméras de vidéoprotection et celles installées sur des aéronefs[56]. La loi JOP autorise en

complément l'expérimentation de la VSA en temps réel pour assurer la sécurité de manifestations sportives, récréatives ou culturelles. Là encore, le décret d'application du 28 août 2023 neutralise le droit d'opposition des sujets pour faciliter le traitement algorithmique des images[57].

14 Les neutralisations successives du droit d'opposition sont, certes, fondées sur des clauses de limitation des droits prévues par le RGPD[58] et le titre III de la LIL[59]. Elles peuvent, certes, être expliquées par la difficulté de recueillir techniquement les manifestations d'opposition au traitement d'images captées dans l'espace public, en milieu ouvert, du moins lorsqu'il est question d'un traitement extrêmement massif de données. Elles procèdent, certes, de la finalité de police, même administrative, dont l'efficacité suppose de ne pas seulement contrôler les consentants. Ces neutralisations du droit d'opposition illustrent toutefois une tendance symptomatique qui affecte la conciliation opérée entre les droits et libertés d'une part, et l'impératif de sécurité publique de l'autre. Elles attestent la perte de contrôle des sujets de droit sur leurs données personnelles, captées sans consentement et sans opposition possible dans l'espace public, par les pouvoirs publics, au nom de la sécurité publique. De telle sorte qu'il est possible de s'interroger : ces données personnelles deviendraient-elles *avant tout* publiques ?

15 D'autant que d'autres digues qui composent – aux côtés du droit d'opposition – le régime protecteur des données à caractère personnel s'effacent elles aussi avec le déploiement de la technopolice administrative. L'augmentation de la durée de conservation des données traitées dans le cadre de l'expérimentation de la VSA jusqu'en mars 2025 fait partie des symptômes. Habituellement, et depuis 1995[60], les enregistrements des images issues des systèmes de vidéoprotection ne peuvent être conservés au-delà d'un délai d'un mois[61]. Le Laboratoire d'innovation de la Commission nationale de l'informatique et des libertés estimait en 2018, dans un élan d'optimisme, que la VSA permettrait d'améliorer le traitement et l'analyse des images, et que ce gain d'efficacité pourrait permettre de réduire d'autant le délai de conservation des données[62]. Lorsque, cinq ans plus tard, le législateur a finalement autorisé le recours à la VSA, il a au contraire étendu la durée de conservation de certaines images jusqu'à un an. Cette extension doit permettre d'utiliser de manière dérogatoire les images ainsi conservées – et constituées en échantillon – comme données d'apprentissage[63].

16 Les sociétés éditrices des logiciels qui ont bénéficié des marchés publics passés dans le cadre de l'expérimentation de la VSA (*i.e.* Wintics, Videtics, ChapsVision) n'ont *a priori* pas accès aux données conservées aux fins d'entraînement[64]. La fragilisation du principe de limitation de la durée de conservation des données n'est donc pas imputable à un impératif commercial. Juridiquement, les données demeurent « sous la responsabilité de l'État »[65]. Plusieurs incertitudes persistent à ce stade de l'expérimentation quant à ces échantillons[66]. Toujours est-il que si la durée légale de conservation est bel et bien multipliée par douze, pour une masse non négligeable de données, c'est au nom de l'amélioration des dispositifs futurs de VSA qui seront employés pour sécuriser l'espace public. La protection conférée aux données en raison de leur dimension personnelle s'amenuise, et cet affaiblissement est une fois de plus fondé sur le fait qu'elles sont avant tout captées dans l'espace public, par les pouvoirs publics, au nom de la sécurité publique[67].

17 D'autres digues qui composent le régime protecteur des données à caractère personnel sautent, moins en raison des ajustements juridiques – qui neutralisent le droit

d'opposition ou atténuent le principe de limitation de la conservation des données – que de la pratique. Tel est le cas du droit à l'information des citoyens. Prévu aux articles 12 à 14 du RGPD et aux articles 48 et 104 de la LIL, le droit à l'information implique de mettre à disposition des personnes concernées l'identité et les coordonnées du responsable du traitement et du délégué à la protection des données. Il implique encore de préciser les finalités poursuivies par le traitement et contraint celui qui en est responsable à informer de l'existence et des modalités d'exercice du droit d'accès, du droit à la rectification ou à l'effacement des données, comme du droit de demander une limitation du traitement[68].

18 Pour garantir l'effectivité de ce droit, le recours aux caméras aéroportées dans le cadre des opérations de police administrative était, en 2020, régulièrement accompagné de la diffusion par haut-parleurs de messages d'information, audibles jusqu'à quarante mètres[69]. Lorsqu'une base légale a été conférée *a posteriori*[70] (deux ans plus tard) aux caméras installées sur des drones, après avis du Conseil d'État[71], le législateur a pris le soin de préciser que « le public est informé *par tout moyen approprié* de l'emploi de dispositifs aéroportés de captation d'images »[72]. L'analyse d'impact relative à la protection des données réalisée préalablement à l'édiction du décret d'application[73] envisageait deux possibilités : l'intégration aux aéronefs de dispositifs sonores pour avertir le public concerné par un éventuel enregistrement, ou l'installation de dispositifs physiques (*e.g.* barrières) matérialisant les zones du périmètre placé sous surveillance aérienne[74]. Ces moyens semblaient de nature à satisfaire la position de la Commission nationale de l'informatique et des libertés (ci-après CNIL), qui estimait que « l'information des personnes susceptibles d'être filmées doit se faire sur le lieu de l'opération au cours de laquelle les caméras aéroportées seront utilisées »[75]. Toutefois, la pratique qui s'est, depuis, stabilisée, ne repose sur aucun de ces deux dispositifs. L'information du public prend généralement la forme d'une publication de l'arrêté de survol au recueil des actes administratifs et sur le site de la préfecture ; et cette publication est parfois mentionnée sur certains réseaux sociaux sans préciser le périmètre de survol. L'exigence d'une information « aisément accessible »[76] pour les personnes filmées n'apparaît dès lors pas satisfaite.

19 D'autres pratiques contribuent encore à amoindrir le droit à l'information des citoyens. Les arrêtés portant autorisation de captation, d'enregistrement et de transmission d'images au moyen de caméras installées sur des aéronefs ne mentionnent généralement pas l'identité et les coordonnées du délégué à la protection des données compétent, pas plus qu'ils ne précisent l'existence et les modalités d'exercice des droits d'accès, à la rectification ou à l'effacement des données, ainsi qu'à la limitation du traitement[77]. Régulièrement, ces arrêtés renvoient à un plan annexé le soin de préciser le périmètre concerné par la captation des données. Or, ces plans sont parfois imprécis[78], voire absents[79], ce qui altère encore l'effectivité du droit à l'information des citoyens. Surtout, il est possible de constater une pratique récurrente de publication tardive des arrêtés préfectoraux. Beaucoup sont publiés moins de 24 heures avant leur date annoncée d'effet[80] ou le jour même[81]. D'autres sont publiés *a posteriori,* neutralisant le droit à l'information[82]. Cette pratique massive de publication tardive, imputable notamment à la préfecture de police de Paris, dépasse le seul recours aux drones. Elle est aussi observable concernant les arrêtés portant autorisation de l'emploi des logiciels de VSA[83].

20 Le droit des données à caractère personnel a pour fonction la protection de ces données et de leur traitement parce qu'elles constituent le prolongement de leurs titulaires, citoyens, administrés, sujets de droit[84]. En affaiblissant ce régime juridique au nom de l'impératif de sécurité publique, la technopolice administrative tend à faire primer l'intérêt public des données captées sur leur dimension personnelle[85]. La réaction des autorités nationales face à cette dynamique d'affaissement des droits constitue un enjeu majeur. Cette réaction pourrait passer par des contrôles resserrés afin d'encadrer davantage l'action des autorités de police, à différents niveaux, pour renforcer l'effectivité d'un régime juridique malmené. Or, à ce stade, force est de constater que ces contrôles sont relativement lâches[86].

21 La garantie que constitue la réalisation des analyses d'impact relatives à la protection des données (ci-après AIPD) apparaît, d'abord, insuffisante. Ces dernières sont déclaratives, reposent sur une appréciation des risques par le responsable du traitement, et possèdent une portée limitée, notamment en ce qu'elles ne tiennent pas compte des incidences du dispositif déployé (*e.g.* vidéoprotection, VSA, drones) sur les autres droits et libertés (*e.g.* libertés de circulation, d'expression, de manifestation, d'association)[87]. Il n'est au demeurant pas exclu que les sociétés privées attributaires des marchés publics concourent – largement – à la réalisation des AIPD pour les solutions logicielles qu'elles commercialisent. Non contentes d'exclure la prise en compte du point de vue des sujets du traitement[88], les AIPD se résument alors à de simples autoévaluations partiales[89]. La transmission de ces AIPD à la CNIL demeure, ensuite, trop aléatoire. Pourtant, dans tous les cas envisagés, sont en cause (1) des traitements de données à grande échelle (2) par l'application de nouvelles solutions technologiques et (3) dans une finalité de surveillance systématique. Trois des neuf critères fixés par la CNIL de nature à imposer sa consultation préalable sont dès lors remplis[90]. Ces traitements présentent donc bien des risques pour les droits et libertés au sens de la LIL et du RGPD[91]. Là encore, la réalité offre un contraste saisissant. Il est possible de s'étonner que la CNIL ne soit pas systématiquement informée du recours à des logiciels de VSA (en dehors des hypothèses prévues par la loi JOP), que ces logiciels soient utilisés par des collectivités territoriales ou par les services nationaux de police et de gendarmerie[92]. Les articles 62, 63 et 90 de la LIL exigent pourtant une demande d'avis adressée à la CNIL ou une consultation. Il est aussi surprenant et problématique que le conseil d'une communauté de communes énonce – sans conséquence – en audience de référé au Conseil d'État que les services nationaux disposent d'un accès au logiciel de VSA dont elle s'est équipée[93], caractérisant un traitement de données mis en œuvre pour le compte de l'État à des fins de police ou de justice, quand ces traitements doivent être prévus par une disposition *a minima* réglementaire – faisant défaut en l'espèce – après avis motivé et publié de la CNIL[94]. En toute hypothèse, et de manière plus structurelle, les moyens dont dispose cette dernière pour procéder à des contrôles efficaces semblent largement déficients (340 contrôles seulement en 2023, dont 157 sur place et 38 sur pièces)[95].

22 Les garanties offertes en complément par les contrôles juridictionnels apparaissent aussi insuffisantes. En amont, ces contrôles sont largement tributaires des actions contentieuses de la société civile. Or, ces actions demeurent rares, et ne sont entreprises que par quelques associations spécialisées, Quadrature du net, Ligue des droits de l'homme et Association pour la défense des libertés constitutionnelles en tête[96]. La pratique de publication tardive des arrêtés de police tend, en outre, à

neutraliser le droit au recours effectif de ces rares vigies, y compris en référé. Le nombre de ces arrêtés y contribue également : de quelle effectivité peut être créditée l'exigence d'une proportionnalité stricte du recours aux drones – qui a justifié une réserve d'interprétation du Conseil constitutionnel[97] – lorsque des arrêtés de survol sont édictés un jour sur deux (comme cela a été documenté pour la région parisienne au cours de l'été 2024[98]) ? En aval, les garanties du contrôle juridictionnel semblent altérées par la faible expertise dont a parfois témoigné le juge administratif. À titre d'illustration, les tribunaux administratifs de Paris et de Lille n'ont pas hésité à affirmer que, en l'absence d'identification unique, le recours à des caméras aéroportées par une préfecture de police et à un logiciel de VSA par une commune ne permet pas de caractériser un traitement de données à caractère personnel[99], quand bien même la jurisprudence constante[100] et la loi[101] en disposent autrement.

23 En définitive, la protection conférée à la sphère privée des administrés dans l'espace public par le droit des données à caractère personnel est constamment réduite. Ces données, parce qu'elles servent une finalité de sécurité publique, basculent pour partie dans la sphère du régalien. Leur captation est inévitable en raison de la neutralisation de l'opposition et leur accumulation semble procéder d'une dépossession. Quand bien même y verrait-on un simple transfert de données consenti, indirectement crédité du consentement à la législation nationale et à l'autorité de l'État, il n'y aurait là qu'un « marchandage maussien » (*maussian bargain*) biaisé. Ce concept, inspiré de l'anthropologue Marcel Mauss et de son *Essai sur le don*[102], qualifie pour Marion Fourcade et Daniel N. Kluttz un processus spécifique d'appropriation des données au sein de l'économie numérique[103]. Le marchandage en question repose sur l'abandon volontaire des données à caractère personnel de la part de leurs titulaires, qui a pour contrepartie la concession d'un accès gratuit à un service détenu par l'acteur économique accumulant les données par le don. Dans le cas de la technopolice administrative, le marchandage ne pourrait être que biaisé en raison de la dépendance à l'espace public, viciant nécessairement le consentement et le don. Peu importe la perception retenue, l'interrogation persiste : l'espace public a-t-il vocation à voir son accessibilité conditionnée à – ou marchandée par – un renoncement partiel des citoyens à la protection de leurs données ? En l'état, le privé est capté, accaparé. À d'autres égards, il semble nié.

B/ La négation du privé : contre l'anonymat, les traitements biométriques

24 Analyser les dynamiques juridiques qui affectent le sort des droits et libertés dans l'espace public suppose de prêter attention aux transformations solidement avancées, comme la captation en abondance des données. La démarche suppose également d'envisager les trajectoires esquissant des scénarii non encore advenus. Tel est le cas de la « fin de l'anonymat »[104] qui menace d'être provoquée par la multiplication des traitements de données biométriques. Dans sa version la plus nette, la biométrie révèle l'identité civile du sujet. Dans une version édulcorée, elle singularise une personne au sein d'un groupe ou d'un environnement, sans en dévoiler l'identité civile[105]. La qualification de traitements de données biométriques repose dans les deux configurations sur deux éléments : la nature des données (*i.e.* physiques, physiologiques ou comportementales) et la finalité de leur traitement (*i.e.* l'identification unique)[106]. Les traitements biométriques contribuent à leur tour à dissiper l'opacité de la sphère

privée des individus et à accentuer la transparence de l'espace public[107]. Ils altèrent en particulier le maintien – en dehors des contrôles de police matérialisés – d'une identité privée, anonyme[108]. Un pas supplémentaire est franchi. Il ne s'agit plus seulement d'analyser les masses, les flux, mais d'individualiser les citoyens pour leur imputer, le cas échéant, des comportements, qu'ils soient légaux ou illégaux.

