L'instauration d'une " technopolice " administrative en milieu urbain : cadre et enjeux juridiques

Robin Medard Inghilterra

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

25 | 2024
Revue des droits de l'homme - N°25

L'instauration d'une « technopolice » administrative en milieu urbain : cadre et enjeux juridiques

Robin Medard Inghilterra

OpenEdition Journals

Édition électronique
URL : https://journals.openedition.org/revdh/19033
DOI : 10.4000/revdh.19033
ISSN : 2264-119X

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

Référence électronique
Robin Medard Inghilterra, « L'instauration d'une « technopolice » administrative en milieu urbain : cadre et enjeux juridiques », *La Revue des droits de l'homme* [En ligne], 25 | 2024, mis en ligne le 21 janvier 2024, consulté le 16 février 2024. URL : http://journals.openedition.org/revdh/19033 ; DOI : https://doi.org/10.4000/revdh.19033

L'instauration d'une « technopolice » administrative en milieu urbain : cadre et enjeux juridiques

Robin Medard Inghilterra

NOTE DE L'AUTEUR

La présente contribution s'inscrit dans le cadre d'une série d'études relatives à la « technopolice » administrative. Elle en constitue le premier volet, dédié à la définition du phénomène et à de grands enjeux qu'il soulève en droit administratif. Ce premier volet sera complété par deux études – à paraître – spécifiquement consacrées aux risques en matière de droits et libertés et aux Jeux olympiques et paralympiques 2024.

1 Prompt à saisir l'occasion fournie par ses rapports annuels pour envisager les mutations profondes qui affectent le droit administratif, en dessinent le présent et parfois l'avenir, le Conseil d'État a dédié son étude en 2022 à l'intelligence artificielle dans l'action publique[1]. Cette thématique résonne avec celles qui furent traitées au sein des rapports précédents en 2014, *Le numérique et les droits fondamentaux*, et en 2016, *Puissance publique et plateformes numériques*. En appréhendant six ans plus tard la manière dont l'intelligence artificielle (ci-après IA) risque de bouleverser l'action publique, le Conseil d'État s'est livré à une réflexion prospective. Il a surtout esquissé des orientations afin de conjurer ce qu'il qualifie de « double risque », à savoir la distanciation passive du secteur public et la déconnexion subséquente d'un régulateur appelé à encadrer les systèmes d'IA[2] développés par le secteur privé[3].

2 Pour les acteurs publics comme pour les juristes publicistes, les enjeux soulevés par cette thématique imposent une attention rigoureuse et immédiate. D'abord, parce que l'heure du déploiement des systèmes d'IA semble advenue. Entendue comme un

ensemble de « technologies qui combinent données, algorithmes et puissance de calcul »[4], l'IA est inévitablement alimentée par la collecte croissante de données et les progrès constants des calculs qui permettent de les traiter. Ensuite, parce qu'à la maturité – toujours relative – de l'IA, s'ajoute la transversalité de ses usages : son déploiement est envisagé tant au sein de l'administration centrale que des transports, des hôpitaux, des écoles, de la police, en matière de lutte contre la fraude fiscale[5], au soutien de la politique de l'emploi, du fonctionnement de la justice, de l'armée ou des services de renseignements, entre autres. Dès lors que des services publics nationaux s'en emparent, l'échelle de mise en œuvre des systèmes d'IA et l'ampleur de ses effets justifient, encore, de penser en profondeur son statut d'objet juridique.

3 Le projet se révèle, il est vrai, pour le moins inconfortable. D'une part, la rapide évolution du cadre juridique – balbutiant – relatif à l'IA fait courir à l'étude doctrinale le risque de l'obsolescence à brève échéance[6]. D'autre part, les dispositifs technologiques et leurs usages envisagés évoluent, *a fortiori*, à une vitesse telle que l'objet même du propos semble éphémère. À peine le recours aux applications de *tracing* à des fins sanitaires serait-il commenté qu'il ne serait plus d'actualité. Il convient toutefois d'avancer sur ce terrain pour comprendre, questionner et à terme réguler ces technologies[7] dont les usages publics vont croissant.

4 Eu égard à son ampleur, la tâche ne peut qu'être séquencée. Du point de vue territorial, d'abord, ce séquençage peut conduire à mettre en lumière l'action locale, prioritairement. Comme souvent lorsqu'il est question d'expérimentation, les collectivités territoriales se placent, en France, au premier plan. En matière de nouvelles technologies, elles constituent un véritable laboratoire de l'action publique. La proximité dont elles disposent vis-à-vis de leurs territoires et des administrés favorise la collecte et la production de données pertinentes. Leur champ de compétences, à la fois conséquent et hétérogène, fournit un vaste réservoir à l'expérimentation technologique. Quant au lien de confiance, plus fort, qui unit acteurs publics locaux et population, il constitue un facteur précieux d'acceptation des innovations. Le contexte budgétaire tendu au plan local, lui, rend ces innovations d'autant plus inéluctables[8]. Sous cet angle, les collectivités territoriales se muent en un terrain d'étude privilégié.

5 Au niveau politique comme au niveau académique, la figure de la « ville intelligente » (*smart city*) a déjà capté une partie des réflexions émergentes sur les bouleversements induits par les mutations numériques dans une perspective d'optimisation de l'administration du territoire[9]. Le concept focalise en particulier l'attention sur les transformations des structures urbaines (voies publiques, réseaux souterrains, bâtiments publics, aménagement de l'espace public) dans une optique futuriste prestement incarnée par les industriels[10]. Les initiatives emblématiques sont légion et diverses sur l'ensemble du globe : diminution drastique de l'empreinte écologique à Masdar ; urbanisme utopiste[11] d'une ville entièrement nouvelle à Songdo ; *smart nation* pétrie par la collecte et l'exploitation de données à Singapour ; développement de projets pilotes par Toyota et sa Woven City au pied du mont Fuji, ou par Google et son Quayside sur les rives du lac Ontario[12]. La France n'échappe pas à cette tendance. Des projets phares de villes dites « intelligentes » apparaissent, à l'instar de OnDijon. Plus largement, les technologies numériques infusent l'espace urbain hexagonal. Qu'elle constitue l'échelle de décision (*i.e.* communale) ou le support de mise en œuvre d'orientations fixées à un échelon supérieur (*e.g.* intercommunal, départemental,

régional, national), la ville se présente comme le cadre d'analyse idoine pour questionner, comprendre et réguler le recours aux technologies numériques, incluant l'IA, dans l'action publique.

6 À défaut de pouvoir appréhender la problématique sous toutes ses facettes, la présente contribution est contrainte à un séquençage supplémentaire. En plus de placer la focale sur l'échelle de la ville, nous proposons de circonscrire l'attention aux missions de police administrative. En la matière, le « double risque » évoqué en 2022 par le Conseil d'État est criant. Dans son rapport sur *Les polices municipales,* la Cour des comptes s'était déjà inquiétée en 2020 d'un décalage entre les usages publics croissants des technologies innovantes et l'absence d'évolution d'un cadre juridique qui « [faisait] défaut, tant pour les dispositifs d'alerte que pour les moyens de surveillance mobile et les technologies avancées »[13]. Or, elle poursuivait : « comme l'ont montré les dispositifs de surveillance mis en place lors du confinement [...], ce vide juridique conduit à des usages non encadrés de moyens techniques dont les forces – tant nationales que municipales – ont fait l'acquisition et dont elles comptent bien se servir »[14]. Les réformes législatives intervenues depuis n'ont pas couvert l'ensemble des usages recensés dans le champ de la police administrative. Elles n'ont pas non plus épuisé les questionnements relatifs aux défis qu'ils posent et aux transformations qu'ils suscitent, qui plus est dans un contexte politique de méfiance à l'égard de la surveillance publique. De ce point de vue, l'initiative « Technopolice » lancée par l'association la Quadrature du Net en septembre 2019 est symptomatique. Elle dénonce « une mise sous surveillance totale de l'espace urbain à des fins policières » dont « le Big Data et l'intelligence artificielle sont la clé de voûte »[15].

7 Cette initiative et la lecture des contenus qu'elle a produits, spécialement des conventions et autres documents administratifs obtenus par ladite association[16], ont fait émerger les problématiques structurantes de la présente recherche. Elle postule l'existence d'une *technopolice*[17], néologisme qui désigne un phénomène d'équipement et de mobilisation croissante de dispositifs technologiques, en particulier numériques, aux fins d'exercice des missions de police[18]. Face à ce phénomène, qui prend principalement ancrage dans les villes ainsi qu'aux frontières[19], les rapports précités du Conseil d'État en 2022 et de la Cour des comptes en 2020 interpellent en ce qu'ils pointent tous deux l'impréparation du cadre juridique à certaines de ces mutations. Ils invitent à approfondir les réflexions relatives à l'adéquation des notions et des catégories juridiques existantes du droit administratif, à leur éventuelle adaptation, marginale ou fondamentale.

8 S'attacher aux enjeux juridiques essentiels de ce que serait une *technopolice* administrative en milieu urbain force le chercheur à un constat immédiat. La méthode convoquée ne peut se borner à une approche dogmatique. Cette perspective, oscillant entre ordonnancement et évaluation du droit existant, parfois utile, est souvent limitée par l'aridité du contentieux et la concision du droit positif dédié audit objet. Mais, précisément, cette limite méthodologique et le constat qui la fonde ne sont pas anodins. Ils peuvent illustrer le premier pan du « double risque » redouté par le Conseil d'État, à savoir la distanciation passive du secteur public et, avant tout, du législateur. Si une technopolice voit bel et bien le jour d'une part, et que le droit est censé « [faire] corps avec la technologie », « [devenir] un droit augmenté »[20] d'autre part, le constat effectué à titre liminaire interroge la capacité du législateur et du pouvoir réglementaire à se saisir des usages. Un premier enjeu apparaît, relatif à l'ampleur de la mobilisation des

nouvelles technologies et à la manière dont les autorités normatives y font face. L'analyse conduite en réaction permet de cartographier les nouvelles infrastructures de la police administrative et de démontrer qu'elles sont imparfaitement appréhendées par le droit (I). Une réflexion prospective sur les enjeux juridiques que posent ces infrastructures s'avère d'autant plus nécessaire pour limiter le second pan du « double risque » précité. Une fois mesuré un phénomène empirique, et face aux limites de son appréhension juridique, l'anticipation de ses possibles effets normatifs sert, en d'autres termes, l'avertissement du régulateur public. Quoique le propos ne puisse être formulé que modestement, et rester en suspens, dans l'attente d'interventions complémentaires du législateur et d'interprétations authentiques posées par les juridictions, c'est sous cet angle qu'il convient d'envisager les répercussions de la technopolice administrative sur les rapports de l'administration aux tiers (II).

I/ – Cartographier pour appréhender les nouvelles infrastructures de la police administrative

9 Pilier central et historique de la technopolice, la « vidéoprotection »[21], développée dans une optique de sécurité publique depuis plusieurs décennies, est désormais bien saisie par le droit (A). En complément, les municipalités s'équipent d'une multitude de nouveaux dispositifs auxquels sont assignées des finalités de prévention des troubles à l'ordre public plus variés. Pour ces derniers, l'affirmation de la Cour des comptes au sujet des polices municipales selon laquelle « le vide juridique qui caractérise l'emploi des nouvelles technologies est [...] préoccupant et doit être comblé »[22] demeure en partie valable (B).

A/ La vidéoprotection au service de la sécurité publique : pilier normalisé de la technopolice

10 La constante expansion du parc français de vidéoprotection a inévitablement entraîné avec elle la création et l'enrichissement d'un cadre juridique dédié (1). Elle a récemment contribué à faire émerger les centres de supervision urbains (2). Depuis peu, la vidéoprotection se trouve également confrontée à de nouvelles perspectives, qui agitent le législateur, entre traitement automatisé des images et reconnaissance faciale (3).

1/ La vidéoprotection : objet juridique ancien, réseau moderne

11 Infrastructure devenue centrale en l'espace de deux décennies, la vidéoprotection fut saisie par le législateur dès 1995[23]. Elle trouve depuis 2012 une consécration solide en droit positif au sein du Code de la sécurité intérieure (ci-après CSI)[24]. Toute installation nouvelle de caméras (unidirectionnelles, à balayage panoramique, dômes...) est soumise à l'article L. 251-2 du CSI qui impose de déterminer la finalité précise pour laquelle la captation, transmission et l'enregistrement d'images prises sur la voie publique sont envisagés. La disposition mentionne onze finalités exhaustives. Y figurent la prévention des atteintes à la sécurité des personnes et des biens dans des lieux ou zones particulièrement exposés, la prévention d'actes de terrorisme, la protection des bâtiments et installations publics et de leurs abords, ainsi que la prévention et la

constatation des infractions relatives à l'abandon d'objets (*e.g.* ordures, déchets, matériaux divers), des infractions aux règles de la circulation, ou encore la régulation des flux de transport. Hors de la voie publique, la vidéoprotection peut également s'étendre aux lieux et établissements ouverts au public dès lors que la sécurité des personnes et des biens y est menacée par des risques d'agression ou de vol. En pratique, force est de constater qu'elle est principalement déployée pour prévenir les troubles à la sécurité publique. C'est en ce sens qu'elle est intégrée sur demande du ministère de l'Intérieur aux grandes priorités des politiques de prévention pour 2022[25] et 2023[26], puisque l'équipement des collectivités en caméras est financièrement soutenu par l'État[27]. Quelle que soit la finalité retenue, une autorisation d'exploitation délivrée par le préfet après avis de la commission départementale de vidéoprotection est indispensable[28]. Celle-ci est valable pour une durée de cinq ans, renouvelable[29]. Elle fixe le délai maximum de conservation des images, qui ne peut excéder un mois, les conditions de leur exploitation et les personnes habilitées à les visionner[30].

12 Par ces dispositions, le législateur s'est emparé d'un phénomène qui, loin d'être résiduel, devient de plus en plus massif. Certes, la demande de la Cour des comptes, qui souhaitait en 2020 que soit établie une cartographie précise des systèmes de vidéoprotection par les collectivités territoriales[31], n'a pas été satisfaite, de telle sorte que les chiffres diffèrent quant au nombre exact de caméras en service. Certes, les cartes collaboratives qui sont réalisées, si elles offrent un aperçu saisissant, l'initiative la plus notable de ce point de vue étant *Surveillance under Surveillance*[32], s'avèrent incomplètes. Toujours est-il que, en 2018, le ministère de l'Intérieur dénombrait 60 674 caméras en France. La gendarmerie et la police nationale estimaient, elles, le nombre de caméras hors Paris et petite couronne à 76 457 pour la même année, contre 23 214 en 2010[33]. Depuis, la « Technocarte » de l'initiative *Technopolice* tâche d'opérer un suivi des réseaux municipaux de vidéoprotection en fonction des annonces et des marchés conclus : 269 caméras renouvelées à Dijon, 709 acquises à Strasbourg, 230 à Valenciennes, 400 à Toulouse, 700 à Montpellier, 125 caméras à Sète, 524 à Cannes, 3 300 à Nice, 1 200 à La Défense[34], etc. Utilement, la Cour des comptes fournit une vision plus précise sur le cas spécifique de l'Île-de-France. Elle estime que le plan de vidéoprotection de la préfecture de police de Paris repose en 2022 sur 4 000 caméras de la préfecture et sur plus de 37 000 caméras appartenant à des autorités publiques tierces[35], avant tout des collectivités territoriales, interconnectées sur le territoire régional grâce à la construction d'un réseau propre de fibre optique[36]. En définitive, le réseau de vidéoprotection a globalement quadruplé depuis 2010 et le maillage territorial se resserre.

13 L'organisation des Jeux olympiques et paralympiques en 2024 accentue la dynamique. L'installation de 15 000 nouvelles caméras a d'ores et déjà été annoncée par le ministère de l'Intérieur dans le cadre d'un « effort sans précédent », cofinancé à hauteur de 44 millions d'euros par le Fonds interministériel de prévention de la délinquance[37]. Cette somme s'ajoute aux 33 millions d'euros engagés sur 2021 et 2022[38], aux 20 millions d'euros mis à disposition pour restaurer 1 000 caméras des collectivités endommagées à la suite des émeutes de juillet 2023[39], et aux 10 millions d'euros de financement voté par Île-de-France Mobilités pour améliorer le dispositif de vidéoprotection dans les transports publics en vue des Jeux olympiques et paralympiques[40]. Pour le seul plan de vidéoprotection de la préfecture de police de Paris, entre 433 et 481 millions d'euros auront été investis sur seize ans[41]. Cet investissement d'ampleur a permis une

implantation en tout lieu des caméras publiques dans les villes. À tel point que le parc de vidéoprotection s'apparente désormais, selon le Laboratoire d'innovation numérique de la Commission nationale de l'informatique et des libertés (ci-après CNIL), à la cinquième « *utility* » (*i.e.* valeur de services des collectivités), aux côtés du gaz, de l'électricité, de l'eau et des télécommunications[42]. Le législateur ne saurait l'ignorer et lui a consacré le Titre V du Livre II du CSI.

2/ Les centres de supervision urbains : foyers institutionnalisés de la vidéoprotection

14 Créditée d'un fondement légal déjà solide, la vidéoprotection continue de bénéficier d'une attention régulière du législateur qui accélère son institutionnalisation. Pour renforcer la dynamique de mutualisation des moyens par les collectivités territoriales et leurs groupements, l'article 42 de la loi du 25 mai 2021 pour une sécurité globale a, par exemple, créé un cadre propice à la fois à l'acquisition intercommunale d'équipements mobiliers et immobiliers coûteux et à l'amélioration de leur opérationnalisation[43]. Cette mutualisation accentue la création et le développement des centres de supervision urbains (ci-après CSU) dont le nombre a doublé entre 2015 et 2019. Il en existait 903 en 2019[44]. Ces infrastructures font office de point névralgique de la technopolice. Y sont visionnées les images en temps réel par une unité de vidéoprotection composée d'agents assermentés qui sont en mesure de diriger les interventions sur le terrain d'unités opérationnelles[45].

15 La multiplication des CSU incarne à merveille la place désormais occupée par la vidéoprotection dans l'exercice des missions de police administrative générale. Si les CSU travaillent en collaboration étroite avec les services de l'État, police nationale, gendarmerie et service des douanes en tête[46], « il n'y a pas de report automatique d'images vers les forces nationales »[47]. Comme le rappelle la Cour des comptes, les systèmes de vidéoprotection sont « installés et exploités aux frais des communes » et « le plus souvent gérés par le service de police municipale dont ils constituent un outil d'intervention même si les données enregistrées peuvent être confiées, en tant que de besoin, aux services d'enquête judiciaire de la police et de la gendarmerie »[48]. En d'autres termes, l'usage répressif de la vidéoprotection n'apparaît pas nécessairement principal et une place centrale est concédée à l'utilisation préventive qui renforce les missions de police administrative générale. Cette utilisation est faite dans le cadre d'un régime juridique déterminé, y compris en ce qui concerne les modalités de création et de fonctionnement des CSU. Les interventions récentes du législateur et du pouvoir réglementaire ont, là aussi, permis d'appréhender juridiquement différentes configurations[49].

16 Régulièrement conçus à l'échelon municipal pour les villes les plus importantes, les CSU peuvent être instaurés par les maires, autorités de police chargées d'assurer le bon ordre, la sûreté, la sécurité et la salubrité publics sur leurs territoires[50], le cas échéant par l'exploitation d'un réseau de vidéoprotection de la voie publique et des lieux ouverts au public. Christian Estrosi a ainsi créé dès 2010 le CSU de la ville de Nice, doté en 2023 de quatre-vingt-dix agents, de trois salles d'exploitation vidéo, d'une salle d'extraction vidéo, d'une salle de crise, et fonctionnant grâce à un réseau de plus 4 000 caméras[51]. Quelques kilomètres plus à l'ouest, les 829 caméras en service à Cannes en 2023 (une pour quatre-vingt-dix habitants) sont supervisées par vingt-quatre agents au sein d'un CSU municipal[52] quand les 1 500 caméras de la ville de Marseille le sont par

une dizaine d'opérateurs[53]. Même chose à Bobigny[54], à Saint-Denis, à Carcassonne ou à Fort-de-France.

17 Une mutualisation du CSU entre communes par voie conventionnelle – en dehors du cadre d'un établissement public de coopération intercommunale (ci-après EPCI) – est aussi envisageable. Auquel cas, elle doit préserver les pouvoirs de police respectifs des édiles et les compétences de leurs communes. La collectivité qui acquiert les équipements mobiliers et immobiliers doit en contrepartie recevoir une participation financière des autres communes utilisatrices[55]. Les agents affectés au visionnage des images de vidéoprotection doivent, eux, être employés dans le cadre du régime de mise en commun des policiers municipaux prévus par le CSI[56].

18 Plus fréquemment, les CSU se développent dans le cadre de l'intercommunalité[57]. Les EPCI peuvent, en effet, recourir à la vidéoprotection depuis 2007, sous réserve de l'autorisation des communes concernées par l'implantation des caméras et à la condition d'exercer la compétence relative aux dispositifs locaux de prévention de la délinquance[58]. Cette compétence est exercée de plein droit par les communautés d'agglomération, les communautés urbaines et les métropoles[59]. Les communautés de communes, elles, n'en disposent pas nécessairement[60]. Des CSU intercommunaux ont été mis en place par les métropoles de Nantes dès 2018[61], de Nancy dès 2019[62], de Toulouse[63], ou encore, en banlieue lyonnaise, par la communauté de communes de Miribel et du Plateau[64]. Le Gouvernement privilégie cette coopération pour les collectivités de taille moyenne ou réduite et y incite fortement par un financement fléché[65].

19 De manière plus accessoire, les conseils départementaux et régionaux peuvent également s'équiper d'un dispositif de vidéoprotection, pour une finalité exclusive, à savoir la protection des bâtiments et des installations de la collectivité départementale ou régionale. Les routes, bâtiments administratifs, collèges et lycées et leurs abords sont ainsi susceptibles d'être vidéoprotégés. Pour les départements, plus que des CSU autonomes, ce sont des CSU pilotés par des syndicats mixtes ouverts qui s'avèrent les plus appropriés[66]. La concrétisation du projet est dans ce cas soumise à l'approbation de l'ensemble des collectivités composant le syndicat (*i.e.* communes, EPCI et départements limitrophes) et des communes d'implantation de la vidéoprotection[67].

20 Une fois le CSU communal, intercommunal ou syndical acquis et installé, des agents de la police municipale sont affectés à l'enregistrement et au visionnage des images[68]. Ils représentaient selon la Cour des comptes 10 % des effectifs des polices municipales en 2020[69]. Des agents territoriaux peuvent les épauler. Ils doivent pour ce faire être individuellement agréés par le préfet de département, à l'exclusion de toute prérogative de police judiciaire. Ils sont alors placés sous l'autorité hiérarchique du maire de la commune sur le territoire qui fait l'objet de la vidéoprotection[70] et, potentiellement, du président du conseil départemental dans le cas d'un syndicat mixte ouvert. Cette dernière hypothèse est toutefois limitée au visionnage des images relatives au domaine public départemental (*i.e.* biens immobiliers et voie publique afférente)[71] sur lequel le président du conseil départemental exerce un pouvoir de police[72]. Quant aux maires et à leurs adjoints, officiers de police judiciaire[73], ils sont bien entendu habilités à visionner les images relatives au territoire de leur commune.

21 Quel que soit l'échelon de mise en œuvre[74], cet état des lieux atteste l'existence d'un cadre juridique clair et désormais fourni. Il régit la création et le fonctionnement d'un millier de CSU, notamment équipés par l'entreprise Genetec[75], qui traitent 24 h/24 et

7 j/7 les images tirées du réseau de vidéoprotection. C'est dans ce contexte national qu'il convient d'apprécier deux enjeux spécifiques qui ont agité les arènes parlementaires en 2023.

3/ Les nouveaux visages du droit de la vidéoprotection : traitement automatisé des images et reconnaissance faciale

22 Le 19 mai 2023, est entrée en vigueur la loi JOP 2024. Son article 10 ouvre, à titre expérimental et jusqu'au 31 mars 2025, la possibilité de recourir aux traitements algorithmiques des images de vidéoprotection pour assurer la sécurité de manifestations sportives, récréatives ou culturelles. Les images captées et enregistrées dans les lieux accueillant ces manifestations et à leurs abords, ainsi que dans les véhicules et les emprises de transport public et sur les voies les desservant, peuvent désormais – légalement – faire l'objet d'un traitement automatisé. Il s'agit notamment, par l'ajout au réseau existant de vidéoprotection ou à de nouvelles infrastructures d'une couche logicielle reposant sur la « vision par ordinateur » (*computer vision*)[76], de faciliter l'identification de certains évènements pour déclencher un signalement à l'attention des autorités habilitées à intervenir sur site. Le prérequis à toute vidéosurveillance automatisée (ci-après VSA) est donc l'existence d'un logiciel adapté et programmé à détecter d'éventuelles conduites à risque telles que la présence d'un objet abandonné, le port d'arme, le non-respect d'un sens de circulation, le franchissement interdit d'un périmètre ou d'une zone définie, la formation d'un mouvement de foule, la présence d'une personne au sol ou le départ d'un feu[77].