25 Les dernières évolutions juridiques au niveau de l'Union européenne sont considérables en la matière. Elles autorisent expressément l'identification par reconnaissance faciale en temps réel dans l'espace public[109]. Formellement, l'article 5 du Règlement sur l'intelligence artificielle du 13 juin 2024 (ci-après Règlement IA) interdit certains systèmes d'IA considérés comme excessivement dangereux du point de vue des droits et libertés. Parmi les pratiques interdites, figurent les systèmes d'inférence des émotions sur le lieu de travail ou dans les établissements d'enseignement, les systèmes de classement et de notation sociale, ainsi que les systèmes d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives. Le recours à ces derniers est néanmoins permis à titre dérogatoire pour trois motifs : la recherche ciblée de victimes et de personnes disparues ; la localisation ou l'identification des auteurs de certaines infractions ; et la prévention des menaces pour la sécurité physique des personnes – incluant l'hypothèse terroriste[110]. Les débats afférents à cette législation européenne, comme les prises de position des parlementaires français et du Conseil de l'Europe, incluant la Cour EDH, soulignent, tous, la nécessité d'une vigilance spécifique face à cette forme de biométrie eu égard aux risques induits pour les droits et libertés[111]. Outre le fait qu'elle est réalisée sans que le sujet du traitement en ait conscience et sans son consentement (on parle de biométrie « passive »[112]), elle suppose surtout la constitution de vastes bases de données et de fichiers sur les individus (plus de 117 millions de personnes aux États-Unis, 700 millions en Chine)[113]. En France, plusieurs limites pourraient gêner la massification du recours à l'identification biométrique dans l'espace public. À l'examen, leur fragilité apparaît cependant manifeste.

26 La première limite, technique, est fonction de la maturité technologique. S'il n'existe pas de fichier unique centralisant les gabarits des citoyens, le fichier du traitement d'antécédents judiciaires (fichier TAJ) et le fichier des titres électroniques sécurisés (fichier TES) contiennent d'ores et déjà plusieurs dizaines de millions d'images numérisées associées à l'état civil des personnes[114]. L'accès à ces fichiers est, en l'état, limité[115]. En ce qui concerne les solutions logicielles de reconnaissance faciale, certaines sont déjà en usage au sein de la police nationale depuis 2016 à des fins d'enquêtes judiciaires (*e.g.* solution Morpho Video and Image commercialisée par Idemia)[116]. Par conséquent, la disponibilité des fichiers comme celle des logiciels, cumulées au maillage territorial considérable de la vidéoprotection[117], permettent de conclure que la technique n'est plus une limite indépassable. Comme le relevait un groupe de sénateurs en mai 2022 : « les forces de sécurité intérieure pourraient utiliser la reconnaissance faciale sur un vaste périmètre et à partir d'un réservoir de données conséquent »[118].

27 Des limites juridiques persistent par ailleurs, car l'application du Règlement IA se fera sans préjudice du RGPD et de la directive « police-justice » transposée par la LIL[119]. Or, ces textes posent des conditions au contournement de l'interdiction de principe des traitements biométriques[120]. Trois hypothèses à leur usage dérogatoire sont admises par l'article 88 de la LIL. La légalité des traitements biométriques exige alternativement : une disposition législative ou réglementaire ; une finalité de

protection des intérêts vitaux d'une personne physique ; ou des données manifestement rendues publiques. Le fondement offert par la dernière hypothèse est à exclure pour l'identification biométrique en temps réel dans l'espace public. Les données physiques (*i.e.* visages permettant la constitution de modèles ou gabarits) ne peuvent en aucun cas être considérées comme ayant été manifestement rendues publiques du seul fait de la présence des sujets du traitement dans l'espace public[121]. Le fondement offert par la deuxième hypothèse ne saurait être mobilisé que de manière marginale, sauf à diluer à l'excès la notion d'« intérêt vital ». Reste la première hypothèse (une disposition législative ou réglementaire) qui suffirait à fonder l'identification biométrique à distance en temps réel. Considérant que cette identification biométrique serait réalisée pour le compte de l'État à des fins de sécurité publique et sous réserve qu'elle soit considérée nécessaire au contrôle de l'identité des personnes, un simple décret en Conseil d'État pris après avis motivé et publié de la CNIL serait de nature à satisfaire les exigences de la LIL[122]. La Constitution s'en accommoderait plus difficilement, en revanche, dès lors que l'article 34 réserve au législateur le soin d'intervenir lorsque sont en cause les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques. Au bout du compte, une limite juridique impose de légiférer[123] : menu obstacle, d'autant plus qu'une proposition de loi relative à la reconnaissance biométrique dans l'espace public, déposée en 2023 par l'actuel ministre de l'Intérieur, Bruno Retailleau, est déjà en discussion au Parlement[124].

28 Le Règlement IA subordonne en complément le recours à l'identification biométrique en temps réel dans l'espace public à la poursuite de trois motifs, limitativement énumérés. La recherche ciblée de victimes et de personnes disparues ne présente pas le plus grand risque de glissement vers une surveillance généralisée, sous réserve que la recherche demeure bel et bien ciblée. Quant à la finalité de détection et d'identification des auteurs d'infractions, elle possède – finalement[125] – une portée restreinte : seules quelques infractions particulièrement graves sont limitativement énumérées en annexe du Règlement IA[126], même si l'inclusion du trafic de stupéfiants et des vols organisés parmi ces infractions pourrait malgré tout normaliser le recours à la reconnaissance faciale dans l'espace public. À plus forte raison, la brèche est ouverte par le motif de prévention des menaces pour la sécurité physique des personnes – incluant l'hypothèse terroriste. Les dix dernières années ont en effet permis d'illustrer à quel point des dispositifs d'exception – plus ou moins – taillés pour la lutte contre le terrorisme (*e.g.* loi du 3 avril 1955 relative à l'état d'urgence) ont été détournés ou dévoyés. Ils le furent tantôt par des interprétations extensives et un élargissement des motifs conditionnant leur déclenchement (*e.g.* loi du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme), tantôt par des qualifications matérielles abusives des faits de la part des autorités de police qu'un contrôle *a posteriori* du juge administratif n'a su qu'imparfaitement enrayer[127]. La forte légitimité du motif antiterroriste cumulée à une démarche préventive ouvre aisément la voie à un recours massif à l'identification biométrique en temps réel dans l'espace public. C'est d'ailleurs cet alliage de la prévention et de l'antiterrorisme, devenu des plus communs, qui a alimenté la motivation de plus d'une centaine d'arrêtés préfectoraux déployant des moyens technopoliciers en juillet et en août 2024 dans le cadre de l'organisation des Jeux olympiques et paralympiques[128].

29 Une ultime limite, procédurale, est posée par le Règlement IA. Chaque utilisation d'un système d'identification biométrique à distance en temps réel dans des espaces

accessibles au public doit faire l'objet de l'autorisation préalable d'une autorité judiciaire ou administrative indépendante[129] ; charge à cette autorité de vérifier que la nature de l'utilisation projetée, les conséquences de l'utilisation, les limitations géographiques, temporelles et personnelles fixées permettent de satisfaire un rapport de proportionnalité[130]. Deux réserves conduisent toutefois à relativiser la contrainte de ce régime d'autorisation préalable. Premièrement, l'identité de l'autorité administrative chargée de ce pouvoir n'est pas connue, pas plus que la solidité de son indépendance. Deuxièmement, en cas d'« urgence dûment justifiée », dont on sait qu'elle peut être appréciée avec une grande souplesse par l'autorité de police, l'autorisation peut n'être sollicitée qu'*a posteriori*[131].

30 Face à ce nouvel enjeu fondamental pour les droits et libertés, le législateur national devra prochainement opérer des arbitrages et des clarifications juridiques qui détermineront l'avenir de l'identification biométrique en France. Outil marginal ou banal ? Si la question reste en suspens, l'horizon d'une « fin de l'anonymat » dans l'espace public n'est pas à exclure.

31 D'autant qu'une version plus douce des usages de la biométrie dans l'espace public s'est déjà frayé un chemin en France sous les traits de la VSA. La reconnaissance du caractère biométrique de cette technologie n'est, certes, pas unanime. Le secteur industriel l'exclut généralement. Le législateur a, lui aussi, écarté cette qualification par l'article 10 de la loi JOP qui dispose que les traitements algorithmiques « n'utilisent aucun système d'identification biométrique [et] ne traitent aucune donnée biométrique »[132]. Mais la mention ne s'applique qu'au dispositif VSA de la loi JOP, limité à la détection de certains évènements prédéterminés[133]. Elle n'exclut pas, en revanche, que soient qualifiés de biométriques des usages de la VSA accomplis grâce aux logiciels acquis par les collectivités territoriales et leurs groupements, qui les mobilisent en dehors de l'expérimentation de la loi JOP, sur réquisitions ou non, à des fins de police administrative ou de police judiciaire. Or, les fonctionnalités biométriques de ces logiciels sont patentes. À titre d'illustration, le logiciel de VSA commercialisé par BriefCam, qui équipe déjà des dizaines de collectivités[134], comprend un module *Review* qui permet un traitement différé de l'image pour afficher simultanément des évènements survenus à différents moments. Il autorise la recherche multicaméras d'« objets » (personnes ou véhicules) ayant une « similarité d'aspect ». Plusieurs filtres permettent de singulariser des personnes au sein d'une « classe » (homme, femme, enfant), comme les attributs, qu'il s'agisse d'un sac (sac à dos, sac à main), d'un chapeau, d'un vêtement (sans manches, à manches courtes, à manches longues, short/jupe, pantalon), le cas échéant d'une couleur et d'une taille déterminés[135]. Dans ce cas, la qualification de biométrie ne saurait être écartée. Il y a bien, par l'apposition de ces différents filtres, singularisation d'une personne au sein d'un environnement, et donc identification unique, après traitement technique spécifique de données physiques, physiologiques ou comportementales[136].

32 Si la qualification de traitements de données biométriques est régulièrement contestée, c'est parce qu'elle emporte application d'un régime juridique plus protecteur pour les administrés, mais aussi, corrélativement, plus contraignant pour ceux qui déploient les outils de la technopolice administrative comme pour ceux qui les vendent. Admise pour la reconnaissance faciale, elle est parfois niée pour la VSA comportementale permettant la singularisation et le suivi de personnes, et généralement exclue lorsqu'est en cause la VSA qui se borne à la détection en temps réel d'évènements

prédéterminés. Ces visions dénotent une appréhension réductrice et cloisonnée des tâches humaines et technologiques : ne serait biométrique que l'identification exclusivement automatisée. Elles tendent à opérer une confusion problématique entre *traitement* de *données* biométriques[137] et *système* d'*identification* biométrique tel que défini par le Règlement IA, à savoir un « système d'IA destiné à identifier des personnes physiques [...] en comparant les données biométriques d'une personne avec celles qui figurent dans une base de données de référence »[138]. À l'inverse, une analyse en contexte des outils, qui tient compte des interactions entre humains et machines, entre opérateurs et logiciels, conduit à reconnaître un recours de plus en plus ordinaire aux traitements de données biométriques et, par effet de symétrie, une réduction de la garantie d'anonymat dans l'espace public pour les citoyens.

33 Cette levée de l'anonymat au nom de la sécurité publique entre en tension avec le droit au respect de la vie privée. L'application de ce droit dans l'espace public n'est, sans doute, pas pleinement intuitive. Elle découle pourtant de la jurisprudence de la Cour EDH et de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après Convention EDH). La notion de vie privée englobe des dimensions liées à l'intégrité physique et morale, à l'épanouissement personnel et à l'identité « sociale »[139]. L'image des personnes est notamment reconnue comme l'un des attributs principaux de la personnalité, et la protection de l'image faciale, plus particulièrement, est assimilée à une condition essentielle de l'épanouissement personnel[140]. Condition de jouissance du droit au respect de la vie privée, la protection de l'image s'étend sans ambiguïté à l'espace public dès lors que la vie privée couvre les interactions et relations sociales des sujets de droit avec le monde extérieur[141], en contexte public[142]. La Cour EDH ne va toutefois pas jusqu'à faire découler de l'article 8 un droit à l'anonymat dans l'espace public[143].

34 Elle a reconnu en revanche que les relations police-citoyens peuvent porter atteinte au droit au respect de la vie privée. Tel est le cas des fouilles publiques forcées, intrusives ou superficielles[144], et des contrôles d'identité arbitraires matérialisés dans l'espace public[145]. L'inspection visuelle et le contrôle d'identité par la police tombent dans le champ d'application de l'article 8. Qu'en est-il lorsque cette inspection et ce contrôle ont lieu à distance ? La jurisprudence de la Cour EDH est invariable et permet de conclure que la vie privée s'en trouve tout autant affectée. *A maxima,* la captation à distance d'images et leur stockage en vue du recours à un logiciel de reconnaissance faciale portent atteinte à la vie privée dans l'espace public[146]. *A minima*, « 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 »[147], ce qui inclut la simple vidéoprotection. En conséquence, les moyens employés par la technopolice administrative portent nécessairement atteinte au droit au respect de la vie privée dans l'espace public, en particulier en cas de traitement de données biométriques.

35 La question de la justification de ces atteintes mérite alors d'être posée. Elles poursuivent sans conteste un but légitime au sens de la Convention EDH, en l'occurrence la sécurité publique. Leur caractère adapté, nécessaire et proportionné prête davantage à discussion. Jusqu'où le recul de l'anonymat peut-il être admis ? Des craintes pour l'effectivité du droit au respect de la vie privée ont été manifestées en 2022 au sein d'un rapport d'information du Sénat sur la reconnaissance faciale. Les rédacteurs soulignaient que « l'usage d'un outil capable d'identifier une personne sur la

voie publique, d'en suivre les mouvements en temps réel et, le cas échéant, de reconstituer son parcours signerait la fin de l'anonymat dans l'espace public et l'avènement d'une forme de "société de la surveillance" que personne ne peut raisonnablement souhaiter »[148]. Où placer le curseur face à une dynamique qui met en cause la possibilité même d'une vie privée dans l'espace public ? La CNCDH s'en inquiétait également : « ces évolutions et ces perceptions bouleversent en profondeur notre conception de l'espace public en lui retirant toute dimension privée »[149].

36 Une fois de plus, des arbitrages et des clarifications juridiques sont attendus du législateur. Ils permettraient de fixer, le cas échéant, un cadre juridique plus resserré que ce qui demeure envisageable, tant au regard du Règlement IA que de la LIL. Les impératifs de nécessité et de proportionnalité pourraient notamment conduire à considérablement restreindre le champ des possibles pour le recours à l'identification par reconnaissance faciale et à la VSA comportementale. Rien n'interdit de bannir leur usage en dehors de deux hypothèses restreintes : dans une finalité de renseignement, sous contrôle de la Commission nationale de contrôle des techniques de renseignement ; dans une finalité de police judiciaire, par une unité habilitée des services nationaux, sur autorisation et sous le contrôle du juge judiciaire, exclusivement en temps différé. L'interdiction nette de ces technologies à des fins de police administrative et dans les mains des polices municipales gagnerait en particulier à être considérée. Pour être suivie d'effet, cette interdiction supposerait à l'évidence le déclenchement massif de contrôles de la CNIL au sein des collectivités territoriales.

*

37 *In fine*, l'effectivité du droit des données à caractère personnel et du droit au respect de la vie privée paraît précaire. Les évolutions des pratiques comme les évolutions juridiques marquent une tendance à l'admission des limitations de ces droits, dans des conditions permissives, au nom de la sécurité publique. Des rééquilibrages sont envisageables, voire nécessaires, sans qu'ils aient pour conséquence de reléguer la sécurité intérieure à une considération accessoire. En matière de police comme de technopolice administrative, le point d'équilibre est permis par le recours au triple test, fréquemment négligé, au mieux aménagé. Ce constat, valable eu égard aux répercussions de la transparence de l'espace public sur les droits fondamentaux (*i.e.* captation des données à caractère personnel, mise en cause du droit au respect de la vie privée), l'est également lorsque sont considérées les conséquences de la surveillance sur l'exercice des libertés.