23 Les sociétés privées du secteur de la vidéosurveillance proposent, depuis plusieurs années déjà, des logiciels plus ou moins opérationnels. De multiples cas d'expérimentation ont d'ailleurs été recensés avant l'entrée en vigueur de la loi JOP 2024. L'entreprise Briefcam[78] a, par exemple, équipé plus d'une trentaine de municipalités françaises en VSA[79]. La société précise que son service offre « des performances supérieures et une précision inégalée [...] pour la détection et la classification des objets, des classes, des attributs et des comportements, y compris la reconnaissance des visages et des plaques d'immatriculation »[80]. D'autres collectivités de l'agglomération lilloise ont choisi de s'équiper du logiciel d'analyse de contenu vidéo de Briefcam via l'entreprise Lumatech[81]. Certaines choisissent de solliciter les logiciels de XXII et de Wintics[82]. Au titre des autres expérimentations, l'entreprise Huaweï a gracieusement mis à disposition de la ville de Valenciennes 217 caméras disposant d'un « traitement intelligent de l'image avec détection des mouvements de foules, objets abandonnés, situations inhabituelles »[83]. Des « caméras intelligentes » susceptibles de « détecter un objet abandonné par exemple et donner l'alerte » ont été installées dans les transports à Rouen[84]. Des solutions d'analyse automatisée des images ont aussi été expérimentées pour différents scénarios (*i.e.* franchissement d'une zone interdite, détection d'une personne au sol, port d'arme), sans résultats probants, au sein de la Gare du Nord à Paris en octobre 2022[85].

24 Si le cadre juridique demeurait incertain avant mai 2023 en l'absence de texte encadrant spécifiquement le recours à la vidéoprotection dite « augmentée », ces usages de la VSA en France n'étaient pas pour autant explicitement prohibés. Le Gouvernement lui-même incitait par voie de circulaire en 2022 et en 2023 à « privilégier l'amélioration de la technologie » dans l'utilisation des crédits du Fonds interministériel de prévention de la délinquance et à « expérimenter le traitement

automatisé de l'image »[86]. Ni interdits ni autorisés, par principe, les usages de la VSA et leur légalité devaient faire l'objet d'une appréciation au cas par cas au regard du droit des données à caractère personnel, en fonction notamment de la finalité du traitement et du type de données traitées[87]. Le déploiement à titre expérimental par l'entreprise Datakalab et la Régie autonome des transports parisiens de dispositifs de détection automatisés dans les transports publics fut ainsi admis par la CNIL. L'initiative, qui s'est déroulée en 2020, pendant l'épidémie de Covid-19[88], à des fins de lutte contre la propagation du virus pour réaliser des actions de sensibilisation et inciter au respect du port du masque en fonction de la fréquentation et du taux de port effectif de protections respiratoires, présentait, selon la CNIL, des garanties essentielles (*e.g.* absence de verbalisation, de traitement de données biométriques et de stockage des images). Seule une réserve persistait à son estime, relative à l'effectivité du droit d'opposition des sujets du traitement[89]. Un décret du 10 mars 2021 est ensuite intervenu pour conférer un fondement juridique clair à ce type d'expérimentation, limiter le droit d'opposition des sujets du traitement de données à caractère personnel, et préciser que les exploitants de systèmes de vidéoprotection pouvaient intégrer durant une année « un traitement logiciel spécifique permettant l'analyse en temps réel du flux vidéo »[90]. L'ambition affichée était toujours de « faire face à l'épidémie de covid-19 » dans les véhicules ou les espaces accessibles au public et affectés au transport public de voyageurs[91].

25 En ce que la VSA procède à une analyse d'image des personnes – ou de véhicules – dans l'espace public, elle constitue un traitement de données à caractère personnel[92] et sa mise en œuvre est, de ce fait, conditionnée au respect du droit d'opposition des sujets filmés[93]. En pratique impossible à assurer de manière effective ou presque, ce droit d'opposition peut être limité. La captation, la diffusion et l'enregistrement d'images issues des caméras de vidéoprotection constituent ainsi des traitements de données à caractère personnel pour lesquels le droit d'opposition a été limité par voie réglementaire[94]. Lorsqu'elle est greffée à ce dispositif de vidéoprotection pour effectuer une analyse automatisée d'images, la VSA constitue un second traitement de données à caractère personnel, qui s'ajoute au précédent, et peut semblablement faire l'objet d'une limitation du droit d'opposition. Dans cette optique, même lorsque la VSA poursuit un intérêt public ou légitime, et lorsqu'elle relève du règlement général sur la protection des données (règlement 2016/679, ci-après RGPD), la limitation du droit des sujets filmés n'est possible que par voie législative ou réglementaire et sous réserve de proportionnalité[95]. Lorsque la VSA relève du champ d'application de la directive police-justice (directive 2016/680), par exemple lorsque sa finalité est la prévention des menaces à la sécurité publique, un fondement idéalement législatif, *a minima* réglementaire, est également nécessaire pour écarter le droit d'opposition ou rendre le traitement indispensable[96]. Pour ces raisons, l'édiction d'une base légale expresse à la VSA était estimée souhaitable par la CNIL[97]. En termes d'opportunité, cette dernière considérait également que l'intervention du législateur était salutaire afin d'assumer sans ambiguïté un « choix autant éthique et politique que juridique », impliquant « de tracer la ligne, au-delà du "techniquement faisable", entre ce qu'il est possible de faire – parce que socialement et éthiquement acceptable – et ce qui ne l'est pas »[98]. C'est finalement l'article 10 de la loi JOP 2024 évoqué *supra* qui a fourni un tel fondement légal, provisoire et expérimental, à compter du 18 mai 2023, toutefois limité à certains usages seulement[99].

26 Moins d'un mois plus tard, le 12 juin 2023, le Sénat adoptait en première lecture une proposition de loi relative à la reconnaissance biométrique[100] – incluant la reconnaissance faciale – dans l'espace public[101]. Celle-ci devait pouvoir être mise en œuvre pour des motifs d'une exceptionnelle gravité et dans des conditions expérimentales. Un nouvel usage potentiel de la vidéoprotection était ainsi proposé. Pour l'heure, la reconnaissance faciale se traduit principalement en France par les 1 687 rapprochements par photographies opérés en moyenne quotidiennement aux fins d'identification automatisée dans le cadre du recours au fichier TAJ (traitement d'antécédents judiciaires)[102]. Au-delà de ces usages, elle demeure plutôt inhabituelle. Le traitement automatique d'images aux fins d'authentification (*i.e.* confirmation d'une identité supposée) ou d'identification (*i.e.* détection de l'identité, sans que celle-ci soit supposée au préalable, à partir d'une recherche dans une base de données comprenant des gabarits ou modèles de visages) n'est permis que dans un cadre strict, le plus souvent sous réserve du consentement explicite, libre et éclairé, de la part des sujets du traitement automatisé de données personnelles[103]. Le système d'authentification PARAFE (passage rapide aux frontières extérieures) dans les aéroports de Lyon, Marseille, Nice, Paris-Charles de Gaulle et Paris-Orly en constitue une illustration saillante[104]. Au titre des autres expérimentations ponctuelles[105], la ville de Nice a mis en service un dispositif temporaire, en février 2019, à l'occasion de son carnaval. Divers scénarios ont pu être testés sur plusieurs milliers de volontaires (*e.g.* repérer des enfants dans la foule, identifier une personne dangereuse dont l'entrée dans un périmètre déterminé était interdite)[106]. En parallèle, un projet d'authentification par reconnaissance faciale à l'entrée de deux lycées pour en contrôler l'accès avait également été amorcé, à l'initiative du conseil régional de Provence-Alpes-Côte d'Azur. Il fut néanmoins contesté, réprouvé par la CNIL[107], puis sanctionné par le juge. Le tribunal administratif de Marseille estima dans ce cas spécifique que la délibération litigieuse était à la fois entachée d'incompétence et adoptée en méconnaissance de l'exigence d'un consentement libre et éclairé. Le public visé se trouvant « dans une relation d'autorité à l'égard des responsables des établissements publics d'enseignement »[108], l'initiative ne pouvait se prévaloir de la clause de l'article 9, 2., a) du RGPD autorisant à titre dérogatoire le traitement de données biométriques sous réserve du consentement des personnes concernées.

27 Malgré ces expérimentations et la proposition de loi susmentionnée, la généralisation de la reconnaissance faciale aux systèmes de vidéoprotection n'est juridiquement et politiquement pas actée[109]. Elle est cependant techniquement envisageable et le ministère de l'Intérieur considérait dès 2020 son expérimentation dans les espaces publics « hautement souhaitable »[110]. Plusieurs sénateurs relevaient deux ans plus tard dans un rapport d'information que, « en théorie, les forces de sécurité intérieure pourraient utiliser la reconnaissance faciale sur un vaste périmètre et à partir d'un réservoir de données conséquent »[111]. En mai 2023, le rapport d'information des députés Philippe Gosselin et Philippe Latombe sur les enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité recommandait de « prévoir un cadre expérimental permettant de tester des solutions de reconnaissance biométrique » et d'autoriser « le traitement en temps réel de logiciels de reconnaissance faciale pour les forces d'intervention pendant une durée limitée »[112]. Le 9 décembre 2023, enfin, la Commission européenne, le Parlement européen et le Conseil de l'Union européenne aboutissaient dans le cadre d'un trilogue à un accord de principe sur la proposition de règlement établissant des règles

harmonisées concernant l'intelligence artificielle au niveau européen (ci-après règlement IA) autorisant le recours – dans des cas limités – aux systèmes d'identification biométrique dans l'espace public à des fins de police, y compris en temps réel[113].

28 La VSA et la reconnaissance faciale, couplées au dispositif existant de vidéoprotection, qui bénéficie d'un renforcement opérationnel, financier et juridique constant, pourraient constituer des moyens communs de la police administrative de demain, quitte à « créer un phénomène d'accoutumance et de banalisation de technologies intrusives » pour les administrés, et, en définitive, « engendrer une surveillance accrue »[114]. Sur ces deux évolutions du traitement de l'image à des fins de police administrative, il convient de souligner l'absence d'intervention en amont des autorités normatives. Ces dernières n'ont pas jugé opportun de poser une interdiction de principe au moment où se développaient des expérimentations dans les collectivités territoriales[115]. Les politiques locales de sécurité des dernières, doublées des investissements énergiques du secteur industriel, ont donc amorcé un mouvement de terrain. Celui-ci fut accompagné tardivement par le pouvoir réglementaire (*e.g.* décret du 10 mars 2021) et le législateur (*e.g.* loi JOP 2023), principalement afin de lui conférer un fondement juridique qui lui faisait défaut et que d'autres avaient pu dénoncer (CNIL, société civile...).

29 À noter que des dispositifs complémentaires sont déployés en parallèle, y compris pour poursuivre des finalités autres que la préservation des troubles à la sécurité publique.

B/ La multiplication des dispositifs numériques de prévention des troubles à l'ordre public : ramifications originales de la technopolice

30 Parmi les outils complémentaires employés, les drones occupent une place de choix, principalement – mais non exclusivement – dans une optique sécuritaire. Un processus similaire à celui observable pour la VSA et, dans une certaine mesure, pour la reconnaissance faciale, opère. Le pouvoir réglementaire et le législateur interviennent après coup, afin de régulariser des usages originaux ayant subi des revers de la part d'autres acteurs, notamment juridictionnels (1). Aux drones s'ajoutent de multiples capteurs (2) et dispositifs de géolocalisation (3) qui poursuivent, eux, d'autres finalités, et font pour l'heure l'objet d'attentions discrètes.

1/ L'essor des drones : un législateur pris de vitesse face à des vents contraires

31 Utilisés ponctuellement avant la crise sanitaire pour des missions de surveillance des frontières ou des manifestations, les drones se sont rapidement installés au-dessus des villes. Le premier confinement, amorcé en 2020, fut l'occasion de massifier l'utilisation de dispositifs vidéo aéroportés[116], pourtant « sujette à caution » selon la Cour des comptes « en raison de son caractère intrusif »[117]. Il s'agissait dans ce cadre, le plus souvent, de contribuer à l'effectivité des mesures sanitaires telles l'interdiction des déplacements ou des regroupements, l'instauration de couvre-feux, la fermeture des parcs ou des marchés en plein air. Les territoires de plusieurs localités furent surveillés par le biais de drones[118]. La surveillance aérienne et la retransmission d'images en haute résolution permettaient une intervention guidée des unités opérationnelles terrestres à des fins de sanction. Dans une perspective de dissuasion, certains drones ont également été employés afin d'émettre – jusqu'à 40 mètres de distance – des

avertissements par le biais de haut-parleurs. D'autres ont, plus accessoirement, permis de procéder à la désinfection des rues, à Cannes, en projetant dans l'espace public une solution d'hypochlorite de sodium diluée[119]. Dans un avis du 20 septembre 2020, le Conseil d'État soulignait justement que « plusieurs technologies peuvent être associées à une caméra aéroportée. Il en est ainsi [...] des logiciels de reconnaissance faciale ou de reconnaissance de plaques minéralogiques, des capteurs thermiques ou de vision nocturne ou des microphones et systèmes d'enregistrement audio »[120]. La diversité des usages et des augmentations possibles des dispositifs aéroportés contribue à les ériger en outils privilégiés des missions de police administrative[121].

32 L'arrêté du 17 décembre 2015 relatif à l'utilisation de l'espace aérien par les aéronefs qui circulent sans personnes à bord n'était, face à ces pratiques nouvelles, que peu pertinent. C'est en définitive une saga contentieuse qui a contribué, par touches successives, à fournir un cadre juridique à l'intervention de ces outils de police déjà largement déployés avec 490 appareils en 2020[122]. Les pratiques de la préfecture de police de Paris entre mars et mai 2020 ont été singulièrement mises en cause. Celle-ci avait eu recours à quatre drones équipés de caméras et de haut-parleurs, pilotés par des fonctionnaires de police, pour capter, durant deux à trois heures de vol en moyenne chaque jour, à hauteur de 80 à 100 mètres, des images, sans enregistrement ni stockage. Ces images étaient retransmises en direct au sol sous forme de flux vidéo sur une tablette au sein du centre d'information et de commandement. L'opération permettait de surveiller la circulation, les rassemblements ainsi que la progression de cortèges en zone urbaine et rurale afin, le cas échéant, de déployer une unité d'intervention chargée de procéder à la dispersion ou à l'évacuation du lieu, sans constater les infractions ni identifier leurs auteurs[123]. Après le tribunal administratif de Paris, statuant en référé[124], le Conseil d'État saisit à son tour l'occasion fournie par cette affaire pour poser quelques principes cardinaux.

33 Tout d'abord, lorsque l'usage de drones poursuit un objectif de prévention et de détection des infractions, spécialement de prévention de certains troubles à la sécurité publique, il tombe dans le champ d'application de la directive police-justice[125] – transposée au sein du titre III de la loi informatique et libertés (ci-après LIL)[126]. Les données collectées sont, ensuite, des données à caractère personnel au sens de la directive dès lors que les drones peuvent voler à basse altitude, sont dotés d'un zoom optique, et sont en mesure de rendre les personnes filmées identifiables[127]. Puisqu'elle repose sur un ensemble d'opérations (collecte, transmission, consultation) effectuées à l'aide de procédés automatisés, cette surveillance aérienne doit, encore, être regardée comme un « traitement » au sens de ladite directive[128]. Ce traitement de données à caractère personnel poursuit, certes, un objectif légitime, sans porter en soi une atteinte grave et manifestement illégale au droit à la protection de la vie privée et à la liberté d'aller et venir[129]. Il doit toutefois, puisqu'il est mis en œuvre pour le compte de l'État, bénéficier d'un fondement réglementaire, par arrêté ou décret pris après avis motivé et publié de la CNIL[130]. Ce fondement doit autoriser expressément le traitement, en fixer les modalités et les garanties nécessaires[131]. À défaut, l'atteinte au droit au respect de la vie privée et à la liberté d'aller et venir sera caractérisée. Tel était le cas en l'espèce en l'absence de base réglementaire. Le Conseil d'État enjoignit logiquement à l'État de cesser toute surveillance par drone jusqu'à l'adoption d'un texte réglementaire ou, en alternative, jusqu'à la neutralisation technique des caméras

aéroportées afin d'empêcher toute identification des personnes filmées par un procédé qui deviendrait alors dissociable d'un traitement de données à caractère personnel[132].

34 Consécutivement à l'ordonnance rendue par le Conseil d'État en mai 2020, la préfecture de police de Paris continua à assurer la surveillance de grands évènements, notamment de manifestations sur la voie publique, par le biais de drones. Elle adjoignit simplement à ses anciens appareils un logiciel de floutage des données à caractère personnel transmises en temps réel à la salle de commandement. Le procédé fut jugé insuffisant par le Conseil d'État en décembre 2020. Si l'opération de visionnage du flux vidéo ne comprenait, certes, plus de données à caractère personnel, les opérations de collecte des images, de transmission vers le serveur de floutage, la décomposition du flux image par image afin d'opérer un tri et procéder au floutage reposaient, elles, sur de telles données. Conçues dans leur ensemble, ces opérations étaient toujours constitutives d'un traitement de données à caractère personnel pour le compte de l'État au sens de la directive police-justice, laquelle est également applicable en cas de surveillance des manifestations à des fins de prévention des menaces à la sécurité publique[133]. Les conditions posées par la directive et la LIL tenant à l'exigence d'un fondement *a minima* réglementaire ne pouvaient de la sorte être contournées et le Conseil d'État conclut, à nouveau, à l'illégalité du traitement. Il conclut en outre à la suspension de l'exécution de la décision du préfet de police de poursuivre le recours à la surveillance par drones à des fins de police administrative « tant que n'aura pas été pris un texte autorisant la création, à cette fin, d'un traitement de données à caractère personnel »[134].

35 Cette nouvelle ordonnance prolongeait des précisions déjà énoncées quelques mois plus tôt par la section contentieuse dans un avis rendu en septembre 2020 sur saisine du Premier ministre. En dépit d'un encadrement « parcellaire » du recours aux drones, principalement eu égard à la sûreté aérienne, le Conseil d'État avait là encore insisté sur l'absence « de fondement juridique permettant explicitement l'usage de ces dispositifs ainsi que l'exploitation des images captées par les autorités publiques concernées, qu'il s'agisse de l'État (police nationale, gendarmerie nationale, personnels chargés de la sécurité civile, etc.) ou encore des collectivités territoriales (polices municipales notamment) »[135]. Afin de pallier cette carence, le Palais royal envisageait dans un premier temps l'intervention d'un décret en Conseil d'État, plus que d'un arrêté du ou des ministres compétents, considérant, d'une part, que cette forme était exigée en cas de traitement de données sensibles, et que, d'autre part, le survol en particulier des manifestations organisées sur la voie publique et la collecte de données identifiantes étaient susceptibles de révéler les opinions politiques, les convictions religieuses ou philosophiques et l'appartenance syndicale des administrés, qui constituent de telles données sensibles au sens de l'article 6 de la LIL[136]. Mais la section contentieuse insista dans un second temps sur le fait que la surveillance aérienne, eu égard aux atteintes qu'elle est susceptible de porter au droit au respect de la vie privée comme à ses conséquences potentielles sur la procédure pénale, relevait du domaine d'intervention réservé du législateur, parmi lequel figurent les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques[137]. Seule une loi pouvait en conséquence autoriser ce traitement, en définir les finalités, désigner les autorités chargées d'y procéder et prévoir les garanties d'un usage proportionné, incluant le respect du droit à l'information et la limitation de la conservation des éventuels enregistrements[138].

36 Après une tentative mise en échec par le Conseil constitutionnel en 2021[139], c'est la loi relative à la responsabilité pénale et à la sécurité intérieure du 24 janvier 2022 qui permit finalement de fixer le cadre juridique tant attendu du recours aux drones pour des missions de police administrative générale[140]. Son article 15 introduisit au sein du CSI les articles L. 242-1 à L. 242-8 qui instaurent un régime d'autorisation préalable du recours aux drones, sur décision du préfet de département ou du préfet de police, pour une durée maximale de trois mois, renouvelable[141]. Plusieurs finalités limitativement énumérées peuvent justifier leur emploi : la sécurité des personnes et des biens, la protection des bâtiments ou installations publics et de leurs abords immédiats lorsqu'ils sont particulièrement exposés à des risques, la sécurité des rassemblements sur la voie publique ou dans des lieux ouverts au public, la prévention d'actes de terrorisme, la régulation des flux de transport, la surveillance des frontières et, enfin, le secours aux personnes. Sont toutefois exclus les captations de son, les traitements automatisés de reconnaissance faciale, les conservations d'enregistrement au-delà de sept jours ainsi que les rapprochements, interconnexions et mises en relation automatisés, avec d'autres traitements de données à caractère personnel[142]. Surtout, le Conseil constitutionnel a posé une exigence stricte de proportionnalité du recours aux drones, en insistant sur l'obligation de justifier sa nécessité. L'autorisation requise 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 »[143].

37 Ces garanties et cette réserve suffirent à assurer la constitutionnalité des dispositions, du moins lorsque leur mise en œuvre a vocation à soutenir l'action des services de la police nationale, de la gendarmerie ou de l'armée. Le Conseil constitutionnel y ajouta une réserve d'interprétation moindre sur l'interdiction des traitements automatisés de reconnaissance faciale[144] et une censure de la procédure d'urgence envisagée à titre dérogatoire, substituant un régime de déclaration préalable au régime normal d'autorisation préalable du préfet[145]. En revanche, il censura net les dispositions autorisant à titre expérimental les services de la police municipale à recourir aux drones dans leur mission de prévention des atteintes à l'ordre public, avant tout pour assurer la sécurité des manifestations sportives, récréatives ou culturelles. La conciliation opérée par le législateur entre l'objectif à valeur constitutionnelle de sauvegarde de l'ordre public et la protection de la vie privée n'était, dans ce cas précis, pas proportionnée, à défaut de garanties supplémentaires (*e.g.* restriction des usages aux évènements particulièrement exposés, suspension par le préfet de l'autorisation délivrée)[146].

38 Toujours est-il que le CSI fournit désormais un fondement légal solide, qui fut un an plus tard complété par le décret 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[147]. Précisément, l'Association de défense des libertés constitutionnelles (ADELICO), soutenue par cinq autres associations et syndicats[148], forma un référé-suspension à l'encontre de ce décret. S'il rejeta la requête des associations, le Conseil d'État rappela néanmoins à son tour l'exigence de proportionnalité du recours aux drones[149]. Cette exigence de nécessité des moyens employés est depuis vérifiée par le juge administratif, au cas par cas, pour chaque décision d'autorisation dispensée par le préfet[150].

39 C'est sous cet angle que fut contestée en juillet 2023 la décision du préfet des Pyrénées-Atlantiques d'autoriser la captation, l'enregistrement, et la transmission d'images au moyen de caméras installées sur des aéronefs survolant la frontière franco-espagnole sur les territoires des communes d'Hendaye et Urrugne. Le tribunal administratif de Pau, saisi du litige, opéra un contrôle *in concreto* détaillé en tenant compte d'une diversité de paramètres : éléments objectifs ayant fondé la décision du recours aux drones, motifs du choix de la zone de survol et de la détermination de sa superficie, nombre d'habitations présentes dans la zone, possibilité et efficacité du recours à des moyens alternatifs comme une surveillance par véhicules terrestres. Au terme de ce contrôle, il fit droit à la requête des associations[151]. Son appréciation fut confirmée par le Conseil d'État, statuant en référé le 25 juillet 2023, qui retint à son tour l'insuffisance d'éléments suffisamment circonstanciés pour « justifier, sur la base d'une appréciation précise et concrète de la nécessité de la proportionnalité de la mesure, que le service ne peut employer [...] d'autres moyens moins intrusifs au regard du respect de la vie privée [...] ou que l'utilisation de ces autres moyens serait susceptible d'entraîner des menaces graves pour l'intégrité physique des agents »[152]. L'exigence de proportionnalité semble, pour l'heure, faire l'objet d'une vérification méticuleuse de la part du juge administratif[153]. Elle complète utilement un cadre juridique qui a surgi ces dernières années en réaction aux résistances du Conseil d'État, et moindrement du Conseil constitutionnel, bien alimenté par des contentieux stratégiques lancés par la société civile. Face à ces vents contraires, le législateur et le pouvoir réglementaire ont encore réagi pour entériner des cas d'usage croissants qui, forts de leur ancrage juridique, ont d'autant plus été banalisés.

40 À cet égard, et à titre d'illustration, la surveillance par drones fut à nouveau convoquée à Paris, dans les Hauts-de-Seine et la Seine–Saint-Denis en juillet 2023, à des fins sécuritaires et en réaction à plusieurs nuits d'émeutes, sans encourir l'annulation du tribunal administratif de Paris[154]. Le tribunal administratif de Grenoble, lui, sanctionna l'usage de caméras aéroportées en l'absence d'autorisation préalable du préfet de l'Isère et à défaut d'information des participants à une manifestation ciblée par la captation des images. Il enjoignit en complément au préfet de procéder à l'effacement sans délai des enregistrements[155]. Quant au tribunal administratif de Rouen, il ordonna la suspension pour défaut de proportionnalité de l'arrêté du préfet de l'Eure portant autorisation de captation, d'enregistrement et de transmission d'images à l'occasion d'un rassemblement écologiste en opposition à un projet autoroutier[156]. Plus généralement, il est possible de constater une multiplication des arrêtés préfectoraux autorisant le survol de zones par des drones. Sur la seule période allant d'avril à juillet 2023, des arrêtés ont été adoptés dans plus d'une trentaine de départements sur le territoire national. Ils poursuivaient diverses finalités, par exemple prévenir les troubles à l'ordre public à l'occasion du festival d'Avignon[157], des festivals de musique « We Love Green » et « Lollapalooza » à Paris[158], d'une « rave-party » dans la Manche[159], du « Merguez Tuning Show » dans la Nièvre[160], d'une manifestation un 1er mai[161] et de la fête de la musique à Nantes[162], de concerts au Stade de France (Beyoncé, Mylène Farmer, Muse, Blackpink, Rammstein et The Weeknd[163]), de la « fête de la violette » dans le Loir-et-Cher[164], d'un déplacement du Premier ministre à la Réunion[165], d'une manifestation d'extrême-droite dénonçant l'implantation d'un centre d'accueil pour demandeurs d'asile à Saint-Brévin-les-Pins[166], du Tour de France dans l'Ain[167], de manifestations sportives d'ampleur (édition 2023 du tournoi de Roland-Garros, finales de la Coupe de France et du Top 14, match de l'équipe nationale de football et répétition

de la cérémonie d'ouverture des Jeux olympiques et paralympiques[168]), ou encore pour empêcher la tenue de rodéos urbains dans plusieurs départements[169] et prévenir le trafic de stupéfiants à Martigues[170]. La seule préfecture de police de Paris adopta entre avril et octobre 2023, sur une période de sept mois, pas moins de quatre-vingt-seize arrêtés autorisant le recours aux drones sur le territoire francilien. De telle sorte qu'il est possible de considérer que le recours à ces dispositifs alimente le phénomène étudié et bâtit, avec la vidéoprotection, les contours d'une technopolice administrative partiellement – et tardivement – saisie par le droit. Celle-ci repose encore sur d'autres dispositifs, plus accessoires.

2/ Le frémissement des capteurs : expérimentations diverses et clandestines

41 Parmi les autres dispositifs figurent une multitude de capteurs dont se sont dotées plusieurs villes de France. Des capteurs de niveau sonore sont en particulier employés afin d'assurer la tranquillité et la sécurité publiques en détectant d'éventuelles nuisances qui, en 2024, ne disposent pas encore d'assise réglementaire ou législative expresse.

42 Une première expérimentation fut en ce sens amorcée par Saint-Étienne Métropole en 2019 afin d'équiper un quartier d'une dizaine de capteurs, intégrés dans le mobilier urbain, disposés sur le domaine public, au sol ou dans les parcs[171]. Leur fonction consistait à détecter les anormalités sonores pour générer une alerte transmise au CSU qui pouvait, ensuite, dépêcher une patrouille de police municipale sur place, après éventuelle vérification de la situation par l'entremise de la vidéoprotection. Parmi les bruits anormaux à détecter figuraient les coups de feu, cris, utilisations de perceuse, accidents, klaxons, coups de sifflet, chocs, utilisations de bombe aérosol, crépitements, éclatements de pneumatique ou bris de vitre[172]. Cette expérimentation fut toutefois abandonnée à la suite d'un avertissement émis par la CNIL le 25 octobre 2019[173]. En cas d'utilisation cumulée des capteurs sonores et de la vidéoprotection, le procédé permettait une identification des auteurs de sons, y compris à faible intensité comme les voix et les conversations. L'autorité administrative indépendante considéra que ce traitement de données à caractère personnel était contraire à la LIL et au RGPD. Elle estima au surplus qu'à défaut d'applicabilité des dispositions du CSI, limitées à une surveillance visuelle, le principe, la portée comme les garanties dont doit être assortie la « captation indifférenciée et généralisée de sons dans l'espace public » supposent une intervention du législateur[174]. Les répercussions sur les « garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques »[175], comme le droit au respect de la vie privée, les libertés d'expression, de réunion, de manifestation, d'association et la liberté d'aller et venir, *a fortiori* en cas de couplage des capteurs sonores avec la vidéoprotection ou de caméras aéroportées, rendent même cette intervention indispensable. L'obligation de prévoir un fondement juridique solide limitant le droit d'opposition au traitement de données à caractère personnel et autorisant le traitement de données sensibles plaide encore pour une intervention à cette échelle. Le cadre législatif n'a, pour l'heure, pas évolué sur ce point. L'hypothèse d'une intervention *a posteriori* du législateur pour conférer un fondement aux usages expérimentaux ne peut cependant être écartée.

43 Cette consécration législative d'un fait politique existant apparaît d'autant plus crédible que d'autres collectivités et établissements ont depuis développé des initiatives similaires. Paris a implanté à titre expérimental des « radars sonores »[176], des

capteurs « Méduses »[177], et a mis en place une cartographie des décibels mesurés[178]. La Régie des transports de Marseille, elle, a équipé certaines rames de métro de « systèmes d'enregistrements [...] sonores d'ambiance »[179] afin de détecter cris, insultes et menaces, notamment en cas d'agression[180]. Surtout, la commune d'Orléans s'est distinguée par une convention conclue le 12 octobre 2021 avec l'entreprise Sensivic, document une fois de plus obtenu par la Quadrature du Net. Par cette convention, qui a pour objectif « la préservation de l'ordre et de la tranquillité publics »[181], le maire d'Orléans a autorisé ladite entreprise à déployer et à tester des capteurs sonores gracieusement offerts à la commune. Ces derniers étaient articulés au dispositif de vidéoprotection afin d'« analyser en permanence le son ambiant pour pouvoir détecter des anomalies »[182] et émettre une alerte à destination de la police sans retransmission du son ni enregistrement. L'alerte générée permettait là encore d'orienter les caméras vers la source des bruits suspects[183]. Prévue pour une durée d'un an, renouvelable, l'expérimentation s'est achevée en octobre 2022 après avoir été contestée devant le tribunal administratif d'Orléans, qui demeure à ce stade saisi du litige[184]. De son côté, la CNIL a émis un avertissement à la municipalité le 25 septembre 2023, maintenant sa position exprimée en 2019 au sujet de l'expérimentation stéphanoise[185]. En réaction, la ville a manifesté son intention de soutenir la discussion d'un projet ou d'une proposition de loi « pour permettre la mise en place d'un tel dispositif dès 2024 »[186].

44 Au-delà de la seule captation de sons, les municipalités diversifient les dispositifs utilisés pour assurer la tranquillité et la sécurité publiques. À cet égard, la ville de Nice honore sa réputation. Elle a doté des bâtiments recevant du public (établissements scolaires, salles de spectacle, hôpitaux, commerces) de 1 400 boîtiers d'alerte reliés au CSU. Ils permettent, sur actionnement des usagers, de faciliter l'intervention de la police sur place. 244 bornes d'appel d'urgence permettent aussi aux administrés de signaler des atteintes aux biens ou aux personnes auprès de la police municipale pilotant le CSU, laquelle peut si nécessaire avoir recours aux 108 haut-parleurs émettant des messages d'alerte et de prévention en réaction[187]. De son côté, la ville de Metz a installé des capteurs thermiques[188] détectant la présence d'individus aux abords de passages piétons afin de réguler les feux de signalisation lumineux en fonction du nombre de personnes estimées être en attente d'une traversée[189]. L'ambition affichée est de réduire le temps d'attente de ces dernières afin de limiter autant que possible des traversées non conformes au Code de la route et, de la sorte, améliorer la sécurité routière et prévenir les accidents.

45 Outre la sécurité et la tranquillité publiques, les installations peuvent avoir pour objectif d'optimiser la santé publique. Tel est le cas lorsque d'autres capteurs et sondes installés à Dijon mesurent les niveaux de température, le taux d'ensoleillement, la force du vent et la qualité de l'air. Il s'agit alors, dans le cadre de la mise en place d'un observatoire environnemental, d'évaluer le climat urbain, pour identifier les îlots de chaleur[190], soutenir et orienter la végétalisation de l'espace public, mais aussi « renseigner les particuliers sur les espèces végétales à préconiser dans les jardins »[191]. L'initiative peut ici être rapprochée de celle de l'Observatoire de la qualité de l'air en Île-de-France qui a instauré une cartographie détaillée des polluants et particules biologiques présents dans l'air[192]. Optimisation de l'environnement urbain de la *smart city* dans un contexte de réchauffement climatique et prévention des troubles à la santé publique constituent ici les objectifs poursuivis, sans que les répercussions sur les

droits fondamentaux ne soient toutefois équivalentes à celles engendrées par les dispositifs précédemment évoqués.

46 La salubrité publique constitue, enfin, un autre débouché de la *smart city*, en particulier lorsque des capteurs de poids installés sur des poubelles collectives contribuent à la collecte des déchets et optimisent les passages des services de ramassage d'ordures. Une taxation liée à l'émission de déchets des ménages peut encore être envisagée et exige le recours à des cartes individuelles d'ouvertures de bennes à ordures – impliquant cette fois le traitement de données à caractère personnel[193].

47 *In fine*, le potentiel et la diversification des capteurs ou sondes sont susceptibles de les ériger en outils complémentaires de la police administrative, en parallèle d'un usage plus classique de ces instruments dans le cadre des réseaux intelligents (*smart grids*) destinés à la gestion des flux et à la réduction de la consommation énergétique (*e.g.* éclairage connecté avec modulation de la puissance d'éclairement en fonction de la fréquentation[194], régulation du trafic[195]). Tous ne présentent pas le même degré d'intrusion selon qu'ils mesurent de simples flux, des données météorologiques ou des données à caractère personnel. Mais tous se développent côte à côte dans le cadre d'un *continuum* d'équipement technologique des villes et de leurs politiques urbaines qui croît sans faire l'objet d'une régulation spécifique. Ces capteurs sont, le cas échéant, articulés à d'autres appareils, par exemple de géolocalisation.

3/ L'émergence de dispositifs de géolocalisation : *terra nova*

48 S'ils sont plus rares, les dispositifs de géolocalisation fournissent de nouvelles données susceptibles d'être interconnectées avec d'autres, sonores ou visuelles. À ce stade, force est de constater que les données collectées par les collectivités qui concernent la localisation des administrés le sont avant tout dans une optique d'aménagement du territoire et non de pure police administrative[196]. Il s'agit avant tout de décongestionner, de désengorger, de dédensifier les flux[197]. Les deux cadres d'action ne sont cependant pas dénués de tout lien et les techniques développées dans une optique d'aménagement pourraient, à brève échéance, se voir assigner des finalités autres, y compris de police.

49 Le périmètre peut, d'abord, concerner les transports publics. L'entreprise Flowly propose ainsi un « dispositif d'analyse des flux de voyageur » qui repose sur la collecte de l'adresse « physique » (ou adresse MAC – *Media Access Control*) des *smartphones* des administrés. En estimant l'affluence et la charge des véhicules, elle explique servir une multitude de finalités : « ajuster l'offre de mobilité », « satisfaire un besoin dans une zone précise, s'adapter aux nouvelles contraintes sanitaires, restructurer tout ou partie d'un réseau, calibrer son offre, estimer la fraude, augmenter la productivité »[198]. Plusieurs collectivités en France ont adopté ce service (Avignon, La Réunion, Rouen, Valence). D'autres, comme la métropole de Lyon, ont adopté des solutions similaires[199]. Plus largement, les collectivités peuvent vouloir recueillir des données sur l'ensemble du trafic routier. La collecte peut être directe ou, considérant l'importance des coûts à engager pour la personne publique, indirecte, dans le cadre d'un échange de données avec une plateforme privée qui centralise les remontées d'informations de ses utilisateurs. À ce titre, la plateforme de navigation Waze propose aux collectivités depuis 2015 le service « *Waze Connected Citizens* ». En résumé, « la startup fournit un outil de monitoring urbain en échange de données de la ville telles que les données liées aux travaux en cours ou à venir, aux accidents, etc. »[200]. Le laboratoire

d'innovation numérique de la CNIL relevait en 2018 que plusieurs départements et villes moyennes, comme Versailles, avaient souscrit à cette offre en France[201]. L'entreprise multiplie de son côté les arguments pour favoriser les souscriptions des acteurs publics : prévenir les accidents, sécuriser les routes, protéger la population en cas de catastrophe naturelle ou, plus simplement, moderniser le réseau routier, améliorer la circulation et réduire les embouteillages[202]. Cet outil présente, il est vrai, des plus-values évidentes, y compris à des fins de maintien de l'ordre. Plus modestement, les dispositifs de géolocalisation peuvent enfin être utilisés pour mesurer le flux de promeneurs ou la fréquentation d'un centre commercial par des consommateurs[203].

50 Ces différents procédés reposent sur le recueil de données transmises par les citoyens, dans le cadre d'une remontée active d'informations (*crowdsourcing*) ou d'une collecte passive de données « de poche » (*pocketsourcing*). Les téléphones individuels font dans ce dernier cas office de capteurs mesurant les déplacements. Le laboratoire d'innovation numérique de la CNIL relevait à ce sujet, toujours en 2018, non sans ironie : « si les citoyens s'équipent à leurs frais de capteurs modernes et payent eux-mêmes la connexion, il ne paraît pas absurde du point de vue de l'efficacité publique d'en tirer parti »[204]. La puissance publique pourrait choisir à l'avenir d'accentuer l'efficacité de son action en recourant de manière plus appuyée à la collecte de données « de poche ». Elle s'inscrirait alors dans un cadre juridique vierge, ou presque, le CSI n'encadrant pour l'heure que le recueil de ces données à des fins de renseignement[205]. En dehors de cette hypothèse, le législateur et le pouvoir réglementaire n'accordent aux dispositifs envisagés aucune considération spécifique en matière de police administrative. Mais une *terra nova* n'est généralement nouvelle que pour celui qui y pénètre pour la première fois. Si le droit de la sécurité intérieure ignore pour l'heure ces techniques, d'autres pans du droit s'y appliquent.

51 Le droit des données à caractère personnel a précisément infligé un premier revers à cette technologie devant le Conseil d'État en 2017 dans le cadre d'une utilisation privée par la société JCDecaux[206]. La CNIL avait en 2015 refusé à l'entreprise la délivrance d'une autorisation nécessaire à la mise en œuvre d'une mesure quantitative des flux de passants sur la dalle de la Défense[207]. L'expérimentation souhaitée, pour une durée de quatre semaines, consistait en l'installation et l'exploitation « de six boîtiers de comptage wifi, présents sur les mobiliers publicitaires »[208]. Ces derniers devaient permettre « de capter les adresses des appareils mobiles présents dans l'environnement immédiat (portée maximale de 25 mètres de rayon) et dont l'interface wifi [aurait été] activée » afin « de mesurer les volumes de fréquentation, les taux de répétition et les schémas de mobilité »[209] pour, en définitive, « améliorer la valorisation [des] panneaux publicitaires » de la société[210]. Ce refus de la CNIL fut attaqué devant le Conseil d'État qui, à son tour, considéra que le traitement de données à caractère personnel envisagé était illégal en ce qu'il ne garantissait pas l'anonymisation des données[211].

52 En définitive, entre caméras, CSU, VSA, drones, capteurs, sondes, microphones et *smartphones*, les supports des activités de police administrative semblent en pleine diversification, de telle sorte qu'un phénomène de « Technopolice » administrative peut bel et bien être qualifié. Il gagne à être saisi à la lueur de pratiques déjà analysées aux frontières européennes qui ont été désignées en juillet 2023 par la formule de « *Techno-borders* ». Dans les deux cas, les termes se rapportent à « une vaste infrastructure composée de systèmes de surveillance, de bases de données, de

techniques d'identification biométrique et de réseaux d'information [qui] a été instaurée afin de fournir aux autorités [publiques] une connaissance – et par voie de conséquence un contrôle sur – des [sujets de droit] » spécifiques, en l'occurrence des administrés dans la configuration étudiée[212]. Un mouvement similaire affecte, bien sûr, les activités de police judiciaire. Tombent dans ce champ les pratiques croissantes de vidéoverbalisation : dispositifs « LAPI » (lecture automatisée de plaques d'immatriculation)[213], vidéosurveillance automatisée permettant la constatation d'infraction en cas de dépôt sauvage d'ordure à Roubaix[214], ou de circulation sur les voies réservées aux bus à Paris[215]. Tombe aussi dans le champ de la police judiciaire le recours aux technologies de police prédictive : outils cartographiques et statistiques comme « *Map Revelation* », utilisés par plusieurs collectivités, et « Paved » (plateforme d'analyse et de visualisation évolutive de la délinquance), par la gendarmerie nationale[216]. Tombent toujours dans ce champ les fichiers de police dont les bases de données ne cessent de croitre[217]. Ces pratiques excèdent toutefois le périmètre de la présente contribution qui porte sur l'« *instauration* »[218] d'une technopolice *administrative*.

53 Face à ce phénomène, l'analyse montre que la norme suit les usages, tant et si bien que « les dispositions législatives et réglementaires constituent une vitrine du savoir-faire technologique en matière de sécurité »[219]. Mais tous les produits ne sont pas en vitrine, car le législateur et le pouvoir réglementaire agissent au « coup par coup ». La réaction s'avère parfois tardive, et il n'est pas rare que l'adaptation du droit se fasse longtemps après la survenance des premiers cas d'usage – ce qui justifie au demeurant pour le juriste de les considérer attentivement dès leurs prémices. Surtout, puisque la sécurité fait des bonds en avant, mais qu'elle « tolère difficilement les marches arrière »[220], le risque est réel de voir les autorités normatives n'intervenir *a posteriori* que pour intégrer au droit existant les équipements technologiques déjà mobilisés dans les villes[221]. Pour l'heure, les résistances de la CNIL et des juridictions tempèrent utilement les expérimentations trop audacieuses des collectivités, souvent après une contestation à l'initiative de la société civile qui anime les contentieux stratégiques et assume un rôle de vigie. La fragilité de ce scénario implique toutefois, comme l'a fait le Conseil d'État, d'anticiper autant que possible les effets de ces nouvelles infrastructures de la police administrative pour favoriser une régulation rapide, maitrisée plus que subie.

II/ – Anticiper les répercussions des nouvelles infrastructures de la police administrative pour réguler les rapports de l'administration aux tiers

54 De la mutation des outils de l'action publique est susceptible de découler une transformation des relations de l'administration aux tiers, entreprises cocontractantes comme administrés. De nouveaux défis se dévoilent alors, et imposent de questionner l'adéquation des moyens qui régulent en l'état ces relations, tant au stade de l'exercice des missions de police (A) que de l'engagement de la responsabilité (B).

A/ Des rapports incertains dans l'exercice des missions de police administrative : questionnements prospectifs

55 Plusieurs réflexions gagnent à ce titre à être menées afin de saisir l'effet transformatif des nouvelles technologies, en particulier du recours aux systèmes d'IA[222]. Il est d'abord possible de s'intéresser à la régulation contractuelle des collaborations public-privé et aux moyens qui permettent d'assurer une maîtrise des données, du fonctionnement et des usages des systèmes d'IA (1). Le développement de ces systèmes, par exemple dans le cadre de la VSA, implique encore de confronter sans attendre la conception des logiciels utilisés par la personne publique à l'interdiction de délégation de missions de police administrative générale (2). Quant à la transformation des rapports de l'administration aux administrés, elle génère à son tour plusieurs interrogations. Parmi elles figure la question du statut des citoyens qui collaborent à la gestion publique par le biais d'applications numériques mises en service par les collectivités territoriales (3).

1/ L'encadrement nécessaire des relations contractuelles entre administration et entreprises au nom de l'intérêt général

56 La structure technologique ci-dessus envisagée sur laquelle repose désormais l'action des collectivités et des pouvoirs publics suppose l'acquisition d'un équipement par ces derniers. Or, la provenance de cet équipement revêt un caractère éminemment stratégique dès lors que sont en cause des activités de police. Une recherche d'autonomie favorisera une conception publique de ces équipements quand, à l'opposé, une conception privée, par choix ou par nécessité, exposera les acteurs publics à un risque de dépendance. Le Conseil d'État ne s'y trompait pas lorsqu'il soulignait en 2022 au sujet des systèmes d'IA l'importance de l'« arbitrage entre "faire" et "acheter" (option au sein de laquelle on pourrait distinguer "faire faire" [*i.e.* sur mesure] et "acheter tout fait" [*i.e.* sur "étagères"]) »[223]. En l'état, force est de constater que les expérimentations en cours écartent systématiquement ou presque l'option d'une conception interne des outils employés. Le projet de ville intelligente OnDijon est réalisé par quatre entreprises (Bouygues, Citelum, Suez et Capgemini) dans le cadre d'un contrat de concession d'une durée de vingt ans[224]. L'entreprise Thalès est le véritable « chef de file » de l'ambitieux projet de *Safe city* expérimenté durant trois années à Nice[225]. Et il serait possible de multiplier les exemples, détaillant tour à tour les partenariats conclus par conventions entre Saint-Étienne et Serenicity, entre Orléans et Sensivic, entre Rouen et Flowly, entre Valenciennes et Huawei, entre Paris et Evitech, entre Cannes et Datakalab, sans oublier l'entreprise Briefcam qui équipe de nombreuses collectivités françaises[226]. Tant et si bien que ne peut être récusée l'appréciation de Bertrand Warusfel lorsqu'il estime que le « techno-solutionnisme sécuritaire [...] renforce également l'incitation à la privatisation croissante des missions et des prestations de sécurité »[227]. La mise à disposition à titre gracieux de certains dispositifs en phase de test tend même à présenter les collectivités sous les traits de cobayes, certes à moindres frais, de produits en voie de commercialisation[228].

57 Derrière l'enjeu de la provenance des technologies se cache en réalité la question de leur coût. Considérant d'une part les frais colossaux inhérents au développement d'une expertise en interne, plus encore pour des collectivités de taille modeste, et, d'autre part, la centralisation déjà forte des compétences au sein du secteur privé, l'option du « faire faire », voire du « acheter tout fait », semble s'imposer malgré quelques mises en

garde[229]. À noter que les coûts ne se limitent pas au financement de la recherche, au développement du système d'IA et à son acquisition, mais s'étendent, en outre, à sa maintenance et à l'entraînement constant de ses algorithmes afin de conserver des niveaux de performance acceptables[230]. À défaut d'expertise humaine préexistante et de latitudes budgétaires, et à moins d'une mutualisation massive des moyens, il est à parier que les collectivités s'équiperont directement – hors tests gracieux et sur mesure – sur les stands des industriels (au salon Milipol Paris, via les catalogues de l'AN2V…)[231].