II/ – Des libertés éprouvées par la surveillance de l'espace public

38 Degré supplémentaire de la technopolice administrative, la surveillance prolonge la transparence de l'espace public. Elle confère à la levée technique de l'opacité un objectif tactique, politique. Considérer cet objectif invite par répercussion à souligner l'importance de l'espace public pour les activités civiques. En son sein, sont habituellement exercées diverses libertés dont l'essence, les usages et les effets sont eux aussi éminemment politiques (*e.g.* libertés de circulation, d'expression, de réunion et d'association). Or, une mise sous surveillance – de plus ou moins grande intensité –

peut conduire les citoyens à renoncer en tout ou partie à ces libertés (A). Ce constat offre une réponse nette à l'interrogation soulevée en introduction, relative à une « mise en sommeil »[150] des droits et libertés. Ce phénomène semble bel et bien renforcé par la mutation confirmée de l'espace public : aire de liberté devenant zone de contrôles (B).

A/ La renonciation aux libertés : légalité suspecte et effet dissuasif technopolicier

39 La collecte massive de données puis leur traitement biométrique conduisent au recul de l'anonymat dans l'espace public. Ce recul n'est pas étranger à la renonciation à l'exercice des libertés[151]. Plusieurs observateurs posent en ce sens l'hypothèse d'un anonymat comme condition d'exercice des libertés. L'Agence des droits fondamentaux de l'Union européenne l'a par exemple exprimé au sujet de la reconnaissance faciale : l'utilisation de ces technologies « dans l'espace public peut porter atteinte à la liberté d'opinion et d'expression d'une personne, notamment parce qu'un *aspect nécessaire de l'exercice de cette liberté est l'anonymat* »[152]. Il est vrai que l'hypothèse d'un anonymat comme condition *nécessaire* ne semble pas pouvoir être admise en son sens fort. Il est parfaitement possible de circuler, de s'exprimer, de se réunir ou de s'associer dans l'espace public pour des individus dont l'identité civile est connue. L'anonymat peut en revanche être érigé en condition des libertés en un sens faible du terme, en tant qu'élément propice à leur exercice[153].

40 Cela signifie-t-il que seule la qualité de la liberté en dépend ? Que la circulation ou l'association ne seraient que meilleures lorsqu'elles sont anonymes, sans jamais être substantiellement menacées ? Que l'anonymat ne serait en définitive qu'un confort dans l'exercice des libertés ? Une réponse négative doit immédiatement être apportée dès lors que le choix même de les exercer peut, parfois, en dépendre. L'absence d'anonymat provoque dans ces conditions un effet dissuasif dont les répercussions sont suffisantes pour menacer sérieusement la réalisation des libertés. La CNIL en a, au demeurant, pleinement conscience. Au sujet de la mise en œuvre à grande échelle de la VSA, elle a ainsi rappelé que « l'espace public est un lieu où s'exercent de nombreuses libertés individuelles » et que « la *préservation de l'anonymat* dans l'espace public est une dimension essentielle pour l'exercice de ces libertés »[154].

41 Le phénomène est désormais bien connu, abondamment commenté, quoiqu'il demeure difficile à mesurer empiriquement. Parfois évoqué par l'expression de « *chilling effect* », l'effet dissuasif de la surveillance se réfère à la modification des comportements des sujets de droit, citoyens, administrés, par crainte d'une observation du comportement initial envisagé. Cette autocensure limite l'occurrence de comportements dont certains pourraient s'avérer illégaux, mais dont la plupart sont parfaitement légaux. La renonciation est simplement motivée par la peur que ces comportements deviennent préjudiciables, en raison d'une instrumentalisation postérieure ou d'une perception défavorable liée à leur dimension controversée, clivante, militante ou radicale. L'absence de protection effective de ces comportements légaux et légitimes (*e.g.* se rencontrer, manifester, organiser des activités politiques) est d'autant plus problématique qu'ils sont consubstantiels à la vitalité démocratique, aux débats et au pluralisme des courants d'expression. Sept chercheurs britanniques, ougandais et sud-africains ont publié en 2024 l'une des rares études empiriques et qualitatives sur le sujet[155]. Elle repose sur quarante-quatre entretiens réalisés en Ouganda et au Zimbabwe

auprès de membres des partis d'opposition, défenseurs des droits de l'homme, figures de la société civile et journalistes. Ses trois principaux résultats sont attendus. La crainte d'une surveillance génère avant tout une autocensure – *a fortiori* dans des régimes autoritaires ou dictatoriaux. Elle contribue au surplus à l'évitement des contacts avec certaines personnes ou organisations. Elle affaiblit enfin la confiance mutuelle entre les membres de groupes politiquement structurés, affectant de ce fait leur capacité à s'organiser et à se mobiliser[156].

42 En France, l'installation à Saint-Étienne de capteurs de son dans l'espace public, qui devaient permettent une audiosurveillance automatisée, a fait l'objet d'un avertissement de la CNIL pour des raisons proches. L'autorité administrative indépendante a estimé que les libertés d'expression, de réunion, de manifestation, d'association, comme la liberté d'aller et venir étaient menacées, considérant que les personnes concernées pouvaient « être amenées à altérer leur comportement par exemple en censurant eux-mêmes leurs propos tenus sur la voie publique ou en modifiant leurs déplacements [...] pour éviter les zones d'installation de capteurs sonores »[157]. L'analogie conduit à admettre ce risque lorsque sont en cause d'autres dispositifs tels que la captation d'images par drones, le recours à des logiciels de VSA ou à la reconnaissance faciale. Si ces dispositifs exigent une base légale pour être employés, c'est précisément parce qu'ils altèrent l'exercice des libertés publiques par la dissuasion et l'autocensure, et parce qu'il appartient en la matière au législateur de fixer les garanties fondamentales accordées aux citoyens[158]. Les conclusions des sept chercheurs précités pourraient encore prolonger le raisonnement de la CNIL. Au-delà du non-exercice personnel d'une liberté, l'audiosurveillance automatisée se révèle aussi liberticide en ce qu'elle engendre un évitement des contacts avec certaines personnes ou organisations en contexte public[159]. Le danger est, en résumé, celui d'un assèchement des libertés et d'une réduction de l'espace civique[160].

43 Un constat identique est unanimement formulé lorsqu'il est question de reconnaissance faciale. Les chercheurs soulignent le « risque d'un *chilling effect* »[161] quand les sénateurs évoquent « une pression » ou « des atteintes indirectes » aux libertés susmentionnées, causées par la « seule connaissance de l'utilisation, ou de la potentielle utilisation, d'une technologie de surveillance [qui] va amener le citoyen à modifier son comportement »[162]. L'Agence des droits fondamentaux de l'Union européenne employait peu ou prou les mêmes termes en 2019[163]. Une précaution similaire transparait encore du Règlement IA adopté par le législateur européen en 2024. Son préambule concède sans ambages : « l'utilisation de systèmes d'IA pour l'identification biométrique à distance "en temps réel" de personnes physiques dans des espaces accessibles au public à des fins répressives », bien qu'autorisée sous conditions, « est considérée comme particulièrement intrusive pour les droits et les libertés des personnes concernées, dans la mesure où elle peut [...] *susciter un sentiment de surveillance constante* et *dissuader indirectement l'exercice de la liberté de réunion et d'autres droits fondamentaux* »[164].

44 L'assèchement des libertés du fait des activités de surveillance est susceptible de transformer en profondeur l'espace public en lui retirant une fonction politique de construction du corps social ou national, laquelle repose en partie sur les comportements auquel il est renoncé. Les libertés affectées permettent en particulier la participation politique et l'activisme. De leur exercice ou de leur non-exercice dépend la vitalité d'une société démocratique. La Cour EDH l'a saisi dans son arrêt *Glukhin c.*

Russie, rendu le 4 juillet 2023, au sujet du recours à la reconnaissance faciale aux fins d'identification d'un manifestant passible d'une simple amende administrative en raison de ses modalités de manifestation dans le métro moscovite (port d'une pancarte de soutien à un opposant politique). Il n'y avait aucun besoin social impérieux à admettre la restriction de la liberté d'expression au nom de la sécurité publique[165]. L'usage de la reconnaissance faciale était en l'espèce « 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 »[166]. L'affection des régimes autoritaires pour les dispositifs technopoliciers est significative de ce point de vue[167].

45 Le mérite de la Cour EDH est, dans cet arrêt, de s'en tenir aux fondamentaux en soumettant les technologies de surveillance au triple test. Sous réserve de maturité technologique, le caractère approprié des traitements de données sera généralement satisfait ; mais la nécessité et la proportionnalité questionnent, spécialement au regard des standards d'une société démocratique. À ce stade de l'examen, l'effet dissuasif doit être intégré à l'analyse[168]. Il pèse dans la mise en balance de la finalité poursuivie et des effets engendrés. C'est ce qu'a rappelé la Haut-Commissaire aux droits de l'homme des Nations unies chargée d'évaluer les incidences des nouvelles technologies sur la promotion et la protection des droits dans le contexte des rassemblements. Hors éléments concrets attestant la commission en cours d'un délit ou d'un crime grave de nature à justifier un enregistrement ciblé, elle estimait en 2020 que le principe de proportionnalité devrait conduire les pouvoirs publics à s'abstenir d'enregistrer les participants aux rassemblements[169]. Ces conclusions s'avèrent pertinentes lorsque sont déployées des caméras aéroportées. Elles pourraient l'être également pour les systèmes de vidéoprotection. Rien n'impose, en effet, que les caméras installées soient actives et enregistrent en continu, indépendamment des évènements habituels ou exceptionnels se déroulant dans l'espace public, et indifféremment de leur temporalité[170]. Les principes de nécessité et de proportionnalité ne l'imposent pas. Considérant qu'il s'agit là d'une forme générale et systématique de surveillance, ils devraient même l'exclure, assez nettement, comme ils excluent les interdictions générales et systématiques qui résultent de l'exercice des pouvoirs de police administrative traditionnels.

46 Aux côtés de l'effet dissuasif (*chilling effect*) provoqué par la surveillance, le développement d'un autre phénomène susceptible d'alimenter la renonciation aux libertés dans l'espace public mérite une attention particulière : l'utilisation des logiciels de VSA, qui contribue à faire émerger une *légalité suspecte*. La VSA, qu'elle soit comportementale et axée sur le suivi des personnes ou qu'elle se borne à la détection en temps réel de certains évènements prédéterminés (*e.g.* VSA de la loi JOP), permet une analyse des corps. Le maillage territorial de la vidéoprotection, auquel se greffe la VSA, lui offre une portée géographique considérable pour une analyse en tout lieu. Sous réserve d'une puissance de calcul suffisante, son fonctionnement automatisé lui offre une dimension de masse. Cette analyse des corps, automatisée, de masse et en tout lieu, n'est pas complètement advenue dans l'espace public français, où se déroule néanmoins une expérimentation d'ampleur. Les arrêtés préfectoraux portant autorisation de l'emploi de la VSA édictés en Île-de-France en application de la loi JOP entre le 31 mai et le 31 août 2024 ont ainsi concerné soixante stations de métro[171], vingt-et-une gares de RER[172] et treize sites de manifestations sportives[173], sur une durée de soixante-quatre jours glissants. Ils ont permis l'enregistrement et l'analyse automatisée de plusieurs millions de corps. Au niveau juridique, la généralisation de cette expérimentation est envisagée sans pudeur par les parlementaires, les autorités de police et le

gouvernement[174]. Au niveau technologique, l'équipement généralisé des systèmes de vidéoprotection n'est aucunement un obstacle. Penser les effets d'une massification de l'analyse des corps par la VSA dans l'espace public et les transformations qu'elle induit du point de vue des droits et libertés n'a, en conséquence, rien de précipité.

47 La surveillance qui résulte de la VSA est, sans conteste, moins éclatante que l'identification biométrique en temps réel par reconnaissance faciale. Ses effets sont fréquemment euphémisés lorsque ne sont en cause que des logiciels de détection en temps réel d'évènements prédéterminés (*e.g.* présence d'objets abandonnés, port d'armes, non-respect par une personne ou un véhicule du sens de circulation commun, franchissement d'une zone interdite, présence d'une personne au sol, mouvement de foule, densité trop importante de personnes, départ de feu). Des lignes et des points sont analysés. Une alerte est transmise au centre de supervision urbain. L'opérateur humain statue sur l'opportunité d'une intervention. Il y aurait simplement une rationalisation de la surveillance, sans biométrie, et donc sans entrave excessive aux droits des administrés. Deux processus sous-jacents à ces opérations affectent pourtant l'administré. Il est, premièrement, réduit numériquement à un comportement. Il est, deuxièmement, érigé en suspect en cas d'alerte générée, en raison de son écart au regard d'une norme, d'une moyenne, non pas énoncée par une disposition juridique qui est interprétée par des autorités d'application du droit, mais par un code algorithmique qui est ignoré de l'opérateur. Indépendamment de sa légalité, un comportement qui s'écarte de cette moyenne algorithmiquement codée génère ainsi une suspicion. Cette *légalité suspecte* qui, rappelons-le, peut déclencher à elle seule une intervention et un contrôle physique, est – comme la surveillance biométrique – susceptible de conduire à des autocensures et à des modifications comportementales dans l'espace public. Pour l'exprimer trivialement : accompagnée d'un système d'affichage sur site, la VSA possède une fonction de *nudge*[175], intervention subtile et non coercitive qui exploite des biais cognitifs humains. Elle possède quoi qu'il en soit une dimension normalisatrice et disciplinaire[176].

48 Il n'est dès lors pas superflu de s'attacher aux finalités du dispositif et à son fonctionnement. Du côté des objectifs, c'est la lutte contre les actes de terrorisme et contre les atteintes graves à la sécurité des personnes qui motive son déploiement. Le but est une fois de plus légitime et touche au cœur de la sécurité publique. Du côté des moyens, la VSA s'attache aux signaux faibles et développe une approche par les risques. Le législateur l'a prévu : les lieux analysés sont ceux « particulièrement exposés à des *risques* », et non à des actes survenus ou survenant[177]. Inévitablement, la logique de prévention situationnelle implique des répercussions – que d'aucuns qualifieraient de négligeables ou modestes – tels la mise en lumière ou le ciblage de comportements anodins et légaux. Or, la VSA charrie une stigmatisation de ces comportements, puisqu'elle les singularise pour mieux les marginaliser au regard d'une norme idéale typique. Il importe de tenir compte de ces répercussions dans le cadre de l'évaluation de la proportionnalité des atteintes aux droits et libertés. L'appréciation est alors fonction des évènements prédéterminés, considérés comme suspects, que la VSA à la charge de signaler et qui varient selon les dispositifs.