58 Dans cette configuration, le risque important de marchandisation des données de l'espace public ne saurait être nié, y compris des données des administrés. Par exemple, la loi JOP 2024 prévoit qu'« afin d'améliorer la qualité de la détection des événements prédéterminés » par le recours à la VSA, « un échantillon d'images collectées […] au moyen de systèmes de vidéoprotection […] peut être utilisé comme données d'apprentissage » pendant une durée de douze mois[232]. En cas d'externalisation – probable – de la conception et du développement des logiciels de traitement automatique des flux vidéo, qui seront sans doute vendus après la phase d'expérimentation, la matière première du produit commercialisé provient par conséquent de l'espace public et des administrés. Plus prosaïquement, pour la Quadrature du Net : « Les industries de la sécurité peuvent donc faire du profit sur les vies et les comportements des habitants d'une ville, améliorer leurs algorithmes de répression et ensuite les vendre sur le marché international »[233]. L'association mentionne à titre d'illustrations l'amélioration du dispositif de reconnaissance faciale de la société Idémia grâce au premier dispositif PARAFE installé dans les aéroports ainsi que l'entraînement des algorithmes de la société XXII grâce à l'exploitation du système de vidéoprotection à Suresnes[234]. Le Conseil d'État avait déjà formulé des observations similaires un an plus tôt, quoiqu'ayant recours à un registre moins incisif. Il soulignait en particulier le grand risque « d'un transfert indu de richesse (et de données) que les pouvoirs publics doivent se donner les moyens d'éviter »[235].

59 Dans ce contexte, si l'externalisation des solutions technologiques employées par les collectivités devait être actée, elle gagnerait à l'être en étant encadrée par des garanties contractuelles lors de la passation des contrats et marchés publics afin d'assurer la maîtrise des données, du fonctionnement et des usages des outils acquis. En effet, il est probable, et pourtant non souhaitable du point de vue de la protection des données et de l'intérêt général, que les industriels reproduisent en l'absence de contraintes contractuelles un fonctionnement économique fondé sur la monétisation des données et la publicité[236]. Le Laboratoire d'innovation numérique de la CNIL s'inquiétait à cet égard de la fréquence avec laquelle diverses entreprises concessionnaires se trouvent en possession de données détaillées, des utilisations commerciales qui pourraient en être faites, mais aussi de l'absence d'accès à ces données pour les personnes publiques délégataires, qui se trouvent alors dans une position « doublement délicate »[237]. En réaction, le Laboratoire d'innovation numérique soutenait la perspective d'un développement des partenariats public-privé, caractérisés par deux atouts décisifs, en l'occurrence des relations contractuelles établies sur le long terme et modulables par le biais de clauses de renégociation. Pour éviter un « verrouillage du contrat » et une « asymétrie informationnelle », cette option était présentée comme un gage de flexibilité et de transparence[238]. Parce que les systèmes d'IA évoluent à une rapidité particulièrement soutenue, il est toutefois possible que l'intérêt public ne soit pas idéalement servi par le développement d'un partenariat à long terme avec un même acteur, bien que celui-ci dispose d'un avantage technologique à un instant précis. Dans

ce cas, outre le mode de contractualisation, ce sont plutôt les clauses elles-mêmes qui peuvent sécuriser les intérêts de la personne publique.

60 Au titre des objectifs qui pourraient leur être assignés, mentionnons une exigence de transparence et de disponibilité des données collectées dans l'espace public et dans les lieux ouverts au public, possiblement à partir de l'observation du comportement des administrés. La disponibilité de ces données sert indubitablement les intérêts de la personne publique. Elle lui permet de mieux appréhender ses besoins, de les affiner, et de préciser les missions de ses cocontractants futurs, tout en étant en mesure de mieux les choisir. Elle permet encore de renégocier si nécessaire les conditions de partenariats en cours[239]. Cette mise à disposition des données collectées pourrait également servir le développement de l'OpenData à l'instar de ce qui est promu dans la métropole de Nantes ou à Paris[240]. Le contrat de délégation de service public conclu entre le syndicat mixte ouvert Autolib' Vélib' Métropole (maître d'ouvrage) et l'entreprise Smovengo (prestataire), qui a succédé en 2017 à JCDecaux, comprend en ce sens une clause relative à la communication des données d'exploitation (*e.g.* localisation des bornes, disponibilités des véhicules) qui peut servir le développement de services connexes[241]. Les contrats de concession emportent, il est vrai depuis 2016, obligation pour le concessionnaire de fournir à l'autorité concédante les données « collectées ou produites à l'occasion de l'exploitation du service public faisant l'objet du contrat et qui sont *indispensables* à son exécution »[242]. Au-delà de la communication des données, un autre objectif potentiel des clauses pourrait être d'assurer une certaine transparence quant au fonctionnement et aux caractéristiques des systèmes d'IA utilisés dans le cadre de l'exécution des contrats passés[243]. Le recours à l'apprentissage profond (*deep learning*) rend, certes, cette tâche particulièrement complexe pour de nombreux systèmes dont l'explicabilité n'est plus assurée. De même, l'absence de pleine communicabilité des algorithmes employés s'avère être un frein important à une parfaite transparence[244]. La proposition européenne de règlement IA prévoit néanmoins, pour les seuls systèmes d'IA à haut risque, que leur fonctionnement doit être « suffisamment transparent » pour permettre aux utilisateurs d'en interpréter les résultats et de l'utiliser de manière appropriée[245]. Leur emploi, commercial ou non, est à cette fin conditionné à la transmission d'une notice d'utilisation répertoriant des informations « concises, complètes, exactes et claires, qui soient pertinentes, accessibles et compréhensibles pour les utilisateurs »[246] (caractéristiques, capacités et limites de performance, finalité, niveau de robustesse et de cybersécurité, éléments sur les jeux de données d'entraînement, durée de vie attendue, mesures de maintenance nécessaire au bon fonctionnement du système, etc.). Comme l'a relevé le Conseil d'État, le niveau d'information exigé par la personne publique pourrait, le cas échéant, excéder les éléments prévus par la future législation européenne[247]. Il pourrait aussi être étendu aux systèmes d'IA qui présentent des risques modérés.

61 Au titre des moyens pour atteindre ces objectifs, le choix du cocontractant, en fonction de sa disposition à tenir compte ou non de ces contraintes semble évident. Lesdites contraintes pourraient notamment faire l'objet de critères pondérés déterminant l'attribution des marchés publics. Le lieu d'implantation des cocontractants et leur pleine soumission au droit de l'Union européenne s'apparentent à des garanties objectives supplémentaires d'indépendance vis-à-vis de puissances étrangères, particulièrement opportunes pour certains systèmes d'IA touchant aux intérêts fondamentaux de la nation ou à l'exécution de services publics stratégiques[248]. L'article 2 du règlement IA, qui en délimite le champ d'application, est de ce point de

vue à saluer. Il étend l'application de la future législation européenne : « (a) aux fournisseurs, établis dans l'Union *ou dans un pays tiers, qui mettent sur le marché ou mettent en service des systèmes d'IA dans l'Union* ; (b) aux utilisateurs de systèmes d'IA situés dans l'Union ; (c) aux fournisseurs et aux utilisateurs de systèmes d'IA *situés dans un pays tiers, lorsque les résultats générés par le système sont utilisés dans l'Union* »[249]. Le contrôle des usages des systèmes d'IA par la puissance publique constituerait une précaution additionnelle propice à la protection des objectifs évoqués *supra.* Dans son étude sur l'IA et l'action publique, le Conseil d'État relevait dans cette optique que « les contrats devraient définir avec précision les réutilisations autorisées des données par le prestataire, ménager à l'administration un droit de contrôle sur leur usage ou leur transfert, et garantir leur destruction à l'issue de la mission »[250].

62 Ces diverses garanties ne sauraient épuiser l'ampleur des risques inhérents à la porosité entre les secteurs public et privé qu'induit le développement de la technopolice administrative[251]. Celle-ci doit encore, plus spécifiquement, être confrontée à un impératif constitutionnel.

2/ La conception privée des systèmes d'intelligence artificielle face à l'interdiction de délégation de missions de police administrative générale

63 Dès lors que les outils de la police administrative reposent sur des systèmes d'IA, les conditions de leur conception méritent d'être consciencieusement analysées, compte tenu des implications d'une malfaçon potentielle. La vérification de la qualité des données d'apprentissage exige une vigilance particulière en raison d'un risque d'empoisonnement du jeu de données, destiné à altérer les performances ou à ouvrir des brèches de sécurité. Le simple étiquetage des données, opération répétitive régulièrement sous-traitée, peut, lui aussi, entraîner des répercussions de premier ordre sur les performances lors de la mise en œuvre du traitement reposant sur le système d'IA[252]. Les auteurs du rapport parlementaire d'information sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles relevaient pour ces raisons l'importance de développer les algorithmes de systèmes stratégiques en Europe, à partir de données traçables et hébergées sur le sol européen. Il en va de la « protection de notre autonomie technologique » autant que de « la sauvegarde des libertés publiques »[253].

64 Pour autant, l'aspect crucial de cette phase de conception ne saurait suffire à la considérer sous l'angle de la délégation de mission de police administrative. À titre de comparaison, la conception de l'armement n'emporte pas délégation des opérations extérieures militaires. La pertinence d'une appréhension de la conception privée des systèmes d'IA sous l'angle de la délégation devient pertinente lorsque la technologie mobilisée n'est pas un simple moyen d'exécution, mais implique la détermination de la cible de l'activité de police. Ainsi, un logiciel de VSA permettra de générer une alerte à destination de la police municipale, à partir d'une analyse automatisée de ce qui aura été considéré au stade de la conception comme un comportement dangereux ou une situation anormale, par le prestataire privé qui aura entraîné et développé ledit logiciel, lequel pourra de surcroît engendrer de « faux positifs » (*i.e.* alertes injustifiées). C'est parce que la phase de conception repose sur une succession de choix (*e.g.* délimitation du jeu de donnée, nettoyage des données, labellisation, modèle d'algorithme, finalité, entraînement…) qui affectent l'identification de l'objet de la

mission de police administrative qu'elle peut être pertinemment envisagée sous l'angle de la délégation[254].

65 Or, le Conseil constitutionnel a rappelé dans une décision du 20 mai 2021 qu'il résulte de l'article 12 de la Déclaration des droits de l'homme et du citoyen de 1789 (ci-après DDHC) une interdiction de déléguer des compétences de police administrative générale à des personnes privées[255]. Cinq mois plus tard, il érigeait cette interdiction en principe inhérent à l'identité constitutionnelle de la France[256] pour, en 2023, confirmer une portée limitée aux seules missions de police administrative générale « inhérentes à l'exercice de la "force publique" nécessaire à la garantie des droits », et non à toute mission de police administrative[257]. Le litige ayant donné lieu au rappel de ce principe en 2021, comme le litige ayant donné lieu en 2011 à la consécration de son rattachement à l'article 12 de la DDHC[258], procédaient précisément d'une délégation de mission de surveillance de la voie publique à des agents de sécurité privés en vue de la prévention d'actes de terrorisme. Si la délégation de cette mission est constitutionnelle lorsqu'elle est exercée sur les biens dont les agents ont la garde et à leurs abords immédiats, elle ne saurait s'étendre au-delà[259]. C'est également pour sanctionner la délégation d'une activité de surveillance privée de la voie publique que le Conseil d'État confirma l'annulation, en 1997, d'un contrat conclu entre une société de gardiennage et la commune d'Ostricourt[260].

66 L'élaboration du nouveau cadre législatif expérimental à la VSA a permis, pour la première fois en mai 2023, de confronter la conception de logiciels de traitement automatisé des images issues de la vidéoprotection ou de caméras aéroportées au principe constitutionnel d'interdiction de délégation de certaines missions de police administrative générale. Le litige portait sur la constitutionnalité de l'article 10 de la loi JOP 2024. Cette disposition autorise l'État à confier à un tiers le développement du traitement algorithmique qui a pour objet de « détecter, en temps réel, des évènements prédéterminés susceptibles de présenter ou de révéler ces risques [d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes] et de les signaler en vue de la mise en œuvre des mesures nécessaires »[261], notamment par les autorités de police administrative. Or, les débats parlementaires ont distinctement établi une intention de recourir à des prestataires privés « compte tenu de l'état du marché » et considérant qu'il « est illusoire, alors que l'usage de caméras augmentées nécessite l'établissement d'un cadre légal, de penser que l'État peut tout faire tout seul, dans un domaine où les acteurs privés ont déjà plusieurs longueurs d'avance »[262]. Les projets de recherche » Flash JO » attribués par l'Agence nationale de la recherche allaient en ce sens. Six projets de recherche ont en effet été financés à hauteur de 500 000 euros afin de développer pendant 18 mois des solutions logicielles à tester en condition réelle à partir de 2023, en particulier lors de la Coupe du monde de rugby, avant une mise en service pour les Jeux olympiques et paralympiques 2024. Les sociétés Idemia et Evitech étaient les lauréates du projet « GIRAFE », relatif à la gestion des incidents lors des rassemblements de foule. Ce projet visait à « développer des solutions algorithmiques de supervision de la foule à partir des flux vidéo couvrant tout ou partie des zones publiques »[263]. En janvier 2024, le marché mettant en œuvre la loi JOP fut finalement attribué par l'entremise d'un accord-cadre à bons de commande multi-attributaires à quatre sociétés (Wintics, Videtics, Chapsvision)[264]. Dans leur contribution extérieure soumise au Conseil constitutionnel saisi de la loi JOP 2024, plusieurs associations anticipaient avec lucidité que « ce sont bien des personnes privées qui seront, indirectement, chargées d'un grand nombre de pouvoirs de surveillance de la voie

publique et de pouvoirs de police administrative » et qui « se verront déléguer la mission de caractérisation d'évènements anormaux pouvant générer une alerte et déclencher la surveillance active d'opérateurs humains »[265]. Elles concluaient par conséquent à une violation de l'article 12 de la DDHC, moyen que le Conseil constitutionnel n'a pas jugé opportun d'aborder expressément dans sa décision du 17 mai 2023.

67 C'est donc devant le juge administratif que le raisonnement fut poussé plus avant. Le tribunal administratif de Marseille s'est en effet prononcé le 2 juin 2023 sur l'expérimentation de la VSA dans le cadre d'un recours tendant à ce qu'il soit mis fin à l'exécution d'un contrat conclu en 2018 entre la ville de Marseille et la société SNEF pour une durée de quatre ans. Le traitement de données à caractère personnel induit par ce marché répondait, selon la ville de Marseille, à un intérêt public. D'une part, la « prévention propre à sa compétence en matière de police administrative » était assurée grâce à un dispositif automatisé d'analyse en temps réel du flux vidéo et d'alerte des comportements et évènements anormaux ou suspects. D'autre part, l'« assistance à l'autorité judiciaire » était permise par une recherche automatisée d'évènements *a posteriori,* à partir des archives des images tirées de la vidéoprotection[266]. La commune se défendait par ailleurs de procéder au traitement de données biométriques et annonçait avoir entrepris la réalisation d'une analyse d'impact relative à la protection des données, certes après avoir conclu le marché, mais avant d'engager sa mise en œuvre, au stade du paramétrage et de l'adaptation du logiciel de VSA[267]. Les premiers moyens soulevés par l'association requérante, tirés de l'atteinte portée au droit au respect de la vie privée et à la violation du droit des données à caractère personnel, furent considérés comme inopérants dans le cadre du recours « *Transmanche* »[268]. En revanche, le moyen complémentaire, tiré de la délégation à une personne privée de missions de police administrative générale de surveillance de la voie publique, était opérant car susceptible de caractériser le caractère illicite du contrat.

68 En continuité des conclusions de sa rapporteure publique[269] et de l'argumentaire de la ville de Marseille, le tribunal administratif a toutefois écarté ce moyen. Pour ce faire, il s'est fondé sur quatre éléments décisifs qui balisent indirectement la portée de l'interdiction de délégation de missions de police administrative générale. Premièrement, le procédé du logiciel de traitement automatisé des images, qui se borne à une analyse des données afin de déclencher une alerte après avoir identifié des comportements ou évènements anormaux ou suspects, doit être considéré comme une simple aide à la décision des agents chargés de traiter les incidents. Deuxièmement, le visionnage des images traitées par la VSA reste contrôlé et effectué par les opérateurs du CSU. Troisièmement, le logiciel de VSA ne procède à aucune qualification juridique des faits (trouble à l'ordre public ou infraction pénale) et, dès lors, ne se substitue pas aux agents. Quatrièmement, enfin, le paramétrage des algorithmes – sans que l'on ne sache exactement quelles phases cette formule recouvre pour le tribunal administratif (sélection du jeu de données, nettoyage des données, choix du modèle d'algorithme, entraînement initial, sélection des standards de performances, entraînement continu...) – était effectué « en collaboration et pour le compte » de la commune. La requête de l'association fut donc rejetée, d'autant plus que l'expérimentation de la VSA à Marseille était désormais suspendue dans le cadre d'un moratoire[270].

69 Indépendamment de ce cas précis, les critères retenus par le tribunal administratif de Marseille pour apprécier ce qui constitue ou non une délégation illicite de missions de police administrative générale en matière de VSA interrogent. Avant même de savoir s'ils seront endossés ou non par d'autres juridictions, confirmant le cas échéant un « affaissement du principe d'indélégabilité »[271], plusieurs réserves méritent d'être formulées. Cantonner les logiciels de VSA à de simples outils d'aide à la décision peut, d'abord, être perçu sous les traits de l'euphémisme considérant l'importance du flux de données qui rend précisément obsolète tout traitement humain[272]. L'invocation d'un visionnage exclusif des images par les agents des CSU traduit, ensuite, une mécompréhension de l'outil en ce qu'elle semble écarter l'importance du traitement de l'image pour ne retenir – à tort – comme décisif que le regard humain. La CNIL relevait pourtant en 2022 que les dispositifs de VSA « offrent une puissance d'analyse de certains paramètres qu'un œil humain ne [peut] pas atteindre »[273]. Quant à l'argument tiré de l'absence de qualification juridique proposée par le logiciel de VSA, il doit être relativisé face à la massification des données rendant probable une concentration des agents sur les alertes déclenchées, assimilables dans ce contexte à un travail de préqualification. Enfin, la garantie constituée par une élaboration du « paramétrage des algorithmes » en collaboration et pour le compte de la collectivité territoriale pourrait sembler bien faible en l'absence d'une expertise interne accrue, fonction de l'engagement de spécialistes en analyse et en science des données (*data analysts, data scientists*) pour épauler leur délégué à la protection des données, entre autres.

70 Toujours est-il que le principe constitutionnel ici discuté n'apparaît pas, pour l'heure, entraver le développement de la technopolice et du recours aux prestataires privés. En parallèle, le développement des applications numériques de gestion publique invite à questionner le statut des citoyens qui entrent par ce biais en relation avec leur collectivité.

3/ L'indétermination de la collaboration entre citoyens et administration par l'entremise d'applications numériques

71 Les infrastructures évoquées *supra* peuvent laisser accroire que le citoyen se trouve réduit dans la ville dite « intelligente » à l'état de sujet passif, de surveillance ou de collecte de données. Tel n'est pas le cas. La possibilité d'une participation citoyenne ne doit pas être occultée. Celle-ci est parfois captée par la formule de « citoyen intelligent » (*smart citizen*)[274]. Parmi les initiatives qu'il convient de relever figure le développement d'applications numériques permettant une mise en relation des administrés et de l'administration, à son initiative, afin de favoriser la remontée d'informations utiles à la gestion publique. Le citoyen se mue sous cet angle en émetteur actif de données pour déclencher ou affiner l'intervention publique. Les applications successives de *tracing* dans le cade de la police sanitaire mise en œuvre pour lutter contre l'épidémie de Covid-19 en constituent une première illustration en matière de santé publique. De manière plus pérenne, d'autres outils numériques sont élaborés puis testés en vue d'une gestion et d'une surveillance courantes de l'espace public et poursuivent d'autres finalités, notamment la salubrité, la tranquillité et la sécurité publiques. Comme le relève Adèle de Mesnard, il arrive que « le maintien de l'ordre public se conjugue à l'implication des citoyens afin qu'ils participent à la collecte et à la transmission des données permettant une cartographie la plus optimale qui soit »[275]. De nouveaux enjeux émergent alors, tenant en particulier au statut

juridique de celui qui collabore au maintien de l'ordre public par l'émission d'informations.

72 L'exemple typique de ce point de vue est celui des applications municipales s'approchant du modèle « *Fix my street* », largement utilisé en Belgique et au Royaume-Uni, pour signaler en temps réel et géolocaliser une diversité d'incidents au sein de l'espace public (*e.g.* graffitis, dépôt d'encombrants, chaussée abîmée, éclairage public dysfonctionnel)[276]. La ville de Paris a décliné l'expérience avec l'application « Dans ma rue » consacrée aux signalements citoyens des « anomalies », allant du retrait ou de l'effacement des affichages illégaux à la dénonciation des incivilités (*e.g.* stationnement gênant pour obtenir l'enlèvement du véhicule). Les services municipaux sont ensuite chargés de traiter les signalements, souvent par une intervention sur place. De nombreuses communes françaises ont opté en parallèle pour la plateforme THELMA (anciennement « *Tell My City* ») qui possède des fonctionnalités similaires[277]. D'autres villes, comme Dijon et Cannes, choisissent de développer leurs propres applications, éventuellement avec la collaboration d'industriels chargés de la mise en œuvre d'un programme complet de ville intelligente[278]. En améliorant la qualité et la réactivité des services offerts aux administrés par la municipalité, il est le plus souvent question d'améliorer l'environnement urbain immédiat en garantissant l'ordre public matériel[279].

73 De manière plus audacieuse, et dans la droite ligne de son projet de « Safe city », la ville de Nice a expérimenté de janvier à mars 2018 l'application « Reporty », orientée sur une assistance de la police municipale par les citoyens, y compris eu égard à ses missions de police judiciaire[280]. Étaient cette fois visés les signalements pour « une incivilité grave ou une situation critique, dont [l'utilisateur] serait témoin ou victime », tels que des violences, vols, enlèvements, attentats, incendies et accidents[281]. Le dispositif envisagé reposait sur la transmission vidéo (images et son) de l'évènement et la géolocalisation des administrés-utilisateurs, placés directement en lien avec le CSU grâce à leurs *smartphones*[282]. En somme, par le truchement de l'application, le citoyen était appelé à s'engager et à devenir « acteur de sa propre sécurité, et donc de la sécurité collective »[283]. Un net coup d'arrêt au projet de pérennisation fut toutefois porté par la CNIL le 18 avril 2018. Par courrier, elle transmit à la ville de Nice sa prise de position jugeant *a posteriori* l'expérimentation disproportionnée et attentatoire au droit au respect de la vie privée et aux libertés publiques. Elle soulignait que « la collecte et l'enregistrement d'images et de sons par la police municipale intervenant dans l'exercice de sa mission de sauvegarde de l'ordre public » devaient nécessairement « faire l'objet d'un encadrement législatif spécifique »[284], semblablement à la vidéoprotection et aux caméras mobiles envisagées par le CSI, ce qui faisait défaut en l'espèce. Par ailleurs, le champ trop large des incidents ciblés, incluant des infractions délictuelles et criminelles graves, la collecte intrusive de données, y compris d'éventuelles conversations privées, parfois pour des comportements d'une faible gravité[285], les dommages collatéraux (*e.g.* passants filmés étrangers à la survenance de l'évènement, erreurs d'appréciation, dénonciations fondées sur des stéréotypes, règlements de comptes), ainsi que l'absence d'information individuelle des personnes filmées et les « risques particulièrement importants de surveillance incontrôlée » rendait *in fine* le dispositif inacceptable. Jean-François Carrez, rapporteur de la CNIL sur cette affaire, s'interrogeait au surplus sur la constitutionnalité du dispositif en ce qu'il procédait, certes sans dépossessions des agents municipaux, à une délégation « à des

personnes privées de fonctions régaliennes »[286]. Le principe constitutionnel qui interdit de déléguer certaines missions de police administrative inhérentes à l'exercice de la force publique permettrait de prolonger le questionnement. Malgré une demande expresse de la CNIL, aucun bilan de l'expérimentation ne fut élaboré.

74 Que l'on ne s'y trompe pas, l'autorité administrative indépendante n'a pas adopté par cet avis une position générale hostile aux applications numériques de participation citoyenne. Elle s'est d'ailleurs montrée ouverte à « la mise à disposition des administrés d'outils de signalement d'incidents aux agents » municipaux[287]. Les applications développées sur le modèle de « *Fix my street* » ne semblent d'ailleurs pas mises en cause. Dès lors, *quid* du statut des administrés dans ce cadre et des effets juridiques susceptibles de découler de ces participations ? Le Laboratoire d'innovation numérique de la CNIL opérait de manière intéressante un rapprochement entre ces signalements des *smart citizens* et les « micro-tâches » caractéristiques de ce qu'il convient désormais d'appeler le « *digital labor* »[288]. Par ces termes sont visées les contributions en apparence anodines d'utilisateurs de plateformes, de réseaux sociaux ou d'applications (*e.g.* commentaires, recherches, partages de contenu) qui, en raison de leur propension à valoriser ou à entretenir l'économie numérique, sont assimilables à un travail[289]. Sans même envisager l'activité du citoyen qui contribue à la prévention des troubles à l'ordre public matériel par un signalement sur une application publique sous l'angle de la délégation, ce parallèle établi avec le *digital labor* invite à considérer son activité sous l'angle du travail, *a minima* de la collaboration.