49 Certains dispositifs de VSA sont entraînés pour détecter des occupations persistantes ou inertes de l'espace qui sont régulièrement perçues comme menaces à la tranquillité publique : mendicité, rassemblement de jeunes, campements. Ces comportements, licites, sont souvent imputables à des populations précaires qui dépendent de l'espace

public dans lequel s'exerce aussi leur vie privée – y compris par nécessité[178]. Dès lors, ces populations peuvent aisément être visées en qualité de « mauvais » usagers de l'espace public. Il suffit pour ce faire de paramétrer les logiciels de VSA pour qu'ils détectent les corps statiques, les personnes au sol ou certains véhicules utilisés comme résidences mobiles. Si un tel ciblage n'a rien de nouveau dans le cadre de la police administrative, la possibilité qu'il soit réalisé de manière systématique, généralisée et en temps réel, elle, l'est. L'entreprise Videtics, bien connue à Cannes, propose ainsi une VSA dont l'une des fonctionnalités est la « détection de posture »[179]. La société XXII commercialise quant à elle un logiciel de « détection de présence prolongée » à Moissy, Poissy et Versailles[180]. La solution CityVision de Wintics, implantée à Paris, Neuilly-sur-Seine, Joinville-le-Pont, Orléans, Nîmes, Nice, Strasbourg et dans plusieurs départements, propose de sécuriser l'espace public par la « détection des mauvais usages de la voirie »[181]. Les logiciels Eagle et Jaguar commercialisés par Evitech identifient plus spécialement les « arrêts fréquents », la « vitesse insuffisante ou excessive », les « silhouettes accroupies », ou encore un « temps de présence de la même silhouette dans la zone trop long »[182].

50 Sont ici visées des pratiques « à faible légitimité » dans l'espace public, notamment des pratiques « non consommatoires » qui contrastent avec les fonctionnalités souhaitées dans une ville fluide[183]. La crainte principale manifestée par les associations, en premier lieu par La Quadrature du Net, est que la définition retenue – en partie – par le secteur industriel de diverses anormalités comportementales, paramétrées consciemment, algorithmisées, et porteuses d'une conception politique marquée de l'espace public, aboutisse via la VSA à légitimer la traque d'occupations à la fois légales de cet espace public et caractéristiques de certains groupes sociaux[184]. Force est de constater que les outils de la technopolice administrative, en particulier la VSA, interfèrent avec des occupations légales de l'espace public et, ce faisant, les marginalisent, au nom de la traque de pratiques illégales. Ils contribuent ce faisant à une *substitution des normativités*, la norme juridique cédant le pas à la norme technique, au nom de la sécurité publique. La répression cède à la suspicion, la sanction à l'alerte, la causalité à la corrélation ; l'illégalité n'est plus appréciée en aval mais redoutée en amont, et l'appréciation accorde moins d'égards à l'infraction définie par le législateur qu'à l'anormalité co-déterminée par le secteur industriel[185]. Plusieurs auteurs et autrices ont largement documenté et insisté sur le fait qu'il est possible, « par une organisation appropriée de l'espace, [de] diffuser un modèle de *savoir-vivre* » car en « modifiant l'ordonnancement de l'espace on modifie les comportements »[186]. L'ordonnancement de l'espace n'est désormais plus seulement le fait des architectes et des urbanistes. Il est aussi modifié par les dispositifs techniques, numériques, qui déterminent un « savoir-vivre » ou un « savoir-être »[187].

51 À ces pratiques de VSA, déjà déployées sur le territoire, s'ajoute le dispositif singulier de la VSA expérimentée dans le cadre de la loi JOP. Les huit évènements prédéterminés qu'il incombe aux logiciels de signaler en temps réel sont différents : présence d'objets abandonnés, port d'armes, non-respect par une personne ou un véhicule du sens de circulation commun, franchissement d'une zone interdite, présence d'une personne au sol, mouvement de foule, densité trop importante de personnes, départ de feu. À première vue, on serait tenté de ne voir dans une telle liste que des critères objectifs permettant d'identifier respectivement : une bombe, une kalachnikov, une attaque à la voiture bélier, une intrusion délictuelle, une victime d'agression, une réaction collective à une attaque terroriste, une cible facile et un incendie criminel. L'analyse

des discours autour de l'adoption de la loi JOP confirme cette impression. Sans doute, les évènements prédéterminés par le décret d'application constituent des signaux faibles des catastrophes en puissance listées ci-dessus dont la survenance est redoutée de tous. Il convient néanmoins de souligner la relativité de la corrélation établie.

52 À contre-pied, un parallèle pourrait être dressé avec la détection d'autres comportements, bien moins catastrophiques, et sans doute plus récurrents dans les signalements déclenchés. Que l'on songe par exemple aux comportements proscrits au sein des centres commerciaux, ces lieux emblématiques qui, par-dessus tout, doivent être « propres, sûrs… et marchands »[188]. Dans son étude « *The Mall* », Stéphanie Hennette-Vauchez convoque les règlements intérieurs des centres commerciaux pour analyser l'interpénétration des espaces publics et privés et envisager ses implications sur l'exercice des droits et libertés. Elle reproduit *in extenso* le règlement intérieur du centre commercial parisien *Les boutiques du palais*, qu'elle considère comme un règlement intérieur « type ». La lecture croisée de ses clauses et des évènements prédéterminés qui alimentent le fonctionnement de la VSA expérimentée sur le fondement de la loi JOP nous semble éminemment instructive.

« La fréquentation de l'établissement doit s'accomplir de façon à préserver sa quiétude, ce qui implique le respect de la réglementation et exclut tout comportement agité, agressif ou choquant et tout manquement à des dispositions légales et réglementaires. Il est en particulier interdit de :	« Les évènements prédéterminés qu'un traitement algorithmique peut avoir pour objet de détecter, en ce qu'ils sont susceptibles de présenter ou de révéler un risque d'acte de terrorisme ou d'atteinte grave à la sécurité des personnes, sont les suivants :
– fumer dans l'ensemble du "mall" […] à l'exception des zones prévues à cet effet ;	– départs de feux ;
– de détenir, utiliser ou consommer des produits illicites et dangereux ;	– présence ou utilisation d'armes ;
– d'enfreindre les règles d'usages que rappellent les pictogrammes (escalators, coins repos…) ;	– non-respect par une personne du sens de circulation commun ;
– de s'installer au sol (à genoux, assis, couché…)	– présence d'une personne au sol ;
– de déposer des déchets hors des poubelles […], d'encombrer les lieux en y entreposant quoi que ce soit (vélo, paquet, valise, ou autres…) ;	– présence d'objets abandonnés ;
– d'y manifester, courir, crier, chanter […] ;	– mouvement de foule, densité trop importante de personnes ;
– d'y pratiquer des jeux ou des activités sportives en dehors de zones spécifiquement dédiées »[189].	– franchissement ou présence d'une personne dans une zone interdite ou sensible »[190].

53 La symétrie des comportements marginalisés est saisissante. Elle révèle l'ambivalence des logiciels de VSA. Les évènements prédéterminés par le décret d'application de la loi JOP constituent autant des signaux faibles des catastrophes en puissance que des

critères objectifs de manquements – y compris légaux – à des normes sociales édictées par des industriels dans des lieux conçus pour les flux et les activités marchandes. Faut-il en conclure que la VSA participe à la « migration dans d'autres espaces publics » que les centres commerciaux des normes juridiques ou techniques qui les régissent, à commencer par l'interdiction des « usages hétérodoxes » de l'espace[191] ? On ne saurait l'exclure.

54 Toujours est-il que, non contents de dissiper la sphère privée des sujets de droit dans l'espace public par la captation massive des données et les traitements biométriques, les moyens de la technopolice administrative mettent aussi à l'épreuve les libertés d'expression, de réunion, d'association, de manifestation, de circulation… en bref, les libertés jadis qualifiées de « publiques »[192]. Certains outils de surveillance génèrent un effet dissuasif d'autocensure. D'autres, plus latents, posent les jalons d'un ajustement des comportements en réaction à l'avènement d'une *légalité suspecte*. Conjointement, ces outils dessinent une dynamique de non-exercice des libertés qui entraîne l'effectivité de ces dernières sur une crête étroite. La difficulté à quantifier l'effet dissuasif, l'absence – pour le moment – de pérennisation de certains outils, comme la nature insidieuse des atteintes portées empêchent toutefois de formuler des assertions définitives quant à l'avenir desdites libertés dans l'espace public français. À tout le moins, l'ensemble des dynamiques appréhendées ci-dessus participe à la mutation de cet espace.

B/ La mutation de l'espace public : plan de libertés ou zone de contrôles

55 La conception de l'espace est directement liée au projet de société. Elle le matérialise visuellement, géographiquement, et en constitue l'un des principaux outils de perpétuation. À la fois produit et reflet de la société, support des activités humaines et du pouvoir politique, l'espace est d'abord une emprise[193]. Une fois façonné, il performe. Il réalise ces activités et ce pouvoir, les rend possibles et les détermine. En d'autres termes : « l'espace n'est pas le réceptacle indifférencié et le décor neutre des évènements constitutifs de la vie sociale », « il est lui-même simultanément producteur de social »[194]. Si la description de l'espace incarne le point de référence des sociétés, c'est parce qu'il est significatif des rapports sociaux comme des organisations politiques qui l'ont précédé et qu'il alimente. On se réfère ainsi volontiers aux espaces publics d'une société pour la définir : agora, forum, marchés, lieux de culte[195].

56 Dans le cadre d'un travail d'ampleur sur *Le concept d'espace public,* Hugo Avvenire distingue et analyse trois conceptions de l'espace public. Aux visions classiques et dominantes incarnées par les conceptions domaniale et policière, il oppose une conception libérale[196]. La conception domaniale appréhende l'espace public comme un bien d'utilité et de possession publiques. La conception policière fait primer sa fonction de vecteur spatial d'exercice du pouvoir de police, administrative et judiciaire[197]. Quant à la conception libérale, elle souligne l'intérêt particulier de l'espace public pour l'exercice régulier des libertés[198]. Si la première conception apparaît hors de propos pour l'essentiel de notre étude, les deuxième et troisième conceptions permettent d'en prolonger les réflexions.

57 Dans la conception libérale, l'espace public est avant tout envisagé comme un *plan* de libertés, c'est-à-dire à la fois comme une vaste étendue spatiale au sein de laquelle sont

exercées les libertés et comme un programme politique. Deux dimensions se détachent, en l'occurrence l'égal accès et le libre usage de cet espace. Les travaux d'Olivia Bui-Xuan et ceux de Stéphanie Hennette-Vauchez soulignent en ce sens la place prépondérante qu'occupe la finalité d'accueil du public, et donc le libre accès. Selon elles, c'est cette finalité qui confère aux espaces envisagés leur caractère public par opposition aux espaces privés[199]. Le libre accès, en soi, reflète déjà une conception de l'espace où prédomine l'exercice des libertés. Il est la première conséquence de l'exercice de la liberté de circulation *vers* cet espace, avant même qu'elle ne s'y déploie. Outre la finalité d'accueil du public et le libre accès, la conception libérale de l'espace public repose tout entière sur la liberté des usages. Au gré des boulevards, des places, des jardins, des lieux de promenades, des parcs et de leurs bancs, l'espace permet les rassemblements, les associations, les réunions, récréatives ou contestatrices ; il permet l'expression, sous forme d'échanges et de délibérations ; la manifestation de convictions, philosophiques et religieuses, individuelles ou collectives. Ces libertés ont un caractère fortement politique. La diversité comme l'intensité de leurs usages expliquent par ailleurs que les théories de la démocratie accordent à l'espace public une considération centrale[200]. Tel est le cas, en particulier, chez Jürgen Habermas[201]. Sous cet angle, l'espace public est l'horizon des libertés et la vitrine rutilante de la *res publica*.

58 La conception policière de l'espace public, telle que dépeinte par Hugo Avvenire qui en retrace la généalogie[202], insiste davantage sur d'autres fonctions. L'exercice des libertés cède à celui de la puissance publique et au maintien de l'ordre. La perspective privilégiée est celle du contrôle social. L'espace public devient avant tout terrain stratégique du pouvoir politique qui se doit d'en avoir la maîtrise. Puisque le « contrôle d'une population suppose le contrôle d'un territoire », l'espace est érigé en « dimension constitutive »[203] du pouvoir ; il est l'assise de l'*imperium*. En somme, l'ordre social dépend pour partie de l'ordre spatial. La configuration de l'espace est pensée sous l'angle de l'efficacité policière, à la fois pour surveiller et pour façonner les activités humaines. À Danièle Lochak d'ajouter : « l'efficacité du contrôle social est maximale lorsque *l'intériorisation des contraintes et l'observation spontanée* des *normes sociales dominantes* permettent de diminuer la *coercition visible* »[204]. C'est à cette dynamique que participe la technopolice administrative, police « sans contact », qui assoit un certain « savoir-être » de nature sociale – plus qu'un respect de la légalité –, le cas échéant par autocensure et renonciation aux libertés.

59 La technopolice administrative s'inscrit ainsi dans la conception policière de l'espace public. Elle le fait d'abord par l'exclusion progressive des indésirables et par la remise en cause de leur égal accès à – et de leur égale jouissance de – l'espace public[205]. Les techniques classiques de police administrative ont, à cet égard, régulièrement été sanctionnées par les juges. Des arrêtés anti-mendicité[206] aux arrêtés anti-burkini[207], en passant par les arrêtés d'interdiction de distribution de nourriture aux exilés[208], les sanctions juridictionnelles sont tombées en cadence, le plus souvent en référé. Par euphémisation des comportements devenus simples « évènements prédéterminés », la VSA permet un ciblage plus discret, et sans doute plus efficace, des indésirables, vulnérables et précaires[209].

60 La technopolice administrative s'inscrit encore dans la conception policière de l'espace public du point de vue technique, avec le développement du *quadrillage* comme outil du contrôle social et de la surveillance hiérarchique[210]. Développé par Michel Foucault, le

quadrillage est incarné par les figures du camp militaire et de la ville par temps de peste. Il repose sur l'édification de dispositifs tactiques de contrôle d'espaces stratégiques[211]. De nos jours, la presque centaine d'arrêtés périmétriques adoptés au cours de l'été 2024 lors des Jeux olympiques et paralympiques réalise ce quadrillage, avec une ville sous pleine maîtrise policière, où les contrôles sont exacerbés, une ville militarisée[212]. Les arrêtés instituant les périmètres de protection prévus par l'article L. 226-1 du CSI limitent la circulation des personnes, permettent les vérifications, inspections visuelles, fouilles de bagages, visite de véhicules et palpations de sécurité. À ces incarnations physiques, s'ajoutent les outils de la technopolice administrative. Ils rendent possible un quadrillage bien plus diffus, quasiment immatériel[213]. Celui-ci vise moins la discipline d'exception par l'édification de camps que la surveillance généralisée des personnes et de l'espace[214]. Le maillage territorial des systèmes de vidéoprotection en constitue l'incarnation paroxystique[215]. Les périmètres de survol des caméras aéroportés alimentent aussi cette transformation pour un zonage et des contrôles croissants mais plus discrets. Depuis les centres de supervision urbains, comme depuis la tour centrale du Panoptique de Jérémy Bentham, « lieu de convergence pour ce qui doit être su », « on voit tout, sans être jamais vu » ; dans l'espace public comme dans l'anneau périphérique, « on est totalement vu sans jamais voir »[216]. La « surveillance [est] permanente dans ses effets, même si elle est discontinue dans son action », et le citoyen « reprend à son compte les contraintes du pouvoir ; il les fait jouer spontanément sur lui-même »[217].