75 Inévitablement, une question advient : est-il pertinent d'appréhender juridiquement ces actes à travers le statut de collaborateur occasionnel ou bénévole du service public ? Cet enjeu n'a pas été tranché pour l'heure[290]. La réponse qui y sera tôt ou tard apportée est de nature à dissiper certains questionnements qui, eux, ont déjà été formulés. Ainsi, Adèle de Mesnard s'interrogeait sur la responsabilité du « signalant » : « peut-on le poursuivre si le forfait signalé est volontairement imaginaire, ou seulement mal apprécié par lui ? Si le fait dénoncé peut tomber sous le coup d'une sanction, rentre-t-on dans le cadre du délit de dénonciation calomnieuse [...] ?[291] Une telle possibilité d'action en justice ne risque-t-elle pas en retour de paralyser toute action citoyenne ? »[292]. Et, au-delà du dommage causé, l'on pourrait prolonger la réflexion : un citoyen peut-il être indemnisé par la collectivité des dommages qu'il subit (*e.g.* collision) à l'occasion de la transmission à la police municipale des informations sur un accident qui a lieu sur la voie publique par le biais d'une application afin de prévenir d'autres désordres ? Agit-il pour le compte de l'administration au-delà de ce qu'il est possible d'attendre d'un usager du service public en étant animé par un esprit de civisme ? Le statut de collaborateur occasionnel ou bénévole du service public, à admettre qu'il est applicable dans ce cas de figure[293], apporterait plusieurs éléments de réponse, tirés d'un cadre juridique solidement établi[294]. Soulignons que l'absence de réquisition ou de sollicitation de la part de l'administration n'est pas rédhibitoire à l'obtention de ce statut. Il peut, le cas échéant, découler d'une initiative spontanée sous réserve d'une participation effective et justifiée au service public. L'idéal est alors qu'il y ait acceptation de la collaboration par l'administration. À cet égard, la mise en place volontaire et consciente par la collectivité territoriale d'une application numérique dédiée aux signalements doit-elle être considérée comme une acceptation tacite, *ex ante*, des collaborations spontanées que celle-ci a vocation à canaliser ? Faute d'acceptation tacite, il convient de caractériser l'urgence et la nécessité de la collaboration[295]. Face à quels types de signalements ces critères pourraient-ils être

retenus ? S'ils semblent, de prime abord, rarement présents dans les cas débattus, Terry Olson rappelle que « l'urgente nécessité ne suppose pas qu'une personne soit effectivement aux prises avec un danger grave et immédiat ou qu'un délit vienne d'être commis ; elle peut aussi résulter de l'existence d'une situation imposant de mettre fin au danger à titre préventif »[296]. L'action d'un conseiller municipal qui entreprend de mieux fixer des buts de football mobiles installés sur la place du village, dont la stabilité est précaire et, par voie de conséquence, dangereuse, suffit par exemple à caractériser l'urgente nécessité[297]. En irait-il différemment en cas de dommages causés à l'occasion du signalement sur l'application d'un bâtiment menaçant ruine, d'un accident subi au moment de documenter l'existence d'une chaussée déformée, ou de lésions consécutives à une agression engendrée par la dénonciation d'une incivilité commise dans l'espace public ?

76 Toute assertion définitive et générale sur le statut juridique à retenir pour les *smart citizens* apparaîtrait en l'état précipitée. Seules des appréciations au cas par cas sont, en la matière, opportunes. Les interrogations ci-dessus sur les relations entre l'administration et les citoyens mettent néanmoins en lumière un enjeu de la technopolice qui pourrait alimenter le contentieux dans un avenir proche, notamment quant à la « responsabilité administrative de demain »[298]. À ce titre, lorsque sont considérés les dommages occasionnés – non par l'action des citoyens-collaborateurs mais – par le recours aux systèmes d'IA, la voie contentieuse présente moins d'incertitudes. Elle a, en effet, été récemment balisée par le Conseil d'État.

B/ Des rapports balisés en matière de responsabilité : le Conseil d'État face aux systèmes d'intelligence artificielle

77 Dans son rapport de 2022 sur l'IA et l'action publique, le Conseil d'État s'est penché de manière approfondie sur les implications potentielles, en termes de responsabilité, du recours aux systèmes d'IA (ci-après SIA) par l'administration. Pour la section du rapport et des études, l'enjeu central en la matière est de parvenir à concilier équitablement les différents intérêts en présence. Trois parties se détachent et possèdent chacune un intérêt prédominant. L'administration, utilisatrice du SIA, a besoin d'un cadre juridique clair et stable pour développer l'action publique. Le concepteur privé gagne à ce que sa responsabilité ne soit pas trop facilement engagée, ce qui serait de nature à dissuader l'innovation et sa commercialisation subséquente. L'équilibre entre ces deux impératifs ne doit pas pour autant être atteint au détriment d'une troisième partie, le requérant, qui se prétend victime du SIA ou de l'utilisation qui en aura été faite, en droit d'obtenir réparation[299]. Parvenir à cet équilibre s'avère délicat. La tâche peut imposer, au demeurant, d'affronter une difficulté tenant à l'identification du fait générateur, de laquelle dépend l'identification du responsable du dommage. Plonger dans les méandres du fonctionnement des SIA et disséquer ce que des spécialistes peinent parfois à comprendre, *a fortiori* en cas d'imbrication de systèmes alimentés de manière supervisée ou non (*i.e.* apprentissage profond) par des données intraçables, n'est, en effet, pas chose aisée[300]. Actant le fait que « "l'erreur machine" n'est, en réalité, rien d'autre qu'une erreur humaine » et qu'un cadre clair sur la mise en jeu de la responsabilité de personnes identifiées, physiques ou morales, facilite un « rapport apaisé et "normalisé" aux SIA »[301], le Conseil d'État a commencé à

tracer la voie. Celle-ci fluctue entre une responsabilité administrative nécessaire, en particulier en matière de police (1), et une responsabilité civile équitable (2).

1/ L'option nécessaire de la responsabilité administrative en matière de police

78 La responsabilité administrative a fait l'objet de longues considérations de la part du Conseil d'État dans son rapport sur l'IA. Deux principes cardinaux furent avancés à cette occasion. Le premier tient au fait que « la complexité technique des SIA ne devrait jamais constituer un obstacle à la mise en jeu de la responsabilité de l'administration, laquelle ne saurait se retrancher derrière elle pour s'en exonérer »[302]. Le second pose que « les citoyens ne devraient pas être contraints d'engager la responsabilité d'un autre acteur que l'administration utilisatrice du système et "gardienne de la chose" »[303]. Ces principes s'avèrent spécialement adaptés aux actions en responsabilité intentées dans le domaine envisagé par la présente contribution. Le juge administratif considère en ce sens que les clauses de non-responsabilité des collectivités publiques sont inopposables aux tiers qui subissent un dommage du fait de l'exercice de prérogatives de police confiées à une personne privée[304]. La solution est justifiée dès lors que l'opération matérielle reste effectuée sous le contrôle de l'administration[305]. Par conséquent, lorsque le tribunal administratif de Marseille insiste sur la collaboration maintenue de l'administration et sa supervision de l'activité du prestataire privé qui développe une solution logicielle de VSA, il ouvre inévitablement la voie à la responsabilité administrative, y compris en cas de logiciel défectueux. Certes, dans un domaine si technique, la collaboration et la supervision peuvent ne pas être effectives en raison de l'absence d'expertise de la personne publique. Mais alors, « la puissance publique est responsable de la confiance qu'elle a placée dans les personnes privées chargées de la mission »[306]. Si responsabilité civile du prestataire privé il peut y avoir, celle-ci n'intervient en somme qu'accessoirement. La mise en cause des personnes publiques est nécessaire, en premier lieu, dans le cadre de la responsabilité pour faute ou de la responsabilité sans faute.

79 Le premier régime fut anticipé par la section du rapport et des études comme le « régime principal » de mise en cause de la responsabilité administrative en cas d'action publique automatisée ou assistée par l'IA[307]. Il exige cependant la démonstration d'un manquement imputable à l'administration, d'un dommage, et d'un lien direct de causalité. Quatre manquements récurrents se dégagent à la lecture du rapport. Lorsque l'administration est sujette à une obligation de résultat, si l'action à laquelle elle est tenue n'est pas exécutée ou est mal exécutée, et qu'intervient un SIA, peu importe le rôle que celui-ci a joué et la nature de son dysfonctionnement, la faute sera caractérisée[308]. Cette hypothèse se révèle toutefois mal adaptée à l'activité de police administrative, peu sujette aux obligations de résultat[309]. La faute sera aussi caractérisée lorsque la décision à laquelle est parvenue l'administration après recours à un SIA est illégale, quelle qu'en soit la raison[310]. Si le SIA est utilisé comme outil d'aide à la décision et que l'absence de prise en compte de paramètres décisifs conduit à adopter une décision illégale, c'est à elle d'assumer la responsabilité du défaut de fiabilité[311]. Il en ira de même lorsque c'est le recours, en soi, au SIA, qui s'avère illégal. Ainsi, un traitement biométrique mis en œuvre par une collectivité territoriale, mais dépourvu de fondement juridique au regard de l'article 9 du RGPD ou de l'article 88 de la LIL, ne pourra qu'être fautif. Enfin, le Conseil d'État avançait l'hypothèse d'un non-respect d'une obligation de vigilance qui resterait à consacrer par voie prétorienne, le cas

échéant en s'inspirant du droit comparé. Une faute pourrait être constatée en l'absence de respect des « diligences qu'on peut raisonnablement attendre du responsable d'un tel système, en l'état de l'art et des connaissances scientifiques »[312] (*e.g.* principe de primauté humaine). Le régime de l'entretien d'un ouvrage public, qui impose à l'administration de démontrer qu'elle a accompli les diligences requises à la prévention d'un dommage advenu (*i.e.* ni défaut d'entretien ni vice de conception) était également invoqué en guise d'inspiration[313]. Cette configuration est alors à rapprocher de la carence fautive qui permet habituellement la sanction de l'autorité de police défaillante[314], en complément de l'illégalité fautive, que la carence soit juridique, matérielle, totale ou partielle[315].

80 En l'absence de tels manquements, mais en cas de préjudice grave et spécial, la responsabilité administrative sans faute pourrait compléter l'arsenal à disposition des victimes de l'action publique fondée sur des SIA. Tel pourrait être le cas face à une rupture d'égalité devant les charges publiques. Le Conseil d'État avançait ici une configuration particulière, celle d'un SIA qui engendrerait de graves dommages collatéraux pour une catégorie bien circonscrite de personnes de manière résiduelle[316]. La création d'un fonds d'indemnisation était dans ce cas évoquée[317]. La responsabilité de l'administration sans faute pourrait surtout être assise sur le risque inhérent au recours à ces systèmes[318], par exemple lorsque, en dépit du respect des obligations imposées aux fournisseurs du SIA à haut risque par les articles 16 à 23 du règlement IA[319], des dommages résulteraient de l'utilisation dudit système par une personne publique. Et même en cas de non-respect desdites obligations, la responsabilité sans faute de l'administration pourrait s'avérer pertinente. L'application de ce régime de responsabilité est encore soutenue par le risque récurrent qu'impliquent les opérations de police administrative ainsi que par le recours fréquent aux choses et méthodes dangereuses[320], parmi lesquelles devraient figurer certains SIA[321].

81 S'il apparaît nécessaire pour la victime que la responsabilité administrative puisse systématiquement être envisagée, la solution demeurerait pourtant déséquilibrée à défaut de mise en cause du prestataire privé fautif. La responsabilité de celui-ci devrait pouvoir être discutée dans le cadre d'une action subrogatoire ou récursoire. La résolution du Parlement européen du 20 octobre 2020 portant recommandations à la Commission sur un régime – général – de responsabilité civile pour l'intelligence artificielle accréditait cette hypothèse. Rédigée avant la proposition de règlement IA adoptée en avril 2021, elle envisageait la mise en place d'une responsabilité solidaire des « opérateurs » (*i.e.* fournisseurs et utilisateurs) doublée d'une faculté de recours des uns contre les autres[322]. Cette responsabilité solidaire était de surcroît conçue dans le cadre d'un régime de responsabilité sans faute pour les SIA à haut risque[323]. Loin d'ignorer cette prise de position, le Conseil d'État s'en saisissait en 2022 pour asseoir à son tour l'opportunité d'un régime de responsabilité sans faute, le cas échéant doublé, pour parvenir à l'équilibre ci-dessus évoqué, d'une action subrogatoire ou récursoire[324].

2/ L'option équitable de la responsabilité civile à titre accessoire

82 Concernant l'engagement de la responsabilité civile du fournisseur du SIA, elle devrait en règle générale pouvoir être retenue, selon le Conseil d'État, dans deux hypothèses spécifiques. La première tient à un défaut de conception, qui ne saurait être imputé à la seule administration utilisatrice. Cette hypothèse suppose l'identification précise du fait générateur du dommage, qu'il s'agisse d'une mauvaise qualité des données

d'entraînement, d'un étiquetage défaillant des données, d'un choix inadéquat du modèle d'algorithme ou d'un paramétrage hasardeux. Le second cas de figure, lié à la responsabilité civile, situe le dysfonctionnement en aval, au stade de la mise en œuvre du SIA lorsque l'opérateur privé en est bel et bien chargé. Le défaut de maintenance, l'absence de réapprentissage en dépit de clauses contractuelles en ce sens, la piètre qualité de celui-ci, le non-signalement d'une défaillance ou la poursuite de l'exploitation du SIA en dépit d'un constat critique devraient conduire à la mise en jeu de la responsabilité civile. L'intrusion du SIA à des fins malveillantes relèvera de l'une ou l'autre hypothèse, en fonction de ce qui l'aura causée (*e.g.* faille originelle ou défaut de sécurisation liée à une absence de maintenance ou de réapprentissage)[325].

83 Le cadre théorique ici posé par le Conseil d'État possède le mérite de la clarté et de la simplicité. Encore devra-t-il être confronté et éprouvé par les contentieux à venir. En matière de vidéosurveillance automatisée, l'absence de détection d'un évènement prédéterminé comme suspect dans le cahier des charges de la solution logicielle (*e.g.* le port d'arme par un individu) aura-t-elle pour effet d'engendrer une responsabilité du fournisseur – possiblement après indemnisation de la victime par l'administration dans le cadre de la responsabilité sans faute ? L'application du régime de responsabilité civile pour les produits défectueux pourrait renforcer la perspective d'une réponse positive et d'une action, subrogatoire ou récursoire, à l'encontre du prestataire privé. Peuvent en effet entrer en jeu les articles 1245[326] à 1245-17 du Code civil qui délimitent les contours de la responsabilité du fournisseur du SIA dans certaines configurations. Pour que l'action soit concluante, la preuve du dommage, comme celle du défaut affectant le SIA, ainsi que la démonstration d'un lien de causalité, devront toutefois être établies[327]. Étant entendu que la seule circonstance qu'un autre logiciel plus performant a été postérieurement mis en circulation ne saurait suffire pour conclure à la défectuosité du logiciel contesté[328]. Les dispositions précitées du Code civil indiquent encore que des causes exonératoires, par exemple liées à l'état des connaissances scientifiques et techniques au moment de la mise en circulation du SIA, peuvent être avancées par le producteur[329]. Ce régime de responsabilité étant désormais solidement ancré en droit français, sa déclinaison en matière de SIA était envisagée par le Conseil d'État afin de capter les deux hypothèses susmentionnées (*i.e.* défaut de conception et défaut de mise en œuvre)[330], dans le cadre d'une réflexion générale non spécifique à la police administrative. La Commission européenne a, de son côté, apporté plusieurs réserves essentielles.

84 Dans son livre blanc sur l'intelligence artificielle, la Commission a, elle aussi, pointé l'absence de régime clair de responsabilité face au risque croissant de dommage causé par le fonctionnement d'un SIA. Elle s'inquiétait particulièrement du risque d'« insécurité juridique pour les entreprises qui commercialisent leurs produits reposant sur l'IA dans l'UE », susceptible de « nuire à [leur] compétitivité »[331]. Si elle envisageait, elle aussi, la mise en œuvre de la directive sur la responsabilité du fait des produits défectueux, elle insistait à juste titre sur la lourdeur de l'exigence probatoire imposée à la victime – lorsque c'est elle qui agit directement à l'encontre du fournisseur privé, et non l'administration – eu égard à l'opacité de l'IA[332]. Comment attendre de cette victime qu'elle « [reconstitue] l'historique des décisions potentiellement problématiques résultant de l'utilisation de systèmes d'IA » pour prouver sa défectuosité[333] ? De plus, le champ d'application de la directive s'avère – selon la Commission – mal défini lorsque les innovations numériques viennent

éprouver la pertinence et les critères de la distinction entre « produits » et « services »[334]. Au bout du compte, le difficile accès aux éléments de preuve pour les victimes[335] comme l'incertitude quant au champ d'application de la législation conduisait la Commission à privilégier la perspective d'une réforme des régimes nationaux de responsabilité[336].

85 Précisément, l'articulation au niveau national d'une responsabilité administrative engagée préalablement par la victime et d'une responsabilité civile susceptible d'être mise en cause subséquemment par la puissance publique contribue à lever une partie des réserves de la Commission. Sans dissiper les incertitudes relatives au champ d'application de la directive, cette imbrication des régimes de responsabilité permet à la victime de ne pas avoir à supporter un effort probatoire démesuré. Et si cet effort est inévitablement transféré à l'administration agissant à titre subrogatoire ou récursoire, des moyens permettraient d'alléger cette tâche. Parmi eux, figure l'aménagement – voire le renversement – de la charge de la preuve. Une présomption réfragable de faute de l'« opérateur » avait déjà été envisagée par le Parlement européen pour contrer l'ineffectivité du recours de la victime[337]. Elle pourrait également être considérée pour faciliter l'action de l'administration, charge à la personne privée de démontrer qu'elle s'était conformée à son devoir de diligence.

86 En ce qui concerne l'étendue de ce devoir de diligence, un chantier d'ampleur est en cours au niveau européen dans le cadre de l'élaboration du règlement IA[338]. Les articles 16 à 28 du règlement envisagé fixent les obligations qui incombent aux fournisseurs et, plus accessoirement, aux fabricants, aux importateurs et aux distributeurs des SIA à haut risque. Parmi ces obligations figurent le respect de divers standards en matière de qualité de données et de gouvernance des données, l'enregistrement automatique des évènements liés au fonctionnement du SIA, la conformation aux exigences de transparence et de fourniture d'informations aux utilisateurs fixées par la législation, le contrôle humain, l'exactitude, la robustesse et la cybersécurité des SIA[339]. S'y ajoutent l'obligation d'établir un système de gestion des risques, une documentation technique précise, ainsi que l'obligation d'obtenir une certification avant mise sur le marché ou encore de prendre toutes les mesures correctives nécessaires en cas de dysfonctionnement constaté[340]. L'administration tenue responsable qui se retournerait contre son partenaire privé pourrait, à tout le moins, attendre de celui-ci qu'il justifie s'être conformé à ces obligations.

87 Le Conseil d'État relevait néanmoins que, « indépendamment des obligations qu'elle met à la charge des fournisseurs et des utilisateurs, et qui constitueront autant de points d'appui à des actions en responsabilité pour faute, la proposition de règlement IA de la Commission ne traite pas spécifiquement de la question de la responsabilité »[341]. Ces options juridiques et pistes de réflexion n'épuisent donc pas l'ensemble des questionnements. Inévitablement, des incertitudes demeurent et les législateurs nationaux et européen, comme les juridictions, préciseront les orientations juridiques qui apporteront des réponses définitives aux mutations technologiques engagées. Pour l'heure, le droit des produits défectueux et le droit émergeant de l'IA constituent les fondements généraux les plus nets à la mise en jeu de la responsabilité civile des opérateurs privés. Plus instable que la responsabilité administrative, elle se présente logiquement comme son accessoire. Ce partage de responsabilité pourrait encore être articulé à l'avenir avec la notion de « coresponsables » du traitement lorsque trouve à s'appliquer le droit des données à caractère personnel[342]. Au moment

de fonder l'action publique sur des SIA, l'administration est de ce fait astreinte à anticiper la portée des risques inhérents aux technologies mobilisées. Les faits dommageables susceptibles d'en résulter forment, en effet, de « nouveaux gisements de [sa] responsabilité »[343]. Et si l'enjeu de la responsabilité surgit de manière aussi centrale, c'est bien en raison des risques induits par le recours à l'IA, y compris dans le cadre de la technopolice administrative, et de ses répercussions sur les droits et libertés fondamentaux.

NOTES

1. Nous tenons à remercier Caroline Faure, Vincent Louis et Cédric Roulhac pour leurs relectures attentives, ainsi que les évaluateurs du comité de la *RevDH* pour leurs précieux commentaires. Leurs critiques et remarques ont utilement permis d'améliorer ce travail. Nous assumons l'entièreté des imperfections persistantes.

2. Un « système d'IA » est un « logiciel qui est développé au moyen d'une ou plusieurs des techniques et approches [caractéristiques de l'IA, notamment symbolique ou connexionniste] et qui peut, pour un ensemble donné d'objectifs définis par l'homme, générer des résultats tels que des contenus, des prédictions, des recommandations ou des décisions influençant les environnements avec lesquels il interagit » (art. 3, 1), de la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle, 21 avril 2021, COM(2021) 206 final). V. les annexes de la proposition pour une liste précise des techniques et approches concernées.

3. Conseil d'État, *Intelligence artificielle et action publique : construire la confiance, servir la performance,* étude à la demande du Premier ministre adoptée en Assemblée plénière le 31 mars 2022, p. 14.

4. Commission européenne, *Livre blanc. Intelligence artificielle. Une approche européenne axée sur l'excellence et la confiance,* 19 février 2020, COM (2020) 6 final, p. 2.

5. *Idem,* p. 10.

6. En ce sens, Conseil d'État, *IA et action publique, op. cit.,* p. 18.

7. *Idem,* p. 101.

8. *Idem,* p. 84.

9. *Inter alia* : M. Lanna et E. Py, *Smart City et prise de décision,* Mare & Martin, 2023, 238 p. ; J-B., Auby, « Les *Smart Cities* », *in* L. Cluzel-Métayer et *al.* (dir.), *La transformation numérique du service public : une nouvelle crise ?*, Paris, Mare & Martin, 2022, p. 111-131 ; L. Archambault et C. Rotily, « *Smart cities* : les outils d'une révolution juridique maîtrisée », *Dalloz IP/IT,* n° 6, 2021, p. 327-333.

10. En ce sens, v. X. Latour, « Sécurité intérieure : un droit "augmenté" ? », *AJDA,* 2018, p. 431 et s. : les technologies s'imposent « sous la double pression de services de police à la recherche de moyens toujours plus performants et d'industriels à la recherche de marchés rentables, indissociables d'une économie de la peur ».

11. V. déjà aux XVIe et XVIIe siècles T. More, *Utopia,* 1516, réédit. 2012, Penguin Books, 146 p. et T. Campanella, *La città del sole – Civitas solis,* 1623, réédit. 2005, Laterza, 184 p.

12. Sur ces projets, v. J-F. Soupizet, « La *smart city* : mythe et réalité », *Futuribles,* n° 434, 2020/1, p. 49-65.

13. Cour des comptes, *Les polices municipales,* rapport public thématique, 2020, p. 75.

14. *Ibidem.* V. aussi A. Korsakoff, « La data-surveillance à l'ère de la Covid-19 : un déploiement en marge du débat démocratique », *Cahiers de la recherche sur les droits fondamentaux,* n° 19, 2021, p. 55-63.

15. Le manifeste fondateur de l'initiative Technopolice est consultable en ligne [https://technopolice.fr/].

16. Sur le développement d'une stratégie associative de « demandes Cada », v. M. Labonde, L. Malhuret, B. Piédallu et A. Simon, *Internet et libertés. 15 ans de combat de la Quadrature du Net*, Vuibert, 2022, p. 161-165.

17. Le relai dans le titre de l'article et dans les développements subséquents du concept de *technopolice*, dont nous déclinons toute paternité quoique nous l'ayons affublé de l'adjectif « administrative » pour les besoins de la présente contribution, illustre cette influence centrale. Le concept est par ailleurs scientifiquement pertinent. Une alternative consisterait à évoquer une police administrative « augmentée » (en continuité de X. Latour, « Sécurité intérieure : un droit "augmenté" ? », *op. cit.*). Cette option, moins évocatrice, dissimule la prédominance d'une approche technologique de la police administrative, laquelle resurgit lorsque le ministère de l'Intérieur ambitionne plus largement de porter ses services et la sécurité intérieure « à la frontière technologique » (ministère de l'Intérieur, *Livre blanc de la sécurité intérieure,* novembre 2020, p. 201 et s.). Sur la « technologisation de la sécurité », v. aussi A. Ceyhan, « Technologie et sécurité : une gouvernance libérale dans un contexte d'incertitudes », *Cultures & Conflits,* n° 64, 2006, p. 11-32, et B. Warusfel, « Technologie et sécurité : réguler pour reprendre le contrôle », *Cahiers de la sécurité et de la justice,* n° 50, 2021, not. p. 257. Soulignons que la notion – moins que le concept – de « Technopolice » est également utilisée pour qualifier les rencontres technico-opérationnelles de la sécurité intérieure, organisées deux fois par an par le service des technologies et des systèmes d'information de la sécurité intérieure (ST(SI)²) du ministère de l'Intérieur.

18. V. principalement M. Labonde, L. Malhuret, B. Piédallu et A. Simon, *Internet et libertés*, *op. cit.*, p. 153-244 et M. Lecoquierre et F. Tréguer, « Villes sous contrôle et technologisation du maintien de l'ordre. Entretien avec Félix Tréguer », *Carnets de géographes,* n° 15, 2021. Pour une démarche évocatrice des dispositifs visés par l'association, v. J. Hourdeaux, « La Cnil saisie d'un recours collectif contre la "technopolice" », *Mediapart,* 25 septembre 2022.

19. V. sur le sujet C. Jones, R. Lanneau & Y. Maccanico, *Europe's Techno Borders,* rapport EuroMed Rights & Statewatch, juillet 2023, 43 p.

20. X. Latour, « Sécurité intérieure : un droit "augmenté" ? », *op. cit*.

21. La notion de « vidéoprotection » fut consacrée par la loi n° 2011-267 du 14 mai 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI 2). Elle permit, pour les dispositifs relatifs à la voie publique et aux lieux ouverts au public, de remplacer la notion de « vidéosurveillance » (art. 17), et de reléguer son emprise persistante aux seuls lieux non ouverts au public. La terminologie de « vidéosurveillance » s'était pourtant tôt imposée, mais présentait l'inconvénient pour les pouvoirs publics d'être moins sécurisante. En somme, il s'agissait avec la LOPPSI 2 de consacrer un « artifice, contestable, de communication » (X. Latour, « La LOPPSI, les collectivités territoriales et la lutte contre la délinquance », *AJDA,* 2011, p. 1075-1081, note 2).

22. Cour des comptes, *Les polices municipales, op. cit.,* p. 76.

23. Art. 10 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité. Sur l'historique de la vidéoprotection, v. not. X. Latour, « La LOPPSI, les collectivités territoriales et la lutte contre la délinquance », *op. cit*.

24. Ordonnance n° 2012-351 du 12 mars 2012 relative à la partie législative du CSI.

25. Ministère de l'Intérieur, circulaire du 11 février 2022 relative aux orientations budgétaires des politiques de prévention de la délinquance et de la radicalisation pour 2022, NOR : INTK2204832J.

26. Ministère de l'Intérieur, instruction du 16 février 2023 relative aux orientations des politiques soutenues par le Fonds interministériel de prévention de la délinquance pour 2023, NOR : IOMK2303419J.

27. Circulaires des 11 février 2022 et 16 février 2023, *op. cit.* Par exemple, dès 2014 : « selon les chiffres du ministère de l'Intérieur, 2 820 communes et 173 EPCI ont été accompagnés pour installer 26 614 caméras, pour un montant total de 148,52 millions d'euros de subventions » (CNIL – LINC, *Les caméras aux villages. Dynamiques de développement de la vidéosurveillance dans les petites communes françaises*, 2021, p. 7-8). Sur l'historique de ce soutien étatique, v. déjà en 2011 X. Latour, « La LOPPSI, les collectivités territoriales et la lutte contre la délinquance », *op. cit*. Plus récemment, ce soutien s'est manifesté en relation avec les signatures des contrats de sécurité intégrée instaurés en continuité de la loi du 25 mai 2021 pour une sécurité globale. V. Premier ministre, circulaire du 16 avril 2021 relative à la mise en œuvre des contrats de sécurité intégrée, n° 6258-SG. Sur la question, v. O. Renaudie et J. Martin, « Le contrat de sécurité intégrée : un symbole et des interrogations », *JCP A,* n° 46, 2020, 2999.

28. Art. L. 252-1 du CSI.

29. Art. L. 252-4 du CSI.

30. Art. L. 252-2, L. 252-3 et L. 252-5 du CSI. Sur ces questions, v. aussi décret n° 2023-1102, du 27 novembre 2023 portant application des articles L. 251-1 et suivants du Code de la sécurité intérieure et relatif à la mise en œuvre des traitements de données à caractère personnel provenant de systèmes de vidéoprotection et des caméras installées sur des aéronefs.

31. Cour des comptes, *Les polices municipales, op. cit.,* p. 77. Dans le même sens, plus récemment, v. 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, p. 114 (recommandation n° 34).

32. Accessible en ligne [https://sunders.uber.space/?lat=43.2961743&lon=5.3699525&zoom=14].

33. CNIL – LINC, *Les caméras aux villages, op. cit.,* p. 9.

34. Accessible en ligne [https://technopolice.fr/villes/]

35. Cour des comptes, communiqué du 10 février 2022 accompagnant le référé du 2 décembre 2021 relatif au plan de vidéoprotection de la préfecture de police de Paris, S2021-2194.

36. Cour des comptes, référé du 2 décembre 2021 relatif au plan de vidéoprotection de la préfecture de police de Paris, S2021-2194. Ces chiffres sont confortés par l'étude d'impact du projet de loi JOP 2024 qui relaie les informations fournies en 2020 par la préfecture de police de Paris. Premier ministre, *Étude d'impact. Projet de loi relatif aux Jeux olympiques et paralympiques 2024,* NOR : SPOX2233026L/Bleue-1, 20 décembre 2022, p. 76.

37. « JO 2024 : Darmanin demande de préparer des plans "zéro délinquance" aux préfets », *Le Figaro & AFP* 25 octobre 2022.

38. Instruction du 16 février 2023, *op. cit*.

39. H. Jouanneau, « Vidéoprotection : le gouvernement débloque 20 millions d'euros pour la réparation des caméras », *La Gazette des communes*, 3 juillet 2023.

40. « Plus de caméras dans les gares d'Île-de-France ! », *PSM. Protection sécurité magazine,* n° 280, nov./déc. 2023, p. 16-17 ; L. Da Veiga, « Paris 2024 : la vidéoprotection renforcée dans 21 gares d'Île-de-France », *Les Échos,* 25 octobre 2023.

41. Contre 225 millions initialement prévus dans le cadre du contrat de partenariat conclu avec la société IRIS PVPP. Cour des comptes, communiqué du 10 février 2022, *op. cit.* Semblablement, sur le cas de Marseille, v. J-M. Manach, « Vidéo-protection : les 500 nouvelles caméras coûteront trois fois plus cher que prévu », *Marsactu,* 11 avril 2018. Étant entendu qu'au coût unitaire, qui oscille de 25 000 à 40 000 euros en moyenne selon le type de caméra, s'ajoute les coûts de raccordement ou d'abonnement 4G/5G et les coûts d'entretien. Sur cette question, v. La Quadrature du Net,

Projet de loi relatif aux Jeux olympiques et paralympiques de 2024 : dossier d'analyse de la vidéosurveillance automatisée, 17 février 2023, p. 24, y compris notes 33 et 34 relatives à la ville de Toulouse.

42. 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. 40.

43. V. la modification de l'art. L. 132-14 du CSI et la création de l'art. L. 132-14-1 du même code. Plus généralement, sur cette dynamique de mutualisation des moyens au soutien du développement de politiques locales de sécurité, v. X. Latour, « La sécurité intérieure, entre échelon national et échelon local », *AJDA,* 2022, p. 614-620.

44. CNIL – LINC, *Les caméras aux villages, op. cit.*, p. 26. Les chiffres sont néanmoins débattus et les sources divergent.

45. Cour des comptes, *Les polices municipales, op. cit.,* p 64.

46. Sur l'articulation des politiques locales et nationales de sécurité, v. CREOGN, « Les polices municipales : partenaire indispensable des forces publiques nationales ? », note n° 7, novembre 2014 et X. Latour, « La sécurité intérieure, entre échelon national et échelon local », *op. cit.*

47. Cour des comptes, *Les polices municipales, op. cit.,* p 68.

48. *Idem,* p. 63. Sur la montée en puissance des polices municipales, v. X. Latour, « Les polices municipales et la coproduction de sécurité », *in Annuaire du droit de la sécurité et de la défense,* Paris, Mare & Martin, 2019, p. 111-121.

49. Pour une approche complète du cadre juridique, v. ministère de l'Intérieur et ministère de la Cohésion des territoires et des Relations avec les collectivités territoriales, Instruction du 4 mars 2022 relative à l'acquisition, l'installation et l'entretien de dispositifs de vidéoprotection par les collectivités territoriales et leurs groupements, ainsi que sur l'habilitation du personnel territorial procédant au visionnage, NOR : TERB2205640J.

50. Art. L. 2212-2 du CGCT. À noter, en complément, que « le maire est tenu de signaler sans délai au procureur de la République les crimes ou les délits dont il acquiert la connaissance dans l'exercice de ses fonctions » (art. L. 132-2 du CSI).

51. V. la présentation du CSU sur le site internet de la ville [https://www.nice.fr/fr/securite/le-centre-de-supervision-urbain].

52. V. la présentation du CSU sur le site internet de la ville [https://www.cannes.com/fr/cadre-de-vie/prevention-des-risques-majeurs-securite/securite/police-municipale.html]. V. aussi L. Hélin, « À Cannes, de nouvelles caméras de vidéoprotection "camouflées" dans le mobilier urbain », *Le Figaro,* 8 février 2023.

53. Pour Marseille, les chiffres sont tirés des conclusions de Madame Célie Simeray, rapporteure publique sur TA Marseille, 2 juin 2023, *LQDN c. ville de Marseille,* n° 2009485.

54. V. la présentation du CSU sur le site internet de la ville [https://www.bobigny.fr/la-tranquillite-publique/la-videoprotection/le-centre-de-supervision-urbain-1211.html].

55. Art. L. 1311-15 du CGCT.

56. Art. L. 512-1 à L. 512-3 du CSI.

57. Pour une mise en contexte au regard de la montée en puissance de l'intercommunalité en matière de police administrative, v. O. Renaudie, « Intercommunalité et police administrative », *in Annuaire du droit de la sécurité et de la défense,* Paris, Mare & Martin, 2018, p. 295-308 et, spéc. sur la mise en commune des policiers municipaux p. 304-306.

58. Art. 1 de la loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance. Aujourd'hui, v. art. L. 132-14 du CSI.

59. Respectivement art. L. 5216-5, I, 4°, L. 5215-20, I, 4° et L. 5217-2, I, 4°, b) du CGCT.

60. Art. L. 5214-16 du CGCT, II, 2° bis.

61. V. la présentation du CSU sur le site internet de la métropole [https://metropole.nantes.fr/actualites/2021/securite-tranquillite-publique/decouverte-centre-supervision].

62. Nancy métropole dispose d'un CSU doté de sept opérateurs sous la direction d'un policier municipal. Le coût de création est estimé à 750 000 euros. V. CNIL – LINC, *Les caméras aux villages, op. cit.*, p. 26.

63. V. la présentation du CSU sur le site internet de la métropole [https://metropole.toulouse.fr/mon-environnement/prevention-et-securite/police-municipale].

64. V. la présentation du CSU sur le site internet de la communauté de communes [https://cc-miribel.fr/services/prevention-et-securite/le-centre-de-supervision-urbaine-intercommunale-csui/].

65. Circulaire du 11 février 2022, *op. cit*.

66. Type de syndicat défini à l'article L. 5721-8 du CGCT. Il est également possible, en vertu de l'art. L. 132-14, II, du CSI, qu'un CSU soit instauré et géré dans le cadre d'un syndicat mixte fermé (défini à l'art. L. 5711-1 du CGCT), composé exclusivement de communes et d'EPCI exerçant la compétence relative aux dispositifs locaux de prévention de la délinquance.

67. Art. L. 132-14, III, du CSI. La disposition précise que la présidence du syndicat mixte ouvert ne peut alors être assurée que par un maire ou un président d'EPCI, à l'exclusion du président du conseil départemental, afin de « de réserver la présidence de ce syndicat [...] à une autorité dont le rôle en matière de prévention de la délinquance est déjà consacré par le CSI » (Instruction du 4 mars 2022, *op. cit.*).

68. En application de l'art. L. 511-1 du CSI.

69. Cour des comptes, *Les polices municipales, op. cit.,* p 29.

70. Art. L. 132-14-1 du CSI.

71. *Idem*.

72. Art. L. 3221-4 du CGCT.

73. Art. 16 du CPP.

74. De manière plus récente, soulignons encore l'inauguration en juillet 2022 d'un centre de supervision spécifique, en l'occurrence le CCOS (Centre de coordination opérationnelle de sûreté) qui vise à sécuriser les transports du Grand Paris en coordonnant différents acteurs : préfecture de police, RATP et SNCF. Au niveau national, la SNCF dispose, elle, de son Poste de commandement national sûreté (PCNS).

75. Association nationale de la vidéoprotection, *PIXEL 2024*, p. 206.

76. La vision par ordinateur est une technologie de l'IA qui repose sur l'analyse d'images numériques dans le but d'en extraire des informations, qu'il s'agisse de détecter des formes, des silhouettes, des mouvements, des objets ou des attributs de ceux-ci.

77. Sur ces exemples, v. Observations du Gouvernement sur la loi JOP 2024, transmises au greffe du Conseil constitutionnel le 10 mai 2023, en amont de la décision 2023-850 DC, p. 13. V. ensuite l'art. 3 du 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, pris en application de l'article 10 de la loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions.

78. Sur le contentieux « Briefcam », v. récemment TA Caen, ord., 22 novembre 2023, *Ligue des droits de l'homme et autres,* n° 2303004, TA Nice, ord., 23 novembre 2023, *Ligue des droits de l'homme et autre,* n^{os} 2305692, 2306593, 2305712, TA Lille, 29 novembre 2023, *Ligue des droits de l'homme et autres,* n^{os} 231013 et 2310163, CE, ord., 21 décembre 2023, *Communauté de communes Cœur Côte Fleurie,* n° 489990 et CE, 20 décembre 2023, *La Quadrature du net,* n° 463151.

79. À l'instar d'Aix-les-Bains, Aulnay-sous-Bois, Cannet, Caudry, Comines, Deauville, Denain, Gex, Lambersart, Moirans, Nancy, Nice, Nîmes, Perpignan, Quimper, Rennes, Roanne, Roubaix, Saint-Marcel-lès-Valence, Saint-Tropez, Vannes, Vaulx-en-Velin, Versailles, Vienne ou encore Vitrolles. V. Association nationale de la vidéoprotection, *PIXEL. Le guide de la vidéoprotection 2020,*

p. 326, *PIXEL. Le guide des technologies de sûreté 2022,* p. 246, 313, 322, *PIXEL. Le guide des technologies de sûreté 2023,* p. 239, *PIXEL 2024,* p. 172.

80. Association nationale de la vidéoprotection, *PIXEL. Le guide des technologies de sûreté 2023, op. cit.,* p. 239.

81. *Inter alia* : La Madeleine, Mouvaux, Saint-André-lez-Lille ou Villeneuve-d'Ascq. *Idem,* p. 309. Pour une liste plus fournie des collectivités clientes, v. le site de cette société [http://lumatech.fr/].

82. V. Association nationale de la vidéoprotection, *PIXEL 2024,* p. 303 et 305.

83. Huawei, « Valenciennes inaugure un nouveau système de vidéo-protection et s'inscrit dans une démarche de "ville intelligente" avec Huawei », communiqué du 13 février 2017. V. aussi C. Pourré, « JO de Paris 2024 : pourquoi la vidéosurveillance automatisée fait débat », *Le Monde,* 20 mars 2023.

84. Métropole Rouen Normandie, « Agir sans attendre pour la social-écologie, le soutien aux entreprises, la lutte contre les violences faites aux femmes », communiqué de presse, 22 juillet 2020.

85. 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, op. cit.*, p. 67-70.

86. Circulaire du 11 février 2022, *op. cit.*, p. 8. La circulaire du 16 février 2023 évoque la nécessité de « tenir compte des évolutions technologiques susceptibles d'être autorisées par le projet de loi relatif aux JOP 2024 » (p. 11), soit la VSA, précisément. Les deux circulaires appliquent en ce sens la mesure 26 de la Stratégie nationale de prévention de la délinquance 2020-2024.

87. V. CNIL, « Caméras dites 'intelligentes' ou 'augmentées' dans les espaces publics », 2022, p. 11. Cette position fut réaffirmée par les services de la CNIL par la voix de M. Dutheillet de Lamothe lors d'une audience devant le juge des référés du Conseil d'État le 15 décembre 2023, ayant débouché sur CE, ord., 21 décembre 2023, *op. cit.*

88. Sur cette expérimentation, v. : AlgorithmWatch, *Automated Decision-Making Systems on the Covid-19 Pandemic: A European Perspective,* report, special issue, 2020, p. 22 ; D. Leloup, « La RATP va tester des caméras "intelligentes" pour mesurer le taux de port du masque dans la station Châtelet », *Le Monde,* 7 mai 2020 ; M. Labonde, L. Malhuret, B. Piédallu et A. Simon, *Internet et libertés*, *op. cit.*, p. 215-216. V. aussi à Cannes, M. Szadkowski, « À Cannes, des tests pour détecter automatiquement par caméras le port du masque », *Le Monde,* 28 avril 2020.

89. Courrier du directeur de la conformité de la CNIL, émis le 11 juin 2020 [https://data.technopolice.fr/fr/entity/rgp85zlnz8e].

90. 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. V. art. 1, y compris sur la limitation du droit d'opposition en application de l'art. 23 du RGPD.

91. *Idem*.

92. En ce sens, v. TA Caen, ord., 22 novembre 2023, *Ligue des droits de l'homme et autres,* n° 2303004, § 8, et TA Nice, ord., 23 novembre 2023, *Ligue des droits de l'homme et autre,* n^{os} 2305692, 2306593, 2305712, § 8.

93. Art. 21 du RGPD.

94. Décret n° 2023-1102 du 27 novembre 2023, précité, dont l'art. 3 introduit au sein du CSI un art. R. 253-6, V, ainsi libellé : « 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 ».

95. Sous les réserves additionnelles mentionnées à l'art. 23 du RGPD.

96. Art. 110, al. 2, de la LIL : « Les dispositions du premier alinéa ne s'appliquent pas lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte instaurant le traitement ».

97. CNIL, « Caméras dites 'intelligentes' ou 'augmentées' dans les espaces publics », *op. cit.,* p. 15

98. *Idem,* p. 16.

99. Fondement légal précisé par le décret n° 2023-828 du 28 août 2023, précité. Pour des commentaires doctrinaux de ce fondement légal spécifique et expérimental, v. not. : A. Guillard et V. Louis, « La loi "jeux olympiques" : l'arbre de l'expérimentation algorithmique cache la forêt de l'extension sécuritaire », *RevDH – Lettres ADL,* 18 septembre 2023 ; M. Bartolucci, « L'expérimentation de la vidéosurveillance algorithmique », *Droit administratif,* étude 7, novembre 2023 ; M-A. Granger, « Les pouvoirs de police administrative de la loi relative aux Jeux olympiques et paralympiques », *AJDA,* n° 41, 2023, p. 2222-2228.

100. Sur les possibles usages de la biométrie vocale et de l'odorologie, v. ministère de l'Intérieur, *Livre blanc de la sécurité intérieure, op. cit.*, p. 260-263. Sur la reconnaissance faciale et son expérimentation, v. p. 263-265. Plus généralement, sur la reconnaissance faciale et la physiognomonie, v. les excellents travaux de Caroline Lequesne-Roth, not. : 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, 96 p. ; C. Lequesne-Roth & J. Keller, *Surveiller les foules. Pour un encadrement des IA "physiognomoniques"*, livre blanc pour l'Observatoire de l'éthique publique, 2023, 90 p.

101. Sénat, texte n° 128, adopté le 12 juin 2023.

102. Art. R. 40-26 du Code de procédure pénale : « Peuvent être enregistrées dans le présent traitement les catégories de données à caractère personnel et informations suivantes : 1° Concernant les personnes mises en cause : [...] photographie comportant des caractéristiques techniques permettant de recourir à un dispositif de reconnaissance faciale (photographie du visage de face) ». 615 871 utilisations étaient dénombrées pour l'année 2021 par un rapport d'information du Sénat (Sénat (M-P. Daubresse, A. Belenet et J. Durain), *Rapport d'information fait au nom de la Commission des lois sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles,* n° 627, 10 mai 2022, p. 38), contre 375 000 en 2019 (M. Labonde, L. Malhuret, B. Piédallu et A. Simon, *Internet et libertés*, *op. cit.*, p. 190-191). Ce dispositif, qui peut avancer jusqu'à 200 réponses avec un taux minimal de correspondance de 40 %, fut validé par le Conseil d'État : CE, 26 avril 2022, *LQDN c. Premier ministre,* n° 442364. Pour un état des lieux détaillé sur ce sujet, v. 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, op. cit.*, p. 83-89. Pour une approche comparée de pratiques similaires, v. CREOGN, « Numérisation du visage : opportunités et limites de la reconnaissance faciale », note n° 18, avril 2016, p. 2-3.

103. Art. 44 de la LIL et art. 9 du RGPD.

104. Art. R. 232-6 à R. 232-11-2 du CSI. V. sur le sujet : Sénat (Sénat (M-P. Daubresse, A. Belenet et J. Durain), *Rapport d'information sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles*, *op. cit.*, p. 38-40 ; C. Lequesne-Roth, *New Surveillance Technologies in Public Spaces, op. cit.*, p. 32-33 ; 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, op. cit.*, p. 89-90.

105. Sur deux projets du secrétariat général de la Défense et de la Sécurité nationale visant à expérimenter des dispositifs de contrôle d'accès pour les arbitres à Roland-Garros et au stade Vélodrome, v. *idem,* p. 43. Sur une autre expérimentation de la société Aéroport de Paris permettant un embarquement autonome, v. p. 43-44.

106. Sur cette expérimentation, v. *idem,* p. 44-47 et M. Labonde, L. Malhuret, B. Piédallu et A. Simon, *Internet et libertés*, *op. cit.*, p. 178-179. V. aussi ville de Nice, *Rapport – expérimentation reconnaissance faciale,* 2019, 37 p., accessible en ligne [https://data.technopolice.fr/fr/entity/2xggtjtwovm?page=1].

107. CNIL, « Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position », communiqué du 29 octobre 2019. Le dispositif fut considéré disproportionné et contraire au principe de minimisation des données.

108. TA Marseille, 27 février 2020, *LQDN et autres,* n° 1901249. Sur l'expérimentation, v. aussi M. Labonde, L. Malhuret, B. Piédallu et A. Simon, *Internet et libertés*, *op. cit.*, p. 179-180.

109. En ce sens, v. CREOGN, « Reconnaissance faciale et contrôles préventifs sur la voie publique, l'enjeu de l'acceptabilité », note n° 43, septembre 2019, p. 4.

110. Ministère de l'Intérieur, *Livre blanc de la sécurité intérieure, op. cit.,* p. 263.

111. Sénat (M-P. Daubresse, A. Belenet et J. Durain), *Rapport d'information sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles*, *op. cit.*, p. 53.

112. 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, op. cit.*, not. p. 103-105.

113. European Parliament, « Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI », press release, 9 décembre 2023 [https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai].

114. 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. La CNIL soulignait également en 2022 que les augmentations évoquées « modifient la nature des dispositifs de vidéoprotection » et que « la perspective d'une surveillance et d'une analyse algorithmique permanentes d'espaces publics peut générer ainsi de fortes inquiétudes » (CNIL, « Caméras dites 'intelligentes' ou 'augmentées' dans les espaces publics », *op. cit.,* p. 3).

115. Sur le possible recours expérimental à la reconnaissance faciale, v. aussi 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.