61 Au bout du compte, la technopolice administrative contribue aux transformations de l'espace public et renforce sa conception policière. Même invisible, elle participe de manière décisive à l'ordre spatial, à l'ordre social. Du point de vue des libertés, elle fait courir le risque d'une dévitalisation de l'espace public puisqu'elle accroît considérablement – mais discrètement – sa mutation en un espace disciplinaire. L'ensemble est réalisé dans le cadre de la prévention situationnelle qui déséquilibre la conciliation entre droits et libertés d'une part, et sécurité publique de l'autre, au profit de cette dernière. À mesure que l'emprise de cette doctrine s'étend, le régime juridique de garantie des droits et libertés accentue son volet préventif, au détriment de leur effectivité. Pas à pas, et très prosaïquement, l'immobilisme de deux personnes sur un banc passe d'une présomption de romantisme ou d'amitiés à une suspicion de *deal*. Reste à savoir si les pouvoirs publics, en premier lieu le législateur, après avoir envisagé – et après avoir été manifestement séduit par – le plein potentiel de la technopolice administrative, seront indifférents aux mutations engagées ou, à l'inverse, seront épris d'une nostalgie libérale, et, à nouveau, des *bancs publics*[218]...

NOTES

1. Conclusions du commissaire du gouvernement L. Corneille sous CE, 10 août 1917, *Baldy,* n° 59855, *in Recueil des arrêts du Conseil d'État statuant au contentieux des décisions du Tribunal des conflits et de la Cour des comptes,* Paris, Librairie de la société du recueil Sirey, t. 87, 2e série, 1917, p. 640.

2. De vifs remerciements s'imposent pour Hugo Avvenire, Xavier Dupré de Boulois, Béatrice Guillaumin, Stéphanie Hennette Vauchez et Serge Slama. Leurs relectures critiques et leurs commentaires ont utilement permis d'améliorer ce travail.

3. Par exemple, Manuel Valls : « La sécurité est la première des libertés. C'est pour cette raison que d'autres libertés ont été ou peuvent être temporairement limitées » (*Déclaration sur les grandes orientations du projet de loi prorogeant l'état d'urgence et modernisant le régime d'exception de la loi du 3 avril 1955,* Assemblée nationale, 19 novembre 2015). D'un point de vue littéraire, l'oxymore caractéristique de la formule peut être rapproché du deuxième slogan du Parti dans le célèbre roman *1984* de George Orwell : « La liberté c'est l'esclavage ». L'ancien Premier ministre avait d'ailleurs répété l'hommage à la novlangue (*Newspeak*) au sujet des premier et troisième slogans du Parti d'Océania, à savoir : « La guerre c'est la paix » (« Nous sommes en paix et, en même temps, nous vivons en guerre », *Déclaration sur les principes et les grandes lignes de l'action du gouvernement en 2016,* 28 janvier 2016) et « L'ignorance c'est la force » (« Expliquer, c'est déjà vouloir un peu excuser », *Déclaration sur la lutte contre le terrorisme et l'antisémitisme,* 9 janvier 2016).

4. V. not. art. 2 de la DDHC et art. 5 de la Convention EDH.

5. M.-A. Granger, « Existe-t-il un "droit fondamental à la sécurité" ? », *RSC*, 2009, p. 273 et s. ; V. Champeil-Desplats, « Les enjeux normatifs de la fondamentalisation du droit à la sécurité », *in* M. Touillier (dir.), *Le Code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre*, Paris, Dalloz, 2017, p. 81 et s. ; X. Dupré de Boulois, « Existe-t-il un droit fondamental à la sécurité ? », *RDLF,* chron. n° 13, 2018 ; V. Champeil-Desplats, « L'autonomisation relative des références à la sécurité dans les décisions du Conseil constitutionnel », *Jus Politicum,* n° 21, 2018, p. 271-284.

6. Art. 4 de la DDHC.

7. Not. droit au procès équitable, droit au respect de la vie privée, liberté de pensée, de conscience et de religion, liberté d'expression, liberté d'association et de réunion, liberté de circulation. V. art. 6, 8, 9, 10 et 11 de la Convention EDH, art. 2 du protocole additionnel n° 4 à la Convention EDH, art. 12, 14, 17, 19, 21 et 22 du PIDCP.

8. Pour une définition du phénomène, à savoir l'équipement et la mobilisation croissante de dispositifs technologiques – en particulier numériques – aux fins d'exercice des missions de police administrative, et une cartographie de ses principaux outils, nous renvoyons le lecteur au site internet de la campagne « Technopolice » et au premier volet de cette série d'études : R. Medard Inghilterra, « L'instauration d'une "technopolice" administrative en milieu urbain : cadre et enjeux juridiques », *RevDH,* n° 25, 2024. Sur la provenance du concept, v. en particulier § 6-7, y compris note 17. À noter la parution prochaine d'un important ouvrage sur le sujet, signé d'un membre actif de la campagne « Technopolice » : F. Tréguer, *Technopolice. La surveillance policière à l'ère de l'intelligence artificielle,* Quimperlé, Éditions divergences, octobre 2024, 200 p.

9. Pour une analyse détaillée de ce test et de son application par le juge administratif, v. not. C. Roulhac, « La mutation du contrôle des mesures de police administrative – Retour sur l'appropriation du "triple test de proportionnalité" par le juge administratif », *RFDA,* 2018, p. 343-356.

10. CE, Ass., 26 octobre 2011, *Association pour la promotion de l'image*, n° 317828, Lebon ; moindrement, pour une simple conciliation entre ordre public et libertés, CE, Ass., 19 mai 1933, *Benjamin,* n° 17413, Lebon.

11. Art. 4, 3° de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après LIL) : « Les données à caractère personnel doivent être : [...] 3° Adéquates, pertinentes et, au regard des finalités pour lesquelles elles sont traitées, limitées à ce qui est nécessaire ou, pour les traitements relevant des titres III et IV, non excessives ».

12. Art. 4, 2° et 5° de la LIL : « Les données à caractère personnel doivent être : [...] 2° Collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement

d'une manière incompatible avec ces finalités ; [...] 5° Conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ».

13. Art. 88 de la LIL, applicable lorsque le traitement vise la prévention ou la détection des infractions pénales, la protection contre les menaces pour la sécurité publique et la prévention de ces menaces.

14. CC, Décision n° 2021-817 DC, 20 mai 2021, *Loi pour une sécurité globale préservant les libertés,* § 141 (censure pour tous les services), puis CC, Décision n° 2021-834 DC, 20 janvier 2022, *Loi relative à la responsabilité pénale et à la sécurité intérieure,* § 138 (censure pour les seuls services de police municipale).

15. TA Orléans, 12 juillet 2024, *LQDN c. commune d'Orléans,* n° 2104478.

16. TA Marseille, 27 février 2020, *LQDN c. conseil régional de PACA,* n° 1901249.

17. Parfois de manière seulement temporaire, comme pour le recours aux drones par les services nationaux, d'abord censuré (CC, Décision n° 2021-817 DC, 20 mai 2021), puis entériné (CC, Décision n° 2021-834 DC, 20 janvier 2022).

18. G. Gormand, *Évaluation de la contribution de la vidéoprotection de voie publique à l'élucidation des enquêtes judiciaires,* étude n° 31300102, CREOGN, septembre 2021, document de synthèse, p. 10.

19. Exploitation du matériel et extraction complexes des images en l'absence de déport, qualités inégales des images, angles incomplets des prises de vues, défaut d'éclairage, pluralité des logiciels d'exploitation pour une même zone vidéoprotégée, identification délicate des responsables du traitement, réquisition des images avant écrasement, détermination de la plage horaire de la séquence souhaitée, délimitation des zones à visionner, objectifs des caméras détériorés ou salis. En ce sens, v. not. : *idem* ; F. Castagnino, « Rendre "intelligentes" les caméras : déplacement du travail des opérateurs de vidéosurveillance et redéfinition du soupçon », working paper, Science Po Cities & Digital Technology Chair, n° 5, 2019 ; C. Gosselin, « La sécurité à l'heure de l'intelligence artificielle », note rapide de l'Institut Paris région, n° 833, février 2020, p. 2 ; L. Mucchielli, *Vous êtes filmés ! Enquête sur le bluff de la vidéosurveillance,* Malakoff, Armand Colin, 2018, 228 p., not. p. 84-86.

20. À l'étranger, v. E. L. Piza & al., « CCTV Surveillance for Crime Prevention. A 40-Year Systematic Reviexw With Meta-Analysis », *Criminology and Public Policy,* vol. 18, n° 1, 2019. En France, v. not. L. Mucchielli, *Vous êtes filmés ! Enquête sur le bluff de la vidéosurveillance, op. cit.,* not. p. 117-119, p. 135-144 et p. 176-177 ; L. Mucchielli, « À quoi sert la vidéosurveillance de l'espace public ? », *Déviance et société,* vol. 40, 2016, p. 25-50 ; L. Mucchielli, « De la vidéosurveillance et de la vidéoverbalisation : usages réels et fantasmés d'une technologie moderne », *Archives de politiques criminelles,* n° 38, 2016, p. 249-264.

21. G. Gormand, *L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de surveillance de la ville de Montpellier*, thèse dactyl., Université Grenoble Alpes, 2017, p. 332.

22. Panel de 1939 enquêtes, réparties sur quatre ans (2017-2020, inclus), pour quatre types d'infractions (violences, vols liés aux véhicules, cambriolages et infractions à la législation sur les stupéfiants) : G. Gormand, *Évaluation de la contribution de la vidéoprotection de voie publique à l'élucidation des enquêtes judiciaires, op. cit.,* not. p. 8 et 12. V. aussi, pour un constat encore moins favorable dans trois cas d'étude, incluant la ville de Marseille, L. Mucchielli, *Vous êtes filmés ! Enquête sur le bluff de la vidéosurveillance, op. cit.,* not. p. 114-117, p. 145-149, p. 165-170 et p. 174-177.

23. E. Lemaire, *L'œil sécuritaire. Mythes et réalités de la vidéosurveillance*, La Découverte, 2019, not. p. 107 à 194.

24. Cour des comptes, *Les polices municipales,* rapport public thématique, 2020, p 70. La Cour des comptes poursuivait (p. 71) : ce constat impose « une appréciation objective de l'efficacité de la vidéoprotection ». Pour une recommandation similaire dans le cas spécifique du plan de

vidéoprotection de la préfecture de police de Paris, v. Cour des comptes, référé du 2 décembre 2021 relatif au plan de vidéoprotection de la préfecture de police de Paris, S2021-2194.

25. Par ex. Chambre régionale des comptes de Rhône-Alpes, *Rapport d'observations définitives. Ville de Lyon. Sécurité publique,* 25 mai 2010, p. 48 : « en l'état actuel des données, relier directement l'installation de la vidéosurveillance et la baisse de la délinquance est pour le moins hasardeux ». Pour un bilan plus complet et convergent des constats posés par les chambres régionales des comptes, y compris à Nice (« il est difficile de lier la baisse de la délinquance à la seule présence de ce dispositif »), v. L. Mucchielli, *Vous êtes filmés ! Enquête sur le bluff de la vidéosurveillance, op. cit.,* p. 97-103.

26. CNIL, Délibération n° 2011-011 du 26 janvier 2021 portant avis sur une proposition de loi relative à la sécurité globale, p. 2 : « l'efficacité de ces systèmes au regard des objectifs légitimes d'ordre et de sécurité publics n'[ont] jamais été rigoureusement évaluée de façon globale ».

27. Assemblée nationale (P. Gosselin et P. Latombe), *Rapport d'information sur les enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité,* n° 1089, 12 avril 2023, not. p. 51.

28. V. not. L. Mucchielli, *Vous êtes filmés ! Enquête sur le bluff de la vidéosurveillance, op. cit.,* p. 73-75.

29. Au sens de l'article L. 251-2 du Code de la sécurité intérieure (ci-après CSI).

30. CAA Nantes, 9 novembre 2018, *Commune de Ploërmel,* n° 17NT02743.

31. CNCDH, Avis sur la surveillance de l'espace public, A-2024-5, 20 juin 2024, not. p. 7-14 : « réaffirmer les exigences de nécessité et de proportionnalité ». En ce sens, v. aussi LQDN, *Projet de loi relatif aux Jeux Olympiques et Paralympiques de 2024 : dossier d'analyse de la vidéosurveillance automatisée,* février 2023, p. 28.

32. Déjà, en 2011, pour la Cour de comptes : « les modalités d'autorisation de l'installation des systèmes de vidéosurveillance de la voie publique ne sont pas toujours conformes aux textes en vigueur. Les préfets remplissent imparfaitement leurs missions quand ils autorisent l'installation de systèmes de vidéosurveillance de la voie publique sans appliquer de façon rigoureuse toutes les dispositions prévues » ; « Les commissions départementales de vidéoprotection, du fait de leurs conditions de fonctionnement, n'exercent qu'un contrôle formel sur la conformité des projets présentés aux textes législatifs et réglementaires. Faute de moyens, elles ne peuvent pas non plus exercer leur pouvoir de contrôle *a posteriori* prévu par la loi. Il en résulte qu'en ce qui concerne le respect de cette conformité, la fiabilité du régime d'autorisation repose entièrement sur la bonne foi des pétitionnaires » (Cour des comptes, *L'organisation et la gestion des forces de sécurité publique,* rapport public thématique, juillet 2011, p. 150-151). Sur le contrôle de la CNIL, v. *infra.*

33. Dès 2020, la CNIL pointait en complément le risque de « créer un phénomène d'accoutumance et de banalisation de technologies intrusives » (CNIL, Délibération 2020-136 du 17 décembre 2020 portant avis sur un projet de décret relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports).

34. Pour un travail approfondi dans cette optique, v. H. Avvenire, *Le concept d'espace public. Contribution à une théorie de la spatialisation du régime des libertés,* thèse dactyl., Université Toulouse Capitole, 2022, 707 p. V. aussi B. Auby, « L'espace public comme notion émergente du droit administratif », *AJDA,* 2021, p. 2565 ; O. Bui-Xuan, « Propos introductifs », *in* O. Bui-Xuan (dir.), *Droit et espace(s) public(s),* Paris, IFJD, 2013, p. 7-16.

35. O. Bui-Xuan, « L'espace public : l'émergence d'une nouvelle catégorie juridique ? », *RFDA,* 2011, p. 551 et s. L'auteure apporte toutefois à la question ainsi soulevée une réponse négative argumentée.

36. V. art. 2 de la loi n° 2010-1192 du 11 octobre 2010 interdisant la dissimulation du visage dans l'espace public et circulaire du 2 mars 2011 relative à la mise en œuvre de la loi n° 2010-1192 du 11 octobre 2010. Pour une critique du contenu assigné par le législateur français et le pouvoir

réglementaire d'application à cette notion juridique, v. *ibidem* Comme plusieurs auteurs l'ont déjà amplement souligné, peu importe le régime de propriété, l'espace public ne se confond pas avec le domaine public.