116. Sénat, *Covid-19 : deuxième rapport d'étape sur la mise en œuvre de l'état d'urgence sanitaire,* rapport de la Commission des lois, 29 avril 2020, p. 35 : « Selon les données communiquées à la commission, entre le 24 mars et le 24 avril, il a été recouru à des drones dans le cadre de 535 missions réalisées par la police nationale, dont 251 missions de surveillance et 284 missions d'information de la population ».

117. Cour des comptes, *Les polices municipales, op. cit.,* p. 72.

118. Not. Ajaccio, Amiens, Cannes, Cergy-Pontoise, Granville, Lille, Limoges, Metz, Montpellier, Nantes, Nice, Paris, Rennes ou Saint-Malo. V. not. la Quadrature du Net, « Covid-19 : l'attaque des drones », 1er avril 2020 [https://www.laquadrature.net/2020/04/01/covid-19-lattaque-des-drones/].

119. A. Carini, « Cannes expérimente un drone pour désinfecter le marché de la Bocca », *Nice Matin,* 10 avril 2020.

120. CE, avis, 20 septembre 2020, n° 401214, cons. 1.

121. Pour des usages au soutien de missions de police judiciaire, v. CNIL, Délibération SAN 2021-003 du 12 janvier 2021, § 10-11.

122. Ministère de l'Intérieur, *Livre blanc de la sécurité intérieure, op. cit.,* p. 231.

123. V. TA Paris, ord. 5 mai 2020, *LQDN et LDH c. préfet de police de Paris,* n° 2006861, not. cons. 4, 8, et 10 à 12.

124. *Ibidem.*

125. CE, ord. 18 mai 2020, *LQDN et LDH c. préfet de police de Paris*, n° 440442, cons. 15. Pour un commentaire de cette ordonnance, v. not. : B. Le Querrec, « Le Conseil d'État ouvre l'espace aux drones », *RDLF,* n° 81, 2020 ; P-E. Audit, « Le Conseil d'État et la légalité de l'utilisation des drones : quelle place pour la vie privée ? », *Recueil Dalloz*, 2020, p. 1336 et s.

126. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
127. CE, ord. 18 mai 2020, *op. cit.*, cons. 16.
128. *Idem,* cons. 17.
129. *Idem,* cons. 13 et 14.
130. Art. 31 de la LIL.
131. CE, ord. 18 mai 2020, *op. cit.*, cons. 18.
132. *Idem,* cons. 19. Pour une analyse critique, v. B. Le Querrec, « Le Conseil d'État ouvre l'espace aux drones », *op. cit.*
133. CE, ord. 22 décembre 2020, *LQDN c. préfet de police de Paris*, n° 446155, cons. 7 et 12.
134. *Idem,* cons. 13. Une position semblable fut retenue par la CNIL dans sa délibération SAN-2021-003 du 12 janvier 2021.
135. CE, avis, 20 septembre 2020, *op. cit.*
136. *Idem,* cons. 3, et art. 31, II., de la LIL.
137. *Idem,* cons. 4.
138. *Idem,* cons. 5.
139. CC, Décision n° 2021-817 DC, 20 mai 2021, *Loi pour une sécurité globale préservant les libertés,* § 129 à 141 censurant le premier dispositif législatif envisagé pour défaut de garanties suffisantes. Sur cette question, v. X. Latour, « Les technologies et la loi relative à la sécurité globale : un flop ? », *AJDA,* 2021, p. 1502-1507.
140. En matière de police judiciaire, v. art. 230-47 à 230-53 du CPP.
141. Lorsque la finalité poursuivie est la sécurité des rassemblements de personnes sur la voie publique ou dans des lieux ouverts au public, la durée de l'autorisation ne peut excéder la durée du rassemblement.
142. Art. L. 242-4 du CSI.
143. CC, Décision n° 2021-834 DC, 20 janvier 2022, *Loi relative à la responsabilité pénale et à la sécurité intérieure,* § 27.
144. *Idem,* § 30 : les dispositions en cause « ne sauraient, sans méconnaître le droit au respect de la vie privée, être interprétées comme autorisant les services compétents à procéder à l'analyse des images au moyen d'autres systèmes automatisés de reconnaissance faciale qui ne seraient pas placés sur ces dispositifs aéroportés ».
145. *Idem,* § 31.
146. *Idem,* § 35-38.
147. Décret n° 2023-283 du 19 avril 2023.
148. La Ligue des droits de l'homme, la Quadrature du Net, le Syndicat de la magistrature, le Syndicat des avocats de France et l'Union syndicale Solidaires.
149. CE, ord., 24 mai 2023, *ADELICO et autres,* n° 473547, cons. 5.
150. *Idem,* cons. 8.
151. TA Pau, ord., 13 juillet 2023, *Avocats pour la défense des étrangers (ADDE) et autres c. préfet des Pyrénées-Atlantiques,* n° 2301796, not. cons. 12.
152. CE, ord., 25 juillet 2023, *ADDE et autres c. préfet des Pyrénées-Atlantiques*, n° 476151.
153. Dernièrement, v. CE, ord., *Mme Hentz et autres,* 12 décembre 2023, n° 489923.
154. TA Paris, ord., 13 juillet 2020, *Association de défense des libertés fondamentales et autres c. préfet de police de Paris,* n° 2316306/9.
155. TA Grenoble, ord., 8 juillet 2023, *M. Slama c. préfet de l'Isère,* n° 2304323.
156. TA Rouen, ord., 5 mai 2023, *ADELICO et autres c. préfet de l'Eure,* n° 2301786. Sur un rassemblement écologiste organisé en opposition à un projet ferroviaire (Tunnel Euralpin Lyon Turin), lui aussi vidéosurveillé par drones, v. Préfecture de la Savoie, arrêté n° 73-202306-15-00003 du 15 juin 2023. Sur la protection par caméras aéroportées du site de la société Arkema en banlieue de Grenoble contre une action de militants écologistes d'Extinction Rebellion, v. Préfecture de l'Isère, arrêté n° 38-2023-05-02-00006 du 2 mai 2023.

157. Préfecture du Vaucluse, arrêté n° 2023/07-03/1 du 4 juillet 2023.

158. Préfecture de police de Paris, arrêtés n° 2023-00622 du 2 juin 2023 et n° 2023-00871 du 20 juillet 2023.

159. Préfecture de police de la Manche, arrêté du 5 mai 2023, rec. des actes administratifs de la Manche, mai 2023, n° 36, p. 3.

160. Préfecture de la Nièvre, arrêté n° 2023-0531-000002 du 31 mai 2023.

161. Préfecture de Loire-Atlantique, arrêtés n° CAB/SPAS/2023/426 et CAB/SPAS/2023/427 du 28 avril 2023.

162. Préfecture de Loire-Atlantique, arrêté n° CAB/SPAS/2023-604 du 20 juin 2023.

163. Respectivement : Préfecture de police de Paris, arrêtés n° 2023-00547 du 25 mai 2023, n° 2023-00738 du 28 juin 2023, n° 2023-00790 du 5 juillet 2023, n° 2023-00843 du 12 juillet 2023, n° 2023-00863 du 18 juillet 2023 et n° 2023-00885 du 26 juillet 2023.

164. Préfecture du Loir-et-Cher, arrêté n° 41-2023-06-2023-00001 du 23 juin 2023.

165. Préfecture de la Réunion, arrêté n° 2023-951/CAB/BPA du 10 mai 2023. Au titre des motifs, était invoquée la possible dissimulation de manifestants dans la végétation avoisinante, la visite ayant lieu sur le site du Maïdo.

166. Préfecture de Loire-Atlantique, arrêté n° CAB/SPAS/2023-410 du 28 avril 2023.

167. Préfecture de l'Ain, arrêté n° 01-2023-07-17-00001 du 17 juillet 2023.

168. Respectivement : Préfecture de police de Paris, arrêtés n° 2023-00561 du 26 mai 2023, n° 2023-00455 du 27 avril 2023, n° 2023-00665 du 15 juin 2023, n° 2023-00666 du 15 juin 2023 et n° 2023-00849 du 13 juillet 2023.

169. Préfecture de l'Eure-et-Loir, arrêté n° PREF-CABINET-SDS-SIDPC 23-04/20 du 29 avril 2023 ; TA Toulouse, ord., 24 mai 2023, *ADELICO et autres c. préfet de la Haute-Garonne,* n° 2302868 ; préfecture du Cher, arrêté n° 2023-0648 du 5 mai 2023 ; préfecture de l'Hérault, arrêté n° 2023.05.DS.0208 du 4 mai 2023. Pour une suspension en référé, v. TA Nantes, 2 août 2023, *M. A. B. et autres c. préfet de Loire-Atlantique,* n° 2310969.

170. Préfecture de police des Bouches-du-Rhône, arrêtés autorisant la captation l'enregistrement et la transmission d'images au moyen de caméras installées sur les aéronefs, rec. des actes administratifs spécial, n° 13-2023-135 bis, 14 juin 2023, puis rec. des actes administratifs spécial, n° 13-2023-155 bis, 10 juillet 2023.

171. V. la description du projet obtenu par la Quadrature du Net auprès de la commune de Saint-Étienne [https://www.laquadrature.net/wp-content/uploads/technopolice/Saint-Etienne/09_Description%20du%20projet.pdf]. V. aussi M. Labonde, L. Malhuret, B. Piédallu et A. Simon, *Internet et libertés*, *op. cit.*, p. 181-183.

172. *Ibidem.*

173. CNIL, courrier du 25 octobre 2019, obtenu par la Quadrature du Net [https://data.technopolice.fr/fr/entity/8cg0lsgcbkr].

174. *Ibidem.*

175. Constitution du 4 octobre 1958, art. 34.

176. Aux fins de verbalisation, v. « Paris expérimente ses premiers radars sonores », 27 avril 2022 [https://www.paris.fr/pages/paris-experimente-ses-premiers-radars-sonores-20411].

177. R. Marhic, « Paris installe plus de capteurs anti-nuisance pour repérer les sources de bruit dans les quartiers festifs », *TraxMag,* 9 mars 2018. Les niveaux mesurés en temps réel par une soixantaine de capteurs sont accessibles en ligne [https://monquartier.bruitparif.fr/].

178. Accessible en ligne [https://carto.bruitparif.fr/]. V. plus accessoirement : https://rumeur.bruitparif.fr/.

179. Art. 7 du Règlement public d'exploitation de la Régie des transports de Marseille du 15 novembre 2018.

180. Les données sont conservées entre trois et quatre jours. V. L. Fernandez, « Vidéoprotection : à Marseille, la régie des transports métropolitains va plus loin que l'image », *La Gazette des communes*, 10 juillet 2020.

181. Convention visant à l'expérimentation des dispositifs Sensivic sur le territoire de la ville d'Orléans, 12 octobre 2021, accessible en ligne [https://www.laquadrature.net/wp-content/uploads/sites/8/2021/12/05-convention_attaquee.pdf].

182. *Ibidem.* La convention passée précise explicitement que les dispositifs de l'entreprise « demandent à être couplés à un système de sécurité et plus particulièrement ceux s'appuyant sur un système de vidéo-protection pour garantir une surveillance optimale ». V. aussi la Quadrature du Net, « Surveillance sonore : LQDN attaque l'expérimentation d'Orléans », 14 décembre 2021. L'entreprise indique par ailleurs posséder plusieurs collectivités locales ainsi que le département des Yvelines comme clients *in* Association nationale de la vidéoprotection, *PIXEL. Le guide des technologies de sûreté 2023, op. cit.*, p. 337.

183. *Ibidem.* V. aussi F. Guéroult, « Sécurité : la ville d'Orléans va tester des détecteurs de sons anormaux », *France Bleu Orléans,* 2 octobre 2021.

184. La Quadrature du Net, « Surveillance sonore : Orléans baratine la justice », 12 janvier 2023.

185. CNIL, courrier du 25 septembre 2023, adressé par la présidente de la CNIL au maire d'Orléans, obtenu par nos soins sur demande CADA.

186. « Les caméras de vidéosurveillance dotées de capteurs de son jugées illégales par la CNIL », *Ouest France,* 4 octobre 2023.

187. V. la présentation du CSU sur le site internet de la ville [https://www.nice.fr/fr/securite/le-centre-de-supervision-urbain].

188. Déjà, sur l'utilisation de caméras thermiques dans le cadre de l'épidémie de Covid-19 afin de contrôler la température corporelle des personnes à Lisses, v. TA Versailles, ord., 22 mai 2020, *Ligue des droits de l'homme,* n° 2002891, puis CE, ord., 26 juin 2020, *Ligue des droits de l'homme,* n° 441065. Un premier dispositif reposait sur le déploiement d'une caméra thermique à l'entrée du pôle administratif communal. Dépourvu de capacité de stockage et ne procédant à aucun enregistrement, le dispositif indiquait aux personnes se plaçant volontairement dans un espace déterminé si leur température était inférieure ou supérieure à la normale. Chaque agent ou usager public avait la possibilité d'entrer dans le bâtiment public en contournant ce système de contrôle automatisé. Le TA de Versailles considéra que l'installation était consécutive à une décision du maire au titre de son pouvoir général d'organisation de ses services, et non de son pouvoir de police administrative générale. Le Conseil d'État estima, lui, qu'il ne s'agissait pas d'un traitement de données à caractère personnel au sens du RGPD. Un second dispositif reposait sur l'utilisation de caméras thermiques portatives à l'entrée des établissements scolaires et périscolaires afin de vérifier la température des enfants accueillis et des personnels encadrants. En cas de détection d'une température corporelle excessive, agents comme élèves étaient invités à quitter l'établissement. La subordination des élèves au directeur de l'établissement neutralisant toute possibilité de fonder la licéité du traitement sur le consentement libre et éclairé au sens de l'art. 9 du RGPD, le Conseil d'État considéra cette fois que le traitement de données sensibles ne pouvait être licite, à la fois « faute de texte régissant l'emploi des caméras thermiques déployées par la commune » et à défaut d'analyse d'impact réalisée en amont, conformément à l'art. 35 du RGPD. V. X. Bioy, « Caméras thermiques et surveillance sanitaire, quel régime ? », *AJDA,* 2020, p. 258 et s.

189. « Capteurs thermiques piétons : un bilan positif », *Le républicain lorrain,* 2 juin 2023 et M. Hecky, « Des caméras à capteurs thermiques pour traverser plus facilement à Metz », *France 3 Lorraine,* 19 mars 2018.

190. R. Dissoubray, « Des capteurs qui aident à penser la métropole de demain », *Le bien public,* 16 décembre 2021.

191. C. Murat, « D'ici juin, un observatoire environnemental », *Le bien public,* 23 novembre 2020.

192. Accessible en ligne [https://www.airparif.asso.fr/toutes-nos-cartes].

193. En ce sens, v. CNIL – LINC, *La plateforme d'une ville, op. cit.*, p. 26.

194. Par exemple, à Dijon, Nantes, Rennes et Paris. V. not. Dijon métropole, *OnDijon. Dijon métropole met en service un projet inédit de smart city en France,* dossier de presse, 11 avril 2019, p. 13 et CEREMA, *Villes et territoires intelligents, de nouveaux défis*, Cerema éditions, 2022, p. 9.

195. Dans le cadre du projet de ville intelligente OnDijon, la métropole bourguignonne a équipé plus d'une centaine de feux de signalisation de capteurs détectant la présence de bus afin d'accorder une priorité de circulation aux transports collectifs. L'initiative permet d'accélérer le déplacement des voyageurs et la fluidité du trafic. D'autres capteurs de stationnement permettent, eux, à Dijon comme à Cannes, de mesurer en temps réel le temps d'occupation et la disponibilité des places de livraison et de stationnement « minute ». En cas de stationnement prolongé, estimé abusif, la police municipale est avertie au « poste de pilotage connecté » qui fait office de CSU amélioré. Sur ces questions, v. *idem*, p. 7, 13 et 14. L'entreprise Synox revendique sur son site internet l'installation de 450 capteurs de stationnement à Dijon. Pour Cannes, v. Syndicat des équipements de la route, « La ville de Cannes expérimente le comptage à la place », 16 mai 2015 [https://www.equipements-routiers-et-urbains.com/content/la-ville-de-cannes-experimente-le-comptage-la-place].

196. Le principal outil de *tracing* utilisé en matière de police administrative l'a cependant été, non au niveau municipal, mais au niveau national, et dans une perspective sanitaire plus que sécuritaire, avec l'application « TousAntiCovid », lors de l'épidémie de Covid-19. L'application de traçage numérique affichait pour ambition de « limiter les risques d'exposition et remonter toutes les chaînes de transmission pour alerter et être prévenu(e) en cas d'exposition à la Covid-19 » (ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique, « Pass sanitaire : toutes les informations utiles », 8 mars 2022 [https://www.economie.gouv.fr/tousanticovid-signal-cahier-rappel-numerique]). Elle reposait par ailleurs sur la technologie *Bluetooth* (*i.e.* ondes radio) et non sur une géolocalisation par GPS (géo-positionnement par satellite). V. sur ce dispositif L. Cluzel-Métayer, « La datasurveillance de la covid-19 », *RDSS,* 2020, p. 918 et s.

197. CNIL – LINC, *La plateforme d'une ville, op. cit.,* p. 24.

198. V. les « études de cas » sur le site de l'entreprise [https://www.flowly.re/etudes-rouen/].

199. Sur l'initiative Optimod, v. CNIL – LINC, *La plateforme d'une ville, op. cit.,* p. 30.

200. *Ibidem*.

201. *Ibidem* et L. Mauron, « L'application Waze et Versailles Grand Parc échange leurs données de trafic », *Le Parisien,* 30 octobre 2016.

202. V. sur la présentation du dispositif sur le site internet de l'entreprise [https://www.waze.com/wiki/UAE/Connected_Citizens_Program], les études de cas [https://www.waze.com/fr/wazeforcities/casestudies], ainsi que la carte en temps réel du réseau mondial [https://www.waze.com/fr/live-map?utm_source=waze_website&utm_campaign=waze_website&utm_medium=website_menu].

203. V. par exemple les initiatives à Lannion et à Rennes relayées par l'initiative Technopolice : V. Fuseau, « Centre-ville de Lannion. Vos pas seront comptés », *Le télégramme,* 25 juin 2019 et C. Allain, « Rennes : les commerçants reportent la mise en service des capteurs wifi suivant les smartphones », *20 minutes,* 9 mars 2017.

204. CNIL – LINC, *La plateforme d'une ville, op. cit.,* p. 25.

205. Art. L. 851-1 à L. 851-6 du CSI. Sur le sujet, v. M-A. Granger, « La géolocalisation de sécurité : approche jurisprudentielle », *in Annuaire du droit de la sécurité et de la défense,* Paris, Mare & Martin, 2023, p. 103-111.

206. CE, 8 février 2017, *Société JCDecaux France,* n° 393714.

207. CNIL, Délibération n° 2015-255, 16 juillet 2015.

208. *Ibidem.*

209. *Ibidem.*

210. CE, 8 février 2017, *op. cit*.

211. *Idem,* cons. 8.

212. C. Jones, R. Lanneau & Y. Maccanico, *Europe's Techno Borders, op. cit.,* p. 5.

213. V. à titre général le rappel à l'ordre de quatre communes par la CNIL : CNIL, « Verbalisation par lecture automatisée des plaques d'immatriculation (LAPI) : la CNIL met en garde contre les mauvaises pratiques », 25 août 2020. V. aussi CE, 27 juin 2016, *Commune de Gujan-Mestras,* n° 385091, Lebon.

214. A-S. Hourdeaux, « Vidéo-surveillance à Roubaix : des technologies de pointe pour garder l'œil sur la ville », *Lille Actu,* 17 janvier 2020, et « À Roubaix, une vingtaine de PV chaque jour », *Nord éclair,* 8 janvier 2021.

215. Cour des comptes, référé S2021-2194, *op. cit*.

216. V. ici : C. Lequesne-Rothe, *New Surveillance Technologies in Public Spaces, op. cit.*, p. 40, renvoyant aussi à C. Castets-Renard, P. Besse, J-M. Loubes et L. Perrussel, *Encadrement des risques techniques et juridiques des activités de police prédictive*, rapport 2019 CHEMI, ministère de l'Intérieur, 12 juillet 2019, p. 13 ; R. Demichelis et M. Warnet, « Quand la gendarmerie utilise les algorithmes pour prévoir les cambriolages », *Les Échos,* 30 juin 2018.

217. Sur cette question, v. Y. Nabat, *Fichiers de police et de justice et libertés fondamentales,* thèse dactylographiée, Université de Bordeaux, 2023, 747 p.

218. Étymologiquement, « *instauratio* » en latin signifie renouvellement. Par ce terme, nous souhaitons insister sur le renouvellement de la police administrative et, en certains points, de ses enjeux et de son cadre juridique. Couramment, l'acception retenue du verbe « instaurer » s'approche de « établir, fonder, instituer » (*Dictionnaire de l'Académie française,* 9e éd.). En transparence, nous souhaitons également convoquer cette nuance d'un renouvellement « fondateur » pour souligner une interrogation quant à la portée de la transformation des structures de la police administrative : continuité ou changement de paradigme – le cas échéant, plus politique que juridique ?

219. X. Latour, « Sécurité intérieure : un droit "augmenté" ? », *op. cit.*

220. X. Latour, « La sécurité intérieure, entre échelon national et échelon local », *op. cit*. V. plus justement encore X. Latour, « Les technologies et la loi relative à la sécurité globale : un flop ? », *op. cit.* : « les retours des expérimentations paraissent rarement conduire à faire marche arrière ». V. aussi B. Warusfel, « Technologie et sécurité : réguler pour reprendre le contrôle », *op. cit.,* p. 258 : « la vidéosurveillance publique nous montre déjà comment le recours à la technologie entraîne presque inévitablement la recherche d'une justification *a posteriori* qui interdit tout retour en arrière (même lorsque le législateur avait prudemment prévu une phase d'expérimentation) ».

221. Dans une perspective critique autre, des parlementaires ont évoqué à cet égard une « aboulie politico-administrative » (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, op. cit.*, p. 73).

222. *Supra*, note 2.

223. Conseil d'État, *IA et action publique, op. cit.,* p. 157.

224. Dijon métropole, *OnDijon, op. cit.,* p. 16-19. V. aussi J-B. Auby, « Les *Smart Cities* », *op. cit.,* p. 120, et note 36 pour des références permettant d'approfondir la relation entre *Smart city* et commande publique.

225. Thales, « Nice : la sécurité à la pointe de la technologie », 9 octobre 2012 [https://www.thalesgroup.com/fr/monde/defence-and-security/news/nice-securite-pointe-technologie]. V. surtout Convention d'expérimentation, de mise à disposition et de démonstration du projet « Safe city », conclue le 2 septembre 2018 entre Thales Communications & Secutity SAS d'une part, et la ville de Nice et la métropole Nice Côte d'Azur d'autre part, une fois de plus obtenu par

la Quadrature du net et accessible en ligne [https://data.technopolice.fr/fr/document/r5cv3oyalj?page=1].

226. Sur la question, v. not. : Technopolice, « Les entreprises », en ligne [https://technopolice.fr/entreprises/] ; Picaud, M., « Les Smart Cities : un gouvernement par la performance à l'échelle locale ? Analyse de la construction d'un marché de dispositifs numériques pour l'espace urbain en France », *working paper,* Science po, Cities and Digital Technology Chair, n° 05/2020 ; Picaud, M., « Mettre en marché les peurs urbaines : le développement des "*safe cities*" numériques », *Sociétés en danger,* 2021, p. 139-156.

227. B. Warusfel, « Technologie et sécurité : réguler pour reprendre le contrôle », *op. cit.,* p. 258. En matière de santé publique, v. aussi L. Cluzel-Métayer, « La datasurveillance de la covid-19 », *op. cit.*

228. CNIL – LINC, *La plateforme d'une ville, op. cit.,* p. 17.

229. V. Conseil d'État, *IA et action publique, op. cit.,* p. 157.

230. *Idem,* p. 157-158.

231. Sur le développement d'un complexe militaro-industriel français, v. *inter alia* les travaux de Mathieu Rigouste, not. « La police du futur », *Revue du crieur,* n° 10, 2018/2, p. 32-47 et « Des jeux dont vous êtes le cobaye. Business sécuritaire et spectacle olympique », *Revue du crieur,* n° 22, 2023/1, p. 46-59.

232. Art. 10, IX, de la loi JOP 2024.

233. La Quadrature du Net, *Projet de loi relatif aux Jeux olympiques et paralympiques de 2024 : dossier d'analyse de la vidéosurveillance automatisée*, *op. cit.,* p. 32-33.

234. *Ibidem.* V. aussi la Convention de partenariat entre la ville de Suresnes et la société XXII group du 1er février 2021, accessible en ligne [https://data.technopolice.fr/fr/entity/qfqn9izd0g].