37. Not. P. Yolka, « Les espaces publics. Libre propos au temps du Covid », *RDLF,* chron. n° 1, 2022 ; O. Bui-Xuan, « L'espace public saisi par le droit » *in* A. Fleury et F. Guérin-Pace (dir.), *Les espaces publics urbains. Penser, enquêter, fabriquer*, Presses universitaires François-Rabelais, p. 73-86, 2022 ; O. Bui-Xuan (dir.), *Masques sanitaires et droit(s),* Paris, Institut francophone pour la démocratie, 2021, 276 p. ; C. Froger, « Manifestation des opposants à la vaccination obligatoire contre la Covid-19 en Nouvelle-Calédonie : interdire ou ne pas interdire pendant l'état d'urgence sanitaire ? », *RDLF,* chron. n° 33, 2021 ; S. Slama, « Les impasses juridiques du pass sanitaire », *RDLF,* chron. n° 26, 2021 .

38. S. Hennette-Vauchez, « *The Mall* », *RFDA,* p. 833 et s.

39. V. déjà en 2013 L. Cluzel-Métayer, « Espace public et vidéoprotection », *in* O. Bui-Xuan (dir.), *Droit et espace(s) public(s), op. cit.*, p. 165-175.

40. R. Medard Inghilterra, « L'instauration d'une "technopolice" administrative en milieu urbain : cadre et enjeux juridiques », *loc. cit.*

41. S. Hennette-Vauchez, « *The Mall* », *loc. cit.*

42. Cette terminologie est empruntée à Caroline Lequesne Roth et Jonathan Keller *in* C. Lequesne Roth et J. Keller, *Surveiller les foules. Pour un encadrement des IA "physiognomoniques"*, livre blanc pour l'Observatoire de l'éthique publique, 2023, p. 31.

43. Pour une approche complémentaire des technologies de surveillance, notamment relative aux dysfonctionnements technologiques, aux lacunes des instruments juridiques applicables et à l'esquisse d'un régime de redevabilité adapté, nous renvoyons aux travaux restitués *in ibidem*.

44. Sur la partition des espaces, la relation entre espace privé et sphère privée, leur sanctuarisation initiale vis-à-vis de l'espace public, puis l'affaiblissement des frontières entre espaces, le lecteur trouvera d'utiles éclaircissements *in* F. Saint-Bonnet, « La liberté des Modernes et la partition de l'espace »*, in Revue Droit & Philosophie*, n° 7, 2015, p. 11-26 et C. Roynier, « ''A man's house is his castle'' : protection de l'intérieur et bien public », *in Droit & Philosophie*, n° 7, 2015, p. 31-46.

45. L'élaboration de la Convention 108 du Conseil de l'Europe, distincte de l'art. 8 de la Convention EDH, ainsi que la séparation des art. 7 et 8 au sein de la Charte des droits fondamentaux de l'Union européenne, l'illustrent. En ce sens, v. FRA, *Handbook on European data Protection Law,* Luxembourg, Office des publications de l'Union européenne, 2018, p. 19.

46. Art. 4 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après RGPD).

47. 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.

48. Art. 4 de la LIL.

49. Lorsque le traitement tombe dans le champ d'application du RGPD et qu'il « est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ». Art. 6 et 21 du RGPD.

50. Lorsque le traitement tombe dans le champ d'application du Titre III de la LIL, soit les « traitements de données à caractère personnel mis en œuvre, 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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, par toute autorité publique compétente ». Art. 87 et 110 de la LIL.

51. Pour un équivalent fonctionnel du droit d'opposition en droit du Conseil de l'Europe, fondé sur cette justification d'une mainmise du sujet sur ses données, v. Cour EDH, GC, 17 octobre 2019, *Lopez Ribalda et autres c. Espagne*, req. n° 1874/13 et 8567/13, § 66.

52. Courrier du directeur de la conformité de la CNIL, émis le 11 juin 2020 au sujet de l'expérimentation de la VSA par l'entreprise Datakalab et la RATP dans la station de métro de Châtelet à Paris.

53. Association nationale de la vidéoprotection (AN2V), *« Quel cadre juridique pour nos technologies de sûreté [sic] ? ». Synthèse des discussions,* compte-rendu de la réunion du 19 octobre 2022, p. 11 (nous soulignons).

54. Décret n° 2021-269 du 10 mars 2021 relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports, art. 1 : « En application du paragraphe 1 de l'article 23 du règlement (UE) 2016/679 du 27 avril 2016 susvisé, les droits d'accès, de rectification, d'opposition ainsi que les droits à l'effacement et à la limitation prévus aux articles 15, 16, 17, 18 et 21 de ce même règlement ne s'appliquent pas à ce traitement ».

55. Art. 9 de la loi JOP n° 2023-380 du 19 mai 2023, modifiant l'art. L. 251-1 du CSI.

56. Décret n° 2023-1102 du 27 novembre 2023 portant application des articles L. 251-1 et s. du CSI, v. art. 3 portant création de l'art. R. 253-6 du CSI : « V.-Le droit d'opposition prévu à l'article 21 du règlement (UE) 2016/679 du 27 avril 2016 précité et aux articles 110 et 117 de la loi n° 78-17 du 6 janvier 1978 précitée ne s'applique pas aux traitements ». V. également art. R. 242-13, II.

57. Décret n° 2023-828 du 28 août 2023 relatif aux modalités de mise en œuvre des traitements algorithmiques sur les images collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs, art. 10 : « III. - Conformément à l'article 23 du même règlement, le droit d'opposition ne s'applique pas au présent traitement ».

58. Art. 23 du RGPD : « Le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter la portée » du droit d'opposition « lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir : a) la sécurité nationale ; b) la défense nationale ; c) la sécurité publique ; d) la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ».

59. Art. 110 de la LIL : le droit d'opposition ne s'applique pas « lorsque le traitement répond à une obligation légale » ou lorsque ce droit « a été écarté par une disposition expresse de l'acte instaurant le traitement ».

60. Art. 10 de la Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité.

61. Art. L. 252-5 du CSI.

62. CNIL – LINC, *La plateforme d'une ville. Les données personnelles au cœur de la fabrique de la smart city,* Cahier IP Innovation & Prospective, n° 5, 2018, p. 39 : « Les améliorations des systèmes dits de "vidéosurveillance intelligents" sont présentés comme permettant de rendre plus aisées et rapides ces phases d'identification : soit par l'amélioration des performances intrinsèques du dispositif, soit par une plus grande capacité à mettre en relation différentes sources de captation. Dans cette logique, il pourrait être cohérent que les durées de conservation soient réduites d'autant que les améliorations des technologies les rendent plus efficaces dans leurs traitements ».

63. Art. 10 de la loi JOP : « IX. - Afin d'améliorer la qualité de la détection des évènements prédéterminés par les traitements mis en œuvre, un échantillon d'images collectées, dans des conditions analogues à celles prévues pour l'emploi de ces traitements, au moyen de systèmes de

vidéoprotection [...] peut être utilisé comme données d'apprentissage pendant une durée strictement nécessaire, de douze mois au plus à compter de l'enregistrement des images ». V. aussi art. 5 et 8 du décret n° 2023-828 du 28 août 2023.

64. Les réponses des délégués à la protection des données de la RATP et de la Préfecture de police de Paris que nous avons reçues après demandes d'accès écartent toute transmission de données enregistrées à ces sociétés.

65. Art. 10 de la loi JOP.

66. V. ici la réponse obtenue par David Libeau à une demande CADA : CADA, Avis n° 20242928 du 4 juillet 2024 [URL : https://dl.dav.li/Avis-CADA-20242928.pdf]. À cette date, préalable à l'essentiel du déploiement de la VSA de la loi JOP, la Commission prenait acte de la réponse du ministère de l'Intérieur déclarant ne pas avoir pour le moment constitué les échantillons.

67. De manière proche, v. récemment le décret n° 2024-901 du 7 octobre 2024 portant injonction, au regard de la menace grave et actuelle contre la sécurité nationale, de conservation pour une durée d'un an de certaines catégories de données de connexion.

68. Art. 104 à 106 de la LIL.

69. Concernant la pratique de la préfecture de police de Paris, v. TA Paris, ord. 5 mai 2020, *LQDN et LDH c. préfet de police de Paris,* n° 2006861, cons. 4. Concernant la pratique de la gendarmerie départementale de Haute-Garonne et du commissariat de Cergy-Pontoise, v. CNIL, Délibération SAN 2021-003 du 12 janvier 2021, cons. 20.

70. Sur la tendance récurrente des autorités normatives à réagir en réaction à des pratiques de technopolice administrative ayant émergé sans base légale expresse pour, *in fine,* entériner ces pratiques, nous renvoyons le lecteur au premier volet de la série d'études : R. Medard Inghilterra, « L'instauration d'une "technopolice" administrative en milieu urbain : cadre et enjeux juridiques », *op. cit*.

71. CE, avis, 20 septembre 2020, n° 401214, v. not. cons. 5.

72. Art. L. 242-3 du CSI. Sur la constitutionnalité de cette disposition, v. CC, Décision n° 2021-834 DC, 20 janvier 2022, *Loi relative à la responsabilité pénale et à la sécurité intérieure,* cons. 22 à 39.

73. Décret n° 2023-283 du 19 avril 2023 relatif à la mise en œuvre de traitements d'images au moyen de dispositifs de captation installés sur des aéronefs pour des missions de police administrative. Le décret d'application réitérait la précaution en créant un art. R. 242-13 au sein du CSI : « L'information du public sur l'emploi des caméras installées sur des aéronefs est délivrée par tout moyen approprié ».

74. Tel que précisé *in* CNIL, Délibération n° 2023-027 du 16 mars 2023 portant avis sur un projet de décret portant application des art. L. 242-1 et s. du CSI et *in* CE, ord., 24 mai 2023, *ADELICO et autres*, n° 473547, cons. 17.

75. *Ibidem.*

76. *Ibidem.*

77. En méconnaissance de l'article 104 de la LIL. *A contrario,* de telles mentions figurent dans les arrêtés préfectoraux portant autorisation de l'emploi d'un traitement algorithmique des images issues d'un système de vidéoprotection. Soulignons que les préfectures ne se prévalent pas dans la motivation des arrêtés de la clause de limitation des droits prévue à l'article 107 de la LIL. Elles ne remplissent dès lors pas les conditions nécessaires à son déclenchement (not. « ces restrictions sont prévues par l'acte instaurant le traitement »). La mention à l'art. R. 243-13 du CSI selon laquelle « les droits d'accès, de rectification, d'effacement et à la limitation des données s'exercent directement auprès du responsable des traitements » ne semble pas suffisante à l'effectivité des dispositions de l'article 104 de la LIL.

78. Pour une illustration, v. arrêté n° 2024-01179 du 9 août 2024.

79. Pour une illustration, v. arrêté n° 2024-00629 du 15 mai 2024 (pour la version publiée sur le site de la préfecture).

80. *E.g.* arrêtés n[os] 2024-00959 du 11 juillet 2024, 2024-01026 du 17 juillet 2024, 2024-01051 du 20 juillet 2024, 2024-01079 du 23 juillet 2024, 2024-01101 du 25 juillet 2024, BPA 2024-498 du 31 juillet 2024, 2024-01153 du 4 août 2024, 2024-01280 du 26 août 2024, 2024-01285 du 27 août 2024, 2024-01286 du 27 août 2024.

81. *E.g.* arrêtés n[os] 2024-00949 du 10 juillet 2024, 2024-00955 du 10 juillet 2024, 2024-00977 du 12 juillet 2024, BPA 2024-499 du 31 juillet 2024, BPA 2024-497 du 31 juillet 2024, 2024-01145 du 1[er] août 2024, BPA 2024-501 du 2 août 2024, 2024-01151 du 3 août 2024, 2024-01158 du 6 août 2024, 2024-01179 du 9 août 2024, 2024-01200 du 13 août 2024, 2024-01244 du 21 août 2024.

82. Arrêté n° 2024-01194 du 10 août 2024.

83. Pour des arrêtés publiés moins de 24 heures avant leur date annoncée d'effet, v. par ex. : arrêtés n[os] 2024-0701 du 31 mai 2024, 2024-00948 du 10 juillet 2024, 2024-1165 du 27 août 2024. Pour des arrêtés publiés le jour de la date annoncée de leur entrée en vigueur, v. par ex : arrêtés n[os] 2024-00847 du 20 juin 2024, 2024-00959 du 11 juillet 2024. Pour des arrêtés publiés *a posteriori,* v. par ex. arrêtés n[os] 2024-1073 du 25 juillet 2024, 2024-1081 du 25 juillet 2024.

84. Indépendamment de la question de l'assimilation des données à des biens d'appropriation, de leur patrimonialisation et de la monétisation comme conséquences d'une reconnaissance formelle d'un droit de propriété du « titulaire » sur celles-ci. Sur le sujet, v. not. M. Bernelin, « La patrimonialisation des données personnelles : entre représentation(s) et réalité(s) juridiques », *JCP,* n° 46, 2019, p. 2034-2041 ; C. Deschanel, « L'instauration d'un droit de propriété des données personnelles : vrai danger ou fausse utilité ? », *Revu Lamy Droit de l'Immatériel,* n° 156, février 2019.

85. Pour d'autres atteintes (*e.g.* principe de minimisation) engendrées par l'expérimentation de la VSA, v. en complément L. Cluzel-Métayer, « L'IA au service de la vidéosurveillance : pour et par-delà les Jeux », *in* S. Boussard, L. Folliot Lalliot et F. Latty (dir.), *L'organisation des Jeux olympiques et paralympiques de Paris 2024 : questions de droit public,* Paris, Dalloz, 2024, p. 294.

86. Sur le sujet, v. L. Chagnon, « "Elle fait de moins en moins peur" : peu de moyens, peu de sanctions… La CNIL protège-t-elle bien vos données personnelles ? », *France Info,* 23 août 2024.

87. Limite déjà dénoncée not. *in* CNCDH, Avis sur la surveillance de l'espace public, *op. cit.*, p. 17 ; L. Cluzel-Métayer, « L'IA au service de la vidéosurveillance : pour et par-delà les Jeux », *op. cit.*, p. 297.

88. Pour un plaidoyer relatif à l'élaboration d'AIPD à intervalles réguliers, par des entités indépendantes, et tenant compte du point de vue des sujets du traitement, v. Conseil de l'Europe, *Lignes directrices sur la reconnaissance faciale,* 2021, p. 25.

89. *E.g.* expérimentation à Roland-Garros en 2020 de plusieurs dispositifs d'authentification du corps arbitral, de détection par VSA des mouvements de foule, de contrôle d'accès du personnel accrédité et de comptage de personnes, mis en œuvre par le Secrétariat général de la défense et de la sécurité nationale – sans avis de la CNIL, informée tardivement. En ce sens, v. aussi C. Lequesne Roth et J. Keller, *Surveiller les foules. Pour un encadrement des IA "physiognomoniques"*, *op. cit.*, p. 72.

90. CNIL, « Analyse d'impact relative à la protection des données : publication d'une liste des traitements pour lesquels une analyse est requise », 6 novembre 2018. V. aussi *idem,* p. 70.

91. Art. 36 du RGPD et art. 63 et 90 de la LIL. V. en ce sens, pour la seule vidéoprotection : Cour des comptes, *Rapport sur les polices municipales*, 2020, p. 63.

92. « Logiciel de vidéosurveillance : la CNIL lance une "procédure de contrôle" visant le ministère de l'intérieur », *Le Figaro / AFP,* 15 novembre 2023.

93. Audience de référé précédant CE, ord., 21 décembre 2023, *Communauté de communes Cœur Côte Fleurie,* n° 489990.

94. Art. 31 et 89 de la LIL.

95. CNIL, *Rapport annuel 2023,* avril 2024, p. 10.

96. Pour un même constat, v. CNCDH, Avis sur la surveillance de l'espace public, *op. cit.*, p. 10.

97. CC, Décision n° 2021-834 DC, 20 janvier 2022, *Loi relative à la responsabilité pénale et à la sécurité intérieure,* § 27 : l'autorisation de survol ne saurait, « sans méconnaître le droit au respect de la vie privée, être accordée qu'après que le préfet s'est assuré que le service ne peut employer d'autres moyens moins intrusifs au regard de ce droit ou que l'utilisation de ces autres moyens serait susceptible d'entraîner des menaces graves pour l'intégrité physique des agents ».

98. C. Le Foll, « En Île-de-France, la police s'autorise à déployer des drones plus d'un jour sur deux », *Mediapart,* 1er mars 2024 ; V. Stoquer, « A Paris, les drones de la police autorisés à survoler la capitale en moyenne un jour sur deux », *Libération,* 15 août 2024.

99. TA Paris, *LQDN et LDH c. préfet de police de Paris, op. cit.*, TA Lille, ord., 29 novembre 2023, *Ligue des droits de l'homme et autres,* nos 231013 et 2310163.

100. Not. CJUE, 11 décembre 2014, *František Ryneš*, aff. C-212/13.

101. Not. art. L. 251-1 du CSI et ministère de l'Intérieur et des Outre-mer, instruction du 20 mars 2024, NOR : IOMD2405307J, p. 16.

102. M. Mauss, *Essai sur le don,* Paris, PUF, 1950.

103. M. Fourcade & D. N. Kluttz, « A Maussian bargain : Accumalation by gift in the digital economy », *Big Data & Society,* 2020, p. 1-16.

104. C. Lequesne Roth, « La fin de l'anonymat : reconnaissance faciale et droit à la vie privée », *Dalloz IP/IT,* 2021, p. 309-313.

105. En ce sens, v. Comité européen pour la protection des données (CEPD), *Lignes directrices 3/2019 sur traitements de données à caractère personnel par des dispositifs vidéo*, V2, janvier 2020, p. 19-20.

106. Art. 4 du RGPD.

107. Sur le sujet, v. not. M. Sztulman, *La biométrie saisie par le droit public. Étude sur l'identification et la localisation des personnes physiques,* Paris, LGDJ, 2019, 468 p.

108. Pour une appréhension de l'anonymat en droit des données à caractère personnel par le Conseil d'État, v. CE, 8 février 2017, *Société JCDecaux France*, n° 393714, cons. 7 et 8. Sur la confusion fréquente entre anonymisation et pseudonymisation, v. CNIL – LINC, *La plateforme d'une ville. Les données personnelles au cœur de la fabrique de la smart city, op. cit.*, p. 13-14. Sur le risque d'une désanonymisation des données par le recours croissant à l'IA, v. Commission européenne, *Livre blanc. Intelligence artificielle. Une approche européenne axée sur l'excellence et la confiance,* 19 février 2020, COM 2020) 6 final, p. 14.

109. Sur ces questions, v. not. les travaux de Caroline Lequesne Roth, « La reconnaissance faciale dans l'espace public : bilan et perspectives européennes », entretien, *Dalloz IP/IT*, n° 6, 2020, p. 332-335 ; « Pour un encadrement démocratique de la reconnaissance faciale », *Recueil Dalloz,* 2020, n° 27, p. 1568 ; « La fin de l'anonymat : reconnaissance faciale et droit à la vie privée », *op. cit.*, p. 309-313 ; « Rapport du Conseil de l'Europe sur la reconnaissance faciale », *Dalloz IP/IT*, n° 6, 2021, p. 361-363 ; « Reconnaissance faciale, le temps de la redevabilité ? », *Recueil Dalloz,* 2022, n° 24, p. 1256.

110. Art. 5, 1, h) du Règlement IA. En cas de menace pour la vie ou la sécurité physique des personnes, la menace doit être « spécifique, substantielle et imminente ». Lorsqu'est visée une menace d'attaque terroriste, celle-ci doit être « réelle et actuelle » ou « réelle et prévisible ».

111. V. par ex. Sénat (M-P. Daubresse, A. Belenet et J. Durain), *Rapport d'information n° 627 fait au nom de la Commission des lois sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles*, 10 mai 2022, p. 52 ; Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Guidelines on Facial Recognition*, 2021, p. 5 ; Cour EDH, *Glukhin c. Russie*, req. n° 11519/20, § 82 (« La nécessité de garanties est d'autant plus forte lorsqu'il est question du recours à une technologie de reconnaissance faciale à la volée »).

112. Défenseur des droits (DDD), *Technologies biométriques : l'impératif respect des droits fondamentaux,* rapport thématique, 2021, p. 8 : « Il convient ainsi de distinguer les technologies

dites actives où l'individu fournit volontairement des informations (par exemple, en plaçant son doigt sur un dispositif de contrôle) des technologies passives où les informations biométriques sont détectées, parfois à l'insu de la personne concernée ».

113. Wired, « Cops Have a Database of 117M Faces. You're Probably in It », 18 octobre 2016 ; Wired, « China Is the World's Biggest Face Recognition Dealer », 24 janvier 2023.

114. Parmi les données contenues dans le fichier TES figurent, entre autres : le nom, le prénom, la date et le lieu de naissance, le sexe, la couleur des yeux, la taille, l'adresse postale de la personne concernée, les noms, prénoms, dates de naissance et nationalité de ses parents, ses empreintes digitales, l'image numérisée de sa signature. De manière proche, pour le fichier TAJ, v. art. R. 40-26 du Code de procédure pénale. V. sur ce dernier J-M. Manach, « Beauvau veut (encore) améliorer le système de reconnaissance faciale de son fichier de suspects », *Next,* 28 août 2024.

115. Pour la liste des personnes autorisées, v. art. R. 40-28 du CPP.

116. Idemia group, « Safran Identity & Security équipe la police nationale française de sa toute dernière plateforme d'analyse vidéos (*sic*) », communiqué de presse, 30 novembre 2016. Plus récemment, v. M. Destal, C. Le Foll et G. Livolsi, « La police nationale utilise illégalement un logiciel israélien de reconnaissance faciale », *Disclose*, 14 novembre 2023. Dans cette affaire, la CNIL a annoncé le 15 novembre 2023 avoir initié des procédures de contrôle.

117. Sur ces points, nous renvoyons à R. Medard Inghilterra, « L'instauration d'une "technopolice" administrative en milieu urbain : cadre et enjeux juridiques », *loc. cit.,* I/, A/, 1.

118. Sénat (M-P. Daubresse, A. Belenet et J. Durain), *Rapport d'information n° 627, op. cit.,* p. 53.

119. Art. 5, 8. du Règlement IA.

120. Art. 6, I de la LIL.

121. Pour une appréciation similaire, v. C. Lequesne Roth, *New Surveillance Technologies in Public Spaces. Challenges and Perspectives for European Law at the Example of Facial Recognition,* Security in Public Places & Urban Agenda for the EU, 2021, p. 57-58 (sur l'écart du consentement comme fondement de la biométrie lorsqu'est en cause le RGPD, v. aussi p. 60) et CEPD, *Lignes directrices 3/2019 sur traitements de données à caractère personnel par des dispositifs vidéo*, *op. cit.,* p. 17.

122. V. art. 88, 89, II et 6, III de la LIL, renvoyant aux art. 31, II et 32.

123. Concernant l'adoption d'une législation nationale, v. aussi art. 5, 4. Du Règlement IA : « Un État membre peut décider de prévoir la possibilité d'autoriser totalement ou partiellement l'utilisation de systèmes d'identification biométriques à distance "en temps réel" dans des espaces accessibles au public à des fins répressives ».

124. Proposition de loi relative à la reconnaissance biométrique dans l'espace public, enregistrée à la présidence du Sénat le 5 avril 2023 (n° 505), adoptée en première lecture le 12 juin 2023 (n° 128) et transmise à la nouvelle législature de l'Assemblée nationale le 23 juillet 2024.

125. Il fut un temps envisagé d'aligner cette portée sur le champ d'application du mandat d'arrêt européen qui inclut des infractions telles que le trafic de stupéfiants, l'aide à l'entrée et au séjour irréguliers, les coups et blessures graves, le racisme et la xénophobie, les vols organisés ou vols avec arme, l'escroquerie, le racket, la contrefaçon ou encore le trafic de véhicules volés. V. art. 2, pt. 2 de la décision-cadre du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres.

126. Annexe II : « terrorisme, traite des êtres humains, exploitation sexuelle des enfants et pédopornographie, trafic de stupéfiants ou de substances psychotropes, trafic d'armes, de munitions ou d'explosifs, homicide volontaire, coups et blessures graves, trafic d'organes ou de tissus humains, trafic de matières nucléaires ou radioactives, enlèvement, séquestration ou prise d'otage, crimes relevant de la compétence de la Cour pénale internationale, détournement d'avion ou de navire, viol, criminalité environnementale, vol organisé ou à main armée, sabotage, participation à une organisation criminelle impliquée dans une ou plusieurs des infractions énumérées ci-dessus ».

127. Sur le sujet, v. not. S. Hennette-Vauchez, J-L. Halpérin et É. Millard, *L'état d'urgence : de l'exception à la banalisation,* Nanterre, Presses universitaires de Paris Nanterre, 2017, 268 p. ; (dir.), S. Hennette-Vauchez (dir.), *Ce qui reste(ra) toujours de l'urgence*, Paris, Institut universitaire Varenne, 2018, 402 p. ; S. Hennette-Vauchez, *La démocratie en état d'urgence. Quand l'exception devient permanente,* Paris, Seuil, 2022, 224 p. ; P. Cassia, *Contre l'état d'urgence*, Paris, Dalloz, 2016, 250 p.

128. L'analyse de ces arrêtés de police constituera le cœur du troisième volet de notre série d'étude sur la technopolice administrative.

129. Sur la préférence – compréhensible – des instances onusiennes pour une autorisation judiciaire, v. 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,* rapport annuel du Haut-Commissaire, 24 juin 2020, pt. 37.

130. V. art. 5, 2. et 3. du Règlement IA.

131. Art. 5, 3. du Règlement IA.

132. Pour un débat nourri sur la question, v. Assemblée nationale, séance du jeudi 23 mars 2023.

133. V. décret n° 2023-828 du 28 août 2023.

134. AN2V, *PIXEL 2024*, p. 172 et 240.

135. Pour une présentation détaillée du module, v. BriefCam, *BriefCam® v5.2.1. Manuel de l'utilisateur,* juin 2018, p. 7-32.

136. En ce sens, v. CEPD, *Lignes directrices 3/2019 sur traitements de données à caractère personnel par des dispositifs vidéo*, *op. cit.,* p. 19 ; DDD, *Technologies biométriques : l'impératif respect des droits fondamentaux, op. cit.*, p. 5-6 ; LQDN, *Projet de loi relatif aux Jeux Olympiques et Paralympiques de 2024, op. cit.*, p. 35-37.

137. Un « traitement » de données au sens de l'art. 4 du RGPD et de la LIL est constitué par « toute opération ou tout *ensemble d'opérations* effectuées *ou non à* l'aide de procédés automatisés » (nous soulignons).

138. Art. 3, 41) du Règlement IA.

139. Cour EDH, *Lopez Ribalda et autres c. Espagne*, *op. cit.*, § 87.

140. Cour EDH, *Guide sur l'article 8 de la Convention européenne des droits de l'homme – Droit au respect de la vie privée et familiale, du domicile et de la correspondance*, Conseil de l'Europe, Strasbourg, 2019, § 138.

141. Cour EDH, GC, *Lopez Ribalda et autres c. Espagne*, *op. cit.,* § 88.

142. *Ibidem* ; Cour EDH, 12 janvier 2010, *Gillan and Quinton v. The United Kingdom*, req. n° 4158/05, § 61 ; Cour EDH, 4 octobre 2023, *Glukhin c. Russie*, *op. cit.*, § 64.

143. En 1992, la Commission estimait que « l'obligation d'être porteur d'une carte d'identité et de la présenter à toute réquisition de la police [levant ainsi tout anonymat] ne [constituait] pas en tant que telle une ingérence dans la vie privée d'une personne au sens de l'article 8 de la Convention » (Commission européenne des droits de l'homme, 9 septembre 1992, *Filip Reyntjens c. Belgique*, req. n° 16810/90). Pour une reconnaissance de l'anonymat dans l'espace public comme « principe fondamental », v. toutefois CNIL, *Reconnaissance faciale. Pour un débat à la hauteur des enjeux,* novembre 2019, p. 7-8.

144. Cour EDH, *Gillan and Quinton v. The United Kingdom, op. cit.,* § 61-63.

145. Cour EDH, 18 octobre 2022, *Basu c. Allemagne,* req. n° 215/19 ; Cour EDH, 18 octobre 2022, *Muhammad v. Spain,* req. n° 34085/17 ; Cour EDH, 18 octobre 2022, *Wa Bail c. Suisse*, req. n^{os} 43868/18 et 25883/21.

146. Cour EDH, *Glukhin c. Russie*, *op. cit.,* § 64 et 67. Dans le même sens, v. 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, op. cit.*, pt. 33.

147. Cour EDH, GC, *Lopez Ribalda et autres c. Espagne*, *op. cit.,* § 89.

148. Sénat (M-P. Daubresse, A. Belenet et J. Durain), *Rapport d'information n° 627, op. cit.,* p. 56-57.

149. CNCDH, Avis sur la surveillance de l'espace public, *op. cit.*, p. 13.

150. S. Hennette-Vauchez, « *The Mall* », *loc. cit.*

151. Le concept de « renonciation » est ainsi entendu – dans le sous-titre et les développements – en un sens faible (*i.e.* non-exercice d'une liberté reconnue), le premier des trois identifiés par Julie Ringelheim et Olivier de Schutter *in* J. Ringelheim et O. de Schutter, « La renonciation aux droits fondamentaux. La libre disposition du soi et le règne de l'échange », *CRIDHO working paper series*, 1/2005, p. 7. V. aussi, en un sens fort, J. Arroyo, *La renonciation aux droits fondamentaux. Étude de droit français,* Paris, Pedone, 2016, 662 p., ainsi que les travaux doctoraux, en cours, de Cécile Degiovanni.

152. FRA, *Technologie de reconnaissance faciale*, Luxembourg, Office des publications de l'Union européenne, 2020, p. 33 (nous soulignons). En un sens similaire, v. CNCDH, Avis sur la surveillance de l'espace public, *op. cit.*, p. 13.

153. En ce sens, v. DDD, *Technologies biométriques : l'impératif respect des droits fondamentaux, op. cit.*, p. 14 : « L'un des aspects nécessaires (*sic*) dans l'exercice de ces libertés repose effectivement sur l'anonymat de groupe, en l'absence duquel les individus peuvent être amenés à altérer leur comportement et à ne pas exprimer leurs pensées de la même manière ».