235. Conseil d'État, *IA et action publique, op. cit.,* p. 159.

236. CNIL – LINC, *La plateforme d'une ville, op. cit.* p. 32.

237. *Ibidem.*

238. *Idem,* p. 33.

239. En ce sens, v. *ibidem.*

240. V. la présentation du projet sur le site de la métropole de Nantes [https://data.nantesmetropole.fr/pages/home/]. V. surtout, plus largement, É. Bothorel et *al*., *Pour une politique publique de la donnée,* rapport de la mission Bothorel remis au Premier ministre, décembre 2020.

241. Souligné not. *in* CNIL – LINC, *La plateforme d'une ville, op. cit.* p. 33-34.

242. Art. L. 3131-2 du Code de la commande publique (nous soulignons).

243. Sur le droit d'accès aux règles définissant le traitement algorithmique ayant engendré une décision individuelle pour l'administré sujet de cette décision, v. art. L. 311-3-1 du CRPA. Sur la publication des règles gouvernant les principaux traitements algorithmiques utilisés par l'administration dans l'exercice de ses missions et fondant des décisions individuelles, v. art. L. 312-1-3 du CRPA. Il existe toutefois trois limites : ne sont pas concernés les traitements algorithmiques qui ne donnent pas lieu à des décisions individuelles ; ne sont communicables que les informations mentionnées à l'art. R. 311-3-1-2 du CRPA ; plusieurs secrets font l'objet d'une protection énoncée à l'art. L. 311-5, 2° du CRPA et sont susceptibles de minimiser les informations communicables (not. g), sur la recherche et la prévention d'infractions, et h), sur les secrets protégés par la loi, en particulier le secret des affaires). V. L. Cluzel-Métayer, « La transparence du service public à l'heure du numérique. Lumière, ombre et aveuglement », *in* L. Cluzel-Métayer et *al.* (dir.), *La transformation numérique du service public, op. cit.,* p. 205-220.

244. Conseil d'État, *IA et action publique, op. cit.,* p. 120.

245. Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle et modifiant certains actes législatifs de l'Union, 21 avril 2021, COM(2021) 206 final.

246. Art. 13 du règlement IA.

247. Conseil d'État, *IA et action publique, op. cit.,* p. 120.

248. *Idem,* p. 200. En ce sens, v. la proposition n° 22 *in* 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, op. cit.*, p. 81-82.

249. Nous soulignons.

250. Conseil d'État, *IA et action publique, op. cit.,* p. 133.

251. Sur les rapports public-privé en la matière, v., entre autres, M. Lecoquierre et F. Tréguer, « Villes sous contrôle et technologisation du maintien de l'ordre. Entretien avec Félix Tréguer », *op. cit.* not. questions 10 à 12.

252. Sur ces enjeux, v. Conseil d'État, *IA et action publique, op. cit.,* not. p 100 et 126. En ce qui concerne les « traitements de données à caractère personnel mis en œuvre pour le compte de l'État et qui intéressent la sûreté de l'État ou la défense », l'article 121 de la LIL dispose que « le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ». Si la personne privée n'est pas responsable du traitement pour le compte de l'État et se borne à une activité de sous-traitance, les dispositions de l'article 122 de la LIL lui seront néanmoins applicables. Il devra à ce titre présenter des garanties suffisantes de sécurité et honorer les obligations de sécurité prévues par le contrat conclu avec le responsable du traitement.

253. Sénat (M-P. Daubresse, A. Belenet et J. Durain), *Rapport d'information sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles*, *op. cit.*, p. 13.

254. En ce sens, v. la Quadrature du Net, *Projet de loi relatif aux Jeux olympiques et paralympiques de 2024 : dossier d'analyse de la vidéosurveillance automatisée*, *op. cit.,* p. 12 et 19.

255. CC, Décision n° 2021-817 DC, *op. cit.* V. en amont, déjà sur la vidéoprotection, CC, Décision n° 2011-625 DC, 10 mars 2011, *Loi d'orientation et de programmation pour la performance de la sécurité intérieure,* not. § 19. V. aussi : CC, Décision n° 2017-637 QPC, 16 juin 2017, *Association nationale des supporters,* § 4-5 ; CC, Décision n° 2017-695 QPC, 29 mars 2018, *M. Rouchdi B. et autres,* § 17 et § 26-27. En doctrine, v. X. Latour, « L'article 12 de la Déclaration des droits de l'homme et du citoyen et le Conseil constitutionnel », *in Annuaire du droit de la sécurité et de la défense,* Paris, Mare & Martin, 2021, p. 31-39.

256. CC, Décision n° 2021-940 QPC, 15 octobre 2021, *Société Air France*.

257. CC, Décision n° 2023-1042 QPC, 31 mars 2023, *Syndicat national unifié des personnels des forêts et de l'espace naturel*, not. § 23 : cette interdiction n'est pas méconnue par l'article L. 222-6, 2°, du Code forestier, par lequel le législateur a pu disposer que l'Office national des forêts « peut employer des agents contractuels de droit privé accomplissant pour son compte des missions de police administrative ». V. sur cette décision J. Petit, « L'exercice de missions de police par des agents de droit privé », *AJDA*, 2023, p. 1691-1699.

258. *Supra,* note 255.

259. CC, Décision n° 2021-817 DC, *op. cit.*, § 51-60.

260. CE, 20 décembre 1997, *Commune d'Ostricourt,* n° 170606, mentionné aux tables. En amont, v. : CE, 1er avril 1994, *Commune de Menton,* nos 144152 et 144241, Lebon ; CE, Ass., 17 juin 1932, *Ville de Castelnaudary,* n° 12045, Lebon. V. ici O. Renaudie, « Police et service public », *in* C. Vautrot-Schwarz (dir.), *La police administrative générale,* Paris, PUF, 2014, p. 46-47.

261. Art. 10, I et VI, de la loi JOP 2024.

262. Assemblée nationale, mercredi 8 mars 2023, compte-rendu n° 41, p. 45 (allocution de Guillaume Vuilletet, rapporteur), souligné not. *in* la Quadrature du Net, Syndicat des avocats de France, Syndicat de la magistrature, CREIS-TERMINAL, Ligue des droits de l'homme, contribution extérieure sur la loi relative aux Jeux olympiques et paralympiques de 2024 et portant diverses

autres dispositions (affaire n° 2023-850 DC), reçue au greffe du Conseil constitutionnel le 19 avril 2023, p. 17. En ce sens, v. aussi la contribution extérieure du député Philippe Latombe, du 21 avril 2023, reçue au greffe du Conseil constitutionnel le 2 mai 2023.

263. ANR, « Lancement des projets lauréats de l'appel à projets Flash JOP24 », communiqué de presse du 23 janvier 2020 [https://anr.fr/]. Parmi les autres lauréats figurent les sociétés Orange (projet DISCRET) et ID3 Technologies (projet EASIMoB).

264. V. l'avis de marché n° 23-181232 du 5 janvier 2024, *Bulletin officiel des annonces de marchés publics*.

265. La Quadrature du Net et autres, contribution extérieure sur la loi JOP 2024, *op. cit.,* p. 17.

266. TA Marseille, 2 juin 2023, *LQDN c. ville de Marseille,* n° 2009485, not. § 1, 6 et 8. Le contrat portait, plus précisément, sur « la fourniture et l'intégration d'une solution globale fonctionnelle » incluant un logiciel de « vidéoprotection intelligente ». Étaient concernés « le déploiement informatique, le paramétrage des fonctionnalités, la formation et la maintenance » ainsi que, le cas échéant, « l'extension du déploiement du dispositif ».

267. V. les moyens *in ibidem.*

268. CE, 30 juin 2017, *Syndicat mixte de promotion de l'activité transmanche,* n° 398445, Lebon.

269. Nous tenons à remercier Madame Célie Simeray, rapporteure publique, pour la communication de ses conclusions dans cette affaire.

270. TA Marseille, 2 juin 2023, *op. cit.*, not. § 8.

271. L. Vanier, « *Saving Private* Radars », *AJDA,* 2020, p. 130-136.

272. Sur l'impossible concentration maintenue des agents face au flux vidéo, v. 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, op. cit.*, p. 61-62.

273. CNIL, « Caméras dites 'intelligentes' ou 'augmentées' dans les espaces publics », *op. cit.,* p. 7.

274. V. ici : A. de Mesnard, « La *Smart city* à l'épreuve du RGPD : l'ambivalence d'une participation citoyenne "mise en vitrine" », *RevDH,* n° 21, 2022, not. § 5-7 ; P. Türk, « La citoyenneté à l'ère numérique », *RDP*, n° 3, 2018, p. 623 et s. Sous un angle différent, v. aussi P. Cardullo & R. Kitchin, « Being a 'citizen' in the smart city: up and down the scaffold of smart citizen participation in Dublin, Ireland », *GeoJournal,* n° 84, 2019, p. 1-13.

275. *Idem,* § 2.

276. V. la présentation de l'application sur le site dédié [https://fixmystreet.brussels/], ainsi que la cartographie élaborée par les signalements [https://fixmystreet.brussels/list].

277. La plateforme, développée par l'entreprise Spallian, compte parmi ses clients de nombreuses collectivités (Agen, Argenteuil, Arras, Cahors, Cholet, Clichy, Fontainebleau, Lacanau, Libourne, Limoges ainsi que Montauban). Pour une liste plus complète, v. le site de l'entreprise. V. aussi : M. Lenhardt, « À Argenteuil, l'application qui fait faire des économies à la ville », *Le parisien,* 2 janvier 2019 ; G. Dyson, « Montauban. La mairie met en place Tell My City, une application pour signaler les problèmes en ville », *La dépêche,* 26 octobre 2021.

278. Dijon métropole, *OnDijon, op. cit.,* p. 7.

279. A. de Mesnard, « La *Smart city* à l'épreuve du RGPD : l'ambivalence d'une participation citoyenne "mise en vitrine" », *op. cit.*, not. § 7.

280. Cette application peut, par ailleurs, être mise en perspective avec l'initiative « Voisins vigilants » ou le dispositif « Participation citoyenne », qui permettent tous deux d'impliquer les citoyens dans une activité de police et de surveillance. Sur ces questions, v. : CNIL – LINC, *Les caméras au village, op. cit.,* 2021, p. 29-30 ; F. Durand, « La participation citoyenne à la sécurité », *in Annuaire du droit de la sécurité et de la défense,* Paris, Mare & Martin, 2020, not. p. 158-163.

281. Ville de Nice, *Application mobile pilote "Reporty". Charte d'utilisation*, janvier 2018, annexée à CNIL, courrier de la présidente du 10 avril 2018, réf. IFP/AME/DI181074, obtenu par la Quadrature du net [https://www.laquadrature.net/files/Avis_CNIL_Reporty_20180723.pdf].

282. « Nice : la ville teste "Reporty", l'application israélienne d'appels vidéo en direct à la police », *20 minutes & AFP,* 15 janvier 2018.

283. Propos du maire de Nice, Christian Estrosi, rapportés *in ibidem* et *in* CNIL, courrier de la présidente du 10 avril 2018, *op. cit.*, p. 3.

284. CNIL, courrier de la présidente du 10 avril 2018, *op. cit.*

285. *Ibidem.* La CNIL relevait ici la « captation de l'image et de l'environnement sonore d'une personne laissant un objet sur le trottoir le temps d'aller chercher sa voiture pour le récupérer, ou encore jetant dans le caniveau un mégot de cigarette ou ne ramassant pas les déjections de son chien sur la voie publique ».

286. *Idem*, p. 8-9. Le Syndicat de défense des policiers municipaux évoquant lui-même la délégation d'« un service public de sécurité à des citoyens » (retranscrit p. 12).

287. *Idem*, p. 6.

288. CNIL – LINC, *La plateforme d'une ville, op. cit.*, p. 44.

289. Sur le concept de « *digital labor* », v. not. : T. Scholtz, *Digital Labor: The Internet as Playground and Factory*, Routledge, 2012, 272 p. ; C. Fuchs, *Digital Labour and Karl Marx*, Routledge, 2014, 424 p. ; D. Cardon et A. Casilli, *Qu'est-ce que le digital labor ?*, INA, 2015, 101 p.

290. Sur la qualification de collaborateur occasionnel du service public d'un informateur des douanes, v. CE, 13 janvier 2017, *M. B. c. ministre du Budget,* n° 386799, Lebon.

291. Sur le refus d'octroi de la protection fonctionnelle à un informateur des douanes en raison d'une faute personnelle détachable du service, v. *ibidem.*

292. A. de Mesnard, « La *Smart city* à l'épreuve du RGPD : l'ambivalence d'une participation citoyenne "mise en vitrine" », *op. cit.*, § 9.

293. Pour une réflexion proche au sujet du dispositif de participation citoyenne « voisins vigilants » et de la réserve citoyenne, v. M. Wujek-Moreau, *La responsabilité du fait des activités de police,* thèse dactylographiée, Université de Limoges, 2019, p. 222-227.

294. Par exemple, sur le principe général du droit selon lequel cette qualification emporte protection fonctionnelle de la part de l'administration, en l'absence de faute personnelle et à moins qu'un intérêt général ne s'y oppose (CE, 13 janvier 2017, *op. cit.,* cons. 3).

295. CE, 9 octobre 1970, *commune de Saint-Michel de Volangis,* n° 74635. V. plus généralement T. Olson, entrée « Collaborateurs occasionnels ou bénévoles du service public – Champ d'application » *in Répertoire de la responsabilité de la puissance publique,* not. § 38-66. Sur l'urgente nécessité, v. spéc. § 47-49.

296. T. Olson, « Collaborateurs occasionnels ou bénévoles du service public – Champ d'application », *op. cit.,* § 49.

297. CE, 14 décembre 1988, *commune de Catillon-Fumechon,* n° 61492, mentionné aux tables.

298. A. Belrhali, « La responsabilité administrative de demain. Potentialités et contentieux potentiels », *AJDA,* 2021, p. 1250 et s. L'auteure relevait not. en préambule : « Dessiner l'avenir de la responsabilité administrative constitue un exercice passionnant d'anticipation. La démarche est néanmoins périlleuse car, immergé dans son contexte et sans don pour la prescience, l'observateur peut bien entendu se tromper ».

299. Conseil d'État, *IA et action publique, op. cit.,* p. 148.

300. *Ibidem.*

301. *Idem,* p. 108.

302. *Idem*, p. 152.

303. *Ibidem.* À cet égard, était évidemment exclue par la section du rapport et des études l'hypothèse fantasmatique et « inutile » d'une responsabilité propre du SIA (p. 149). En ce sens, v. aussi Parlement européen, Parlement européen, *Un régime de responsabilité civile pour l'intelligence artificielle,* résolution du 20 octobre 2020, (2020/2014(INL)), pt. 7.

304. V. M. Wujek-Moreau, *La responsabilité du fait des activités de police, op. cit.,* p. 256-260.

305. En ce sens, CE, 10 octobre 2011, *ministre de l'Alimentation, de l'Agriculture et de la Pêche,* n° 337062, Lebon. V. ici G. Eckert, « Police et contrat », *in* C. Vautrot-Schwarz (dir.), *La police administrative générale, op. cit.*, not. p. 182-183.

306. M. Wujek-Moreau, *La responsabilité du fait des activités de police, op. cit.,* p. 260.

307. Conseil d'État, *IA et action publique, op. cit.,* p. 149.

308. *Idem,* p. 149-150.

309. M. Wujek-Moreau, *La responsabilité du fait des activités de police, op. cit.,* p. 369-370.

310. Sur l'illégalité fautive en matière de police, v. spéc. *idem,* p. 355-364. Quant au degré de la faute, lourde ou simple, v. p. 343-346, not. p. 343 : « le régime de la faute lourde, qui était hier le régime de principe, est désormais devenu le régime d'exception, au point qu'il est permis de se demander s'il existe encore réellement ». V. aussi : G. Éveillard, « Existe-t-il encore une responsabilité administrative pour faute lourde en matière de police administrative ? », *RFDA,* 2006, p. 733-747 ; M. Deguergue, « La responsabilité du fait des activités de police », *in* C. Vautrot-Schwarz (dir.), *La police administrative générale, op. cit.*, p. 221-240.

311. Conseil d'État, *IA et action publique, op. cit.,* p. 149-150.

312. *Idem,* p. 150-151.

313. *Ibidem.* V. aussi CE, 8 mars 1991, *Société Usinor,* n° 70216, Lebon.

314. Depuis CE, 26 juillet 1918, *Époux Lemonnier,* n° 49595, Lebon.

315. Sur la nature de la carence, v. respectivement CE, 28 novembre 20023, *commune de Moissy-Cramayel,* n° 238349, Lebon (carence juridique et tranquillité publique), CE, 14 octobre 1977, *commune de Catus,* n° 01404, Lebon (carence matérielle et sécurité publique), CE, 8 novembre 1985, *commune de Lacanau,* n° 35177, mentionné aux tables (carence totale et sécurité publique), et CE, 27 juillet 2005, *ville de Noisy-le-Grand,* n° 257394, mentionné aux tables (carence partielle et tranquillité publique). Sur la question, v. spéc. P. Bon, entrée « Police municipale : principes de fond », *in Encyclopédie des collectivités territoriales,* folio n° 2220, 2019, § 20.

316. Conseil d'État, *IA et action publique, op. cit.,* p. 151.

317. *Ibidem.* V. déjà European Commission (Experts Group), *Liability for Artificial Intelligence and other emerging digital technologies,* Publications Office of the European Union, 2019, p. 62-65.

318. Sur une responsabilité civile sans faute en cas de matérialisation du risque, v. la position précautionneuse de la Commission européenne *in Rapport sur les conséquences de l'intelligence artificielle, de l'internet des objets et de la robotique sur la sécurité et la responsabilité,* 19 février 2020, COM(2020) 64 final, p. 19.

319. Pour le détail de ces obligations, v. *infra.*

320. Not. CE, 28 mars 1919, *Regnault-Desroziers*, n° 62273, Lebon, et CE, Ass., 24 juin 1949, *Consorts Lecomte*, n° 87335, Lebon.

321. Sur ce point, soulignons, d'une part, que le règlement IA inclut la protection contre les menaces à la sécurité publique ainsi que leur prévention parmi les « fins répressives » (art. 3, 41)) et, d'autre part, les SIA des autorités répressives constituent l'une des huit catégories envisagées de SIA à haut risque au sens de l'article 6, par. 2. Parmi les cas envisagés figurent notamment les SIA participant à l'évaluation individuelle des risques de commission d'une infraction ou de profilage (annexe III, 6, a), e) et f)), ce qui inclut possiblement la VSA en fonction de ses usages. Par ailleurs, les SIA « destinés à être utilisés pour envoyer ou établir des priorités dans l'envoi des services d'intervention d'urgence » tombent aussi dans le champ des SIA à haut risque liés à l'accès au service public (annexe III, 5, c)). Le recours à la VSA aux fins d'optimisation des interventions des unités d'intervention de police pourrait possiblement être couvert par cette hypothèse. Tel est encore le cas des SIA « destinés à être utilisés en tant que composants de sécurité dans la gestion et l'exploitation du trafic routier » (annexe III, 2, a)) et des SIA « destinés à être utilisés pour l'identification biométrique à distance "en temps réel" et "a posteriori" des personnes physiques » (annexe III, 1, a)).

322. Parlement européen, résolution du 20 octobre 2020, *op. cit.*, pt. 13. V. art. 11 de la proposition de règlement. La résolution insistait aussi sur l'obstacle que représente pour la victime la preuve d'une faute du fournisseur privée comme de l'administration utilisatrice en raison des propriétés des SIA : complexité, connectivité, opacité, vulnérabilité et caractère évolutif (pts. 6-7).

323. *Idem,* pt. 14. V. art. 4 de la proposition de règlement. Sur les critères permettant d'identifier un SIA à haut risque, v. pt. 15. Quant à la responsabilité du fait des SIA à risque modéré, elle demeurait envisagée sous l'angle de la responsabilité pour faute.

324. Conseil d'État, *IA et action publique, op. cit.,* p. 152.

325. Conseil d'État, *IA et action publique, op. cit.,* p. 148-149.

326. « Le producteur est responsable du dommage causé par un défaut de son produit, qu'il soit ou non lié par un contrat avec la victime ».

327. Art. 1245-8 du Code civil.

328. Art. 1245-3 du Code civil.

329. Art. 1245-10 du Code civil.

330. En ce sens, v. Conseil d'État, *IA et action publique, op. cit.,* p. 152, note 198.

331. Commission européenne, *Livre blanc. Intelligence artificielle, op. cit.*, p. 15. V. aussi Commission européenne, *Rapport sur les conséquences de l'intelligence artificielle, de l'internet des objets et de la robotique sur la sécurité et la responsabilité, op. cit.*, p. 1.

332. *Ibidem* et, *a fortiori,* Commission européenne, *Rapport sur les conséquences de l'intelligence artificielle, de l'internet des objets et de la robotique sur la sécurité et la responsabilité, op. cit.*, p. 14-17.

333. Soulignons que le secret des affaires pourrait constituer un obstacle supplémentaire. *Supra*, note 243.

334. Commission européenne, *Rapport sur les conséquences de l'intelligence artificielle, de l'internet des objets et de la robotique sur la sécurité et la responsabilité, op. cit.*, p. 16.

335. À cet égard, soulignons l'intérêt de l'art. 145 du Code de procédure civile qui permet le prononcé de mesures d'instruction *in futurum* en référé sous réserve de la démonstration d'un motif légitime, voire d'ordonnances sur requête dans le cadre d'une procédure qui met à l'écart le contradictoire aux fins de sauvegarde des éléments de preuve.

336. Commission européenne, *Livre blanc. Intelligence artificielle, op. cit.*, p. 17-18. *A minima*, une adaptation et une clarification des régimes en vigueur au niveau national devaient selon elle intervenir pour mieux répondre aux spécificités de l'IA. *A maxima,* des dispositions spécifiquement dédiées à l'IA devaient être envisagées.

337. Parlement européen, résolution du 20 octobre 2020, *op. cit.*, pt. 20 et art. 8 de la proposition de règlement.

338. De nombreux travaux ont précédé la proposition de règlement avancée. Parmi eux, plusieurs évoquent l'enjeu de la responsabilité, not. : European Commission, *Liability for Artificial Intelligence and other emerging digital technologies, op. cit.* ; Commission européenne, *Rapport sur les conséquences de l'intelligence artificielle, de l'internet des objets et de la robotique sur la sécurité et la responsabilité, op. cit.* ; Parlement européen, résolution du 20 octobre 2020, *op. cit.*

339. V. ici les art. 9 à 15 du règlement IA.

340. V. ici les art. 16 à 22 du règlement IA.

341. Conseil d'État, *IA et action publique, op. cit.,* p. 152.

342. Art. 9, 7) du RGPD : « Aux fins du présent règlement, on entend par : [...] "responsable du traitement", la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul *ou conjointement avec d'autres*, détermine les finalités et les moyens du traitement » (nous soulignons).

343. A. Belrhali, « La responsabilité administrative de demain », *op. cit.*

RÉSUMÉS

En septembre 2019, un conglomérat 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. La présente contribution prend au sérieux le concept employé et le décline dans le champ de la police administrative. Les rapports prospectifs ou évaluatifs des juridictions, Conseil d'État et Cour des comptes en tête, comme les sanctions et prises de position récurrentes de la CNIL, ainsi que les contentieux et les débats législatifs récents, attestent, en effet, que le phénomène va au-delà de la simple préoccupation associative. Il correspond à un objet juridique moderne. Le présent article envisage dès lors certaines conséquences normatives de l'équipement et de la mobilisation croissante de dispositifs technologiques, en particulier numériques, aux fins d'exercice des missions de police administrative.

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. This contribution takes the concept seriously and applies it to the field of administrative policing. Some reports of administrative courts (Conseil d'État, Cour des Comptes), 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 refers to a modern legal issue. This article therefore considers some of the normative consequences of the equipment and the increasing mobilization of technological – mainly digital – devices for the purposes of carrying out administrative police missions.

INDEX

Mots-clés : technopolice, surveillance, villes numériques, algorithmes, intelligence artificielle
Keywords : technopolice, surveillance, smart cities, algorithms, artificial intelligence

AUTEUR

ROBIN MEDARD INGHILTERRA

Robin Medard Inghilterra est Maître de conférences en droit public à l'Université Paris 1 Panthéon-Sorbonne, membre de l'Institut des sciences juridique et philosophique de la Sorbonne (UMR 8103), chercheur associé au Centre Perelman de philosophie du droit de l'Université libre de Bruxelles