154. CNIL, Délibération 2020-136 du 17 décembre 2020, *loc. cit.*, réitéré *in* CNIL, « Caméras dites "intelligentes" ou "augmentées" dans les espaces publics », 2022, p. 9 (nous soulignons). Dans le même sens, v. LQDN, *Vidéosurveillance algorithmique. Dangers et contre-attaque,* mai 2024, p. 28 ; L. Cluzel-Métayer, « L'IA au service de la vidéosurveillance : pour et par-delà les Jeux », *op. cit.*, p. 290.

155. D. Murray et al., « The Chilling Effect of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe », *Journal of Human Rights Practice,* vol. 16, 2024, p. 397-412.

156. *Ibidem.*

157. CNIL, courrier du 25 octobre 2019, obtenu par la Quadrature du Net, p. 5. De manière moins explicite, v. CNIL, courrier du 25 septembre 2023, obtenu sur demande CADA par nos soins.

158. Sur la réaction *a posteriori* des autorités normatives qui entérinent des usages expérimentaux, v. R. Medard Inghilterra, « L'instauration d'une "technopolice" administrative en milieu urbain : cadre et enjeux juridiques », *loc. cit.* En l'état, la captation de son dans le cadre de la vidéoprotection demeure interdite. V. art. R. 253-1 du CSI : « Peuvent être enregistrées dans les traitements mentionnés à l'article R. 251-1, les données à caractère personnel et informations suivantes : 1° Les images, à l'exclusion des sons, captées par les systèmes de vidéoprotection ».

159. D. Murray et al., « The Chilling Effect of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe », *loc. cit.* Dans le même sens, FRA, *Technologie de reconnaissance faciale*, *op. cit.*, p. 33.

160. Sur le sujet, v. Youth Department of the Council of Europe, *Shrinking space for civil society: the impact on young people and their organisations,* novembre 2018, 22 p. ; T. Deželan & L. Yurttagüler, *Shrinking democratic civic space for youth*, commissioned by the European Union and the Council of Europe, 2021, 34 p.

161. Not. C. Lequesne Roth, *New Surveillance Technologies in Public Spaces, op. cit.,* p. 2 et C. Lequesne, « L'encadrement des technologies de surveillance des foules : réflexions sur la démocratie numérique dans l'espace public », *in* C. Derave, B. Frydman et N. Genicot (dir.), *L'intelligence artificielle face à l'État de droit,* Bruxelles, Bruylant, p. 150-151, y compris note 46.

162. Sénat (M-P. Daubresse, A. Belenet et J. Durain), *Rapport d'information n° 627, op. cit.,* p. 56.

163. FRA, *Technologie de reconnaissance faciale*, *op. cit.*, p. 34 : le « déploiement de technologies de reconnaissance faciale peut avoir un effet dissuasif au regard duquel des personnes s'abstiennent d'exercer légalement leur liberté de réunion et d'association par crainte des conséquences négatives qui pourraient en découler. Elles pourraient ainsi être dissuadées de rencontrer des personnes ou des organisations particulières, d'assister à certaines réunions ou de participer à

certaines manifestations ». Dans le même sens, v. 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, op. cit.*, pt. 31-33.

164. Règlement IA, considérant 32 (nous soulignons). Des juridictions nationales ont parfois tenu un raisonnement similaire pour la simple photographie de manifestants, publiée par les services de police sur les réseaux sociaux à des fins de communication. V. Tribunal administratif de Gelsenkirchen, 23 octobre 2018, 2018, 14 K 3543/18, not. § 66 « La conscience que la participation à un rassemblement est ainsi "enregistrée par l'État" peut avoir *des effets d'intimidation* qui se répercutent en même temps sur les fondements du débat démocratique. En effet, les personnes qui s'attendent à ce que leur participation à un rassemblement soit enregistrée par les autorités et à ce que cela leur fasse courir des risques personnels *peuvent renoncer à l'exercice de leur droit fondamental*. De tels effets d'intimidation peuvent déjà résulter de la simple présence d'une caméra (de police) prête à filmer et dirigée vers les participants à la manifestation, même si l'évènement n'est pas enregistré » (nous soulignons, trad. *Deepl*).

165. Cour EDH, *Glukhin c. Russie*, *op. cit.,* § 89.

166. *Idem,* § 90.

167. Sur la question, v. not. C. Lequesne Roth et J. Keller, *Surveiller les foules. Pour un encadrement des IA "physiognomoniques"*, *op. cit.*, p. 44-45 qui évoque plusieurs cas : Afghanistan, Birmanie, Chine, Hong-Kong, Inde, Iran, Serbie.

168. En ce sens, v. not. Cour EDH, 15 mars 2022, *Communauté genevoise d'action syndicale (CGAS) c. Suisse,* req. n° 21881/20, § 83.

169. 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, op. cit.*, pts 33 et 53, f) et i).

170. En ce sens, CNCDH, Avis sur la surveillance de l'espace public, *op. cit.*, p. 9.

171. Arrêtés 2024-00847 du 20 juin 2024, 2024-00959 du 11 juillet 2024, 2024-1017 du 19 juillet 2024.

172. Arrêtés 2024-00860 du 25 juin 2024, 2024-00948 du 10 juillet 2024, DUPA-2024-1007 du 12 juillet 2024, 2024-1117 du 8 août 2024.

173. Arrêtés DUPA-2024-0701 du 31 mai 2024, DUPA-2024-1073 du 25 juillet 2024, DUPA-2024-1081 du 25 juillet 2024.

174. Récemment, v. E. P., « Après l'expérimentation durant les JO, la vidéosurveillance "algorithmique" va se généraliser », *Le Figaro,* 2 octobre 2024 ; P. Le Cœur, « Le Préfet de police de Paris "favorable" à une prolongation du recours à la vidéosurveillance algorithmique expérimentée pendant les JO », *Le Monde,* 25 septembre 2024.

175. R. Thaler & C. Sunstein, *Nudge. Improving Decision About Health, Wealth and Happiness,* New-York, Penguin Books, 2009, 320 p.

176. Sur le pouvoir normalisateur et disciplinaire de la technique, v. les travaux de Michel Foucault, not. *Surveiller et punir. Naissance de la prison,* Paris, Gallimard, 1975, not. p. 159-216, spéc. p. 201 : « l'exercice de la discipline suppose un dispositif qui contraigne par le jeu du regard ; un mécanisme où les techniques qui permettent de voir induisent des effets de pouvoir ».

177. Art. 10 de la loi JOP et 1 de son décret d'application du 28 août 2023.

178. LQDN, *Projet de loi relatif aux Jeux Olympiques et Paralympiques de 2024, op. cit.*, p. 30.

179. AN2V, *PIXEL 2024*, p. 297.

180. *Idem,* p. 305.

181. *Idem,* p. 303 et AN2V, *PIXEL 2025,* p. 291.

182. https://www.evitech.com/fr/produits/produit-jaguar.

183. T. Jusquiame, *Circulez. La ville sous surveillance,* Paris, Marchially, p. 18.

184. Une fois de plus, v. LQDN, *Vidéosurveillance algorithmique, op. cit.* et LQDN, *Projet de loi relatif aux Jeux Olympiques et Paralympiques de 2024, op. cit.,* not. p. 30.

185. Sur les disciplines non pas comme « infra-droit » mais comme « contre-droit », v. M. Foucault, *Surveiller et punir. Naissance de la prison, op. cit.*, p. 259.

186. D. Loschak, « Espace et contrôle social », *in* CURAPP, *Centre, périphérie, territoire*, Paris, PUF, 1978, p. 192. Sur le sujet, not. sur l'analyse détaillée de divers espaces conçus pour discipliner les corps (*e.g.* prisons, hôpitaux, salles de classe) v. bien sûr *idem.*

187. T. Jusquiame, *Circulez. La ville sous surveillance, op. cit.*, p. 28

188. S. Hennette Vauchez, « *The Mall* », *loc. cit.*

189. Règlement intérieur du centre commercial *Les boutiques du palais*, tel que restitué *in* S. Hennette Vauchez, « *The Mall* », *loc. cit.*

190. Art. 3 du décret n° 2023-828 du 28 août 2023.

191. S. Hennette Vauchez, « *The Mall* », *loc. cit.*

192. Art. 5 du décret n° 62-768 du 10 juillet 1962 fixant le régime des études et des examens de la licence en droit et de la première année de la licence ès sciences économiques. V. not. sur le sujet X. Dupré de Boulois, « La naissance de l'enseignement du droit des libertés en France : faux départ et nouvelle donne », *RDLF,* chron. n° 49 et, dans un autre registre, V. Champeil-Desplats, « Des "libertés publiques" aux "droits fondamentaux" : effets et enjeux d'un changement de dénomination », *Jus Politicum,* n° 5, 2010.

193. *I.e.* surface de terrain acquise pour la construction d'un ouvrage.

194. D. Loschak, « Espace et contrôle social », *op. cit.*, p. 154.

195. H. Avvenire, *Le concept d'espace public, op. cit.* p. 18.

196. *Idem,* v. respectivement p. 109-140, p. 88-108 et p. 145-170.

197. *Idem,* p. 86.

198. *Idem,* p. 75.

199. En ce sens, S. Hennette-Vauchez, « *The Mall* », *loc. cit.* et O. Bui-Xuan, « Propos introductifs », *op. cit.*, p. 8-10 (au sujet *des espaces publics*). Plus largement, v. D. Moeckli, *Exclusion from Public Space,* Cambridge, CUP, 2016, not. p. 412-436.

200. En ce sens, *ibidem.*

201. J. Habermas, *L'espace public,* Paris, Payot, 1988, 322 p.

202. H. Avvenire, *Le concept d'espace public, op. cit.* p. 89-97.

203. D. Loschak, « Espace et contrôle social », *op. cit.*, p. 159-160.

204. *Idem,* p. 192.

205. Sur le sujet, soulignons l'appel à projet « Gestion de l'espace public et stratégies d'évictions des populations dites "indésirables" », lancé par le Défenseur des droits en mars 2023, dont les résultats sont particulièrement attendus, y compris sur le plan juridique avec les contributions des chercheurs du MIL de l'Université Paris-Est Créteil (Noé Wagener et Olga Mamoudy, entre autres).

206. Récemment, TA Amiens, ord., 16 mai 2024, *LDH et autres,* n° 2401685.

207. Par ex. CE, 17 juillet 2023, *LDH,* n° 475636.

208. Par ex. TA Lille, ord., 12 octobre 2022, *Secours catholique – Caritas France et autres,* n^{os} 2007484, 2100364 et 2101109.

209. Soulignons que certains arrêtés de police ont déjà tâché d'opérer par euphémisation des comportements, à l'instar de l'arrêté du 15 octobre 2015 du maire de Saint-Étienne portant « Code de la tranquillité publique ». À des fins de lutte contre la mendicité, étaient notamment visés : la station assise ou allongée lorsqu'elle constitue une entrave à la circulation des piétons ou une utilisation des équipements collectifs de nature à empêcher ou troubler un usage partagé ; le regroupement de plus de deux chiens effectuant une ou plusieurs stations couchées sur la voie publique ; la consommation de boissons alcoolisées dans un secteur géographique déterminé ; la fouille des poubelles aux fins de chiffonnage et de récupération des déchets. V. ici CE, 16 juillet 2021, *LDH c. Ville de Saint-Étienne,* n° 434254.

210. M. Foucault, *Surveiller et punir, op. cit.,* p. 201-208.

211. *Idem,* p. 202 et p. 228-232.
212. Pour une description de la ville comme nouvel aéroport, v. T. Jusquiame, *Circulez. La ville sous surveillance, op. cit.,* p. 227. Outre les Jeux olympiques et paralympiques, l'organisation des G7 illustre aussi le phénomène d'une ville confinée (p. 211-217).
213. Pour reprendre les mots de Danièle Lochak, un quadrillage réalisant une « "utopie capillaire" d'un pouvoir qui domine en s'infiltrant » (D. Loschak, « Espace et contrôle social », *op. cit.*, p. 177).
214. Sur la distinction et l'aspect complémentaire de la discipline d'exception et de la surveillance généralisée, v. M. Foucault, *Surveiller et punir, op. cit.,* p. 244.
215. *Idem,* p. 249 : « Et pour s'exercer, ce pouvoir doit se donner l'instrument d'une surveillance permanente, exhaustive, omniprésente, capable de tout rendre visible, mais à la condition de se rendre elle-même invisible. Elle doit être comme un regard sans visage qui transforme tout le corps social en un champ de perception : des milliers d'yeux postés partout, des attentions mobiles et toujours en éveil, un long réseau hiérarchisé ».
216. *Idem,* p. 204 et p. 235. Sur la représentation du Panoptique, v. not. planches 17 à 27 entre les p. 202 et 203. Sur l'analyse du Panoptique comme « technologie politique » et « schéma disciplinaire » et économique, qui s'exerce spontanément et sans bruit, v. p. 233-243. Plus largement, sur l'aspect central de la visibilité des actions et des individus dans l'espace public, et sur son articulation avec les conceptions policière et libérale dépeintes par Hugo Avvenire, v. H. Avvenire, *Le concept d'espace public, op. cit*., p. 104-109 et p. 175-179.
217. *Idem,* p. 234 et p. 236.
218. *Quand les mois auront passé, quand seront apaisés leurs beaux rêves flambants, quand leur ciel se couvrira de gros nuages lourds, ils s'apercevront émus que c'est au hasard des rues sur un de ces fameux bancs, qu'ils ont vécu le meilleur morceau de leur amour* (G. Brassens, *Les amoureux des bancs publics*, Polydor, 1953).

ABSTRACTS

In September 2019, several associations led by La Quadrature du Net launched the "Technopolice" initiative with the ambition of alerting to the development of surveillance of urban space by digital devices for policing purposes. The concept must be taken seriously and may be specially applied to the field of administrative policing. Some reports of administrative courts, as well as the sanctions and guidance issued by the CNIL, or even recent litigations and legislative debates, reveal that the phenomenon goes beyond a mere associative concern. It entails considerable legal transformations. Among them, the equipment and the increasing mobilization of technological – mainly digital – devices for the purposes of carrying out administrative police missions raise major issues for human rights. This article aims to enlighten and better understand these consequences.

En septembre 2019, un collectif d'associations conduit par La Quadrature du Net lançait l'initiative « Technopolice » avec pour ambition d'alerter sur un phénomène : le développement d'une surveillance de l'espace urbain par des dispositifs numériques à des fins policières. Le concept employé doit être pris au sérieux et peut être décliné spécifiquement dans le champ de la police administrative. Les rapports des juridictions, prises de position de la CNIL, contentieux et débats législatifs récents attestent que le phénomène va au-delà de la préoccupation associative.

Il charrie des transformations juridiques considérables. L'équipement et la mobilisation croissante de dispositifs technologiques – notamment numériques – aux fins d'exercice des missions de police administrative soulèvent en particulier de vifs enjeux pour les droits et libertés que la présente contribution a vocation à décrypter.

INDEX

Keywords: Technopolice, surveillance, personal data, privacy, public space.
Mots-clés: Technopolice, surveillance, données personnelles, vie privée, espace public.

AUTHOR

ROBIN MEDARD INGHILTERRA

Maître de conférences à l'Université Paris 1 Panthéon-Sorbonne