La Smart city à l'épreuve du RGPD : l'ambivalence d'une participation citoyenne « mise en vitrine »

Adèle de Mesnard

Édition électronique

URL : <https://journals.openedition.org/revdh/14244>

DOI : [10.4000/revdh.14244](https://doi.org/10.4000/revdh.14244)

ISSN : 2264-119X

Éditeur

Centre de recherches et d'études sur les droits fondamentaux

Référence électronique

Adèle de Mesnard, « La Smart city à l'épreuve du RGPD : l'ambivalence d'une participation citoyenne « mise en vitrine » », *La Revue des droits de l'homme* [En ligne], 21 | 2022, mis en ligne le 19 janvier 2022, consulté le 15 février 2023. URL : <http://journals.openedition.org/revdh/14244> ; DOI : <https://doi.org/10.4000/revdh.14244>

Ce document a été généré automatiquement le 26 septembre 2022.

Tous droits réservés

La Smart city à l'épreuve du RGPD : l'ambivalence d'une participation citoyenne « mise en vitrine »

Adèle de Mesnard

Introduction

- ¹ A l'aune de la crise sanitaire, la résilience des territoires passe-t-elle par le redéploiement des technologies mises en place au sein des *Smart cities* ? La crise a-t-elle montré les bienfaits du concept de *Smart city* ? C'est le constat que semble opérer un certain nombre de revues spécialisées¹ mettant en lumière une incitation croissante à la collecte et au partage de grands volumes de données personnelles pour le bien commun. Les exemples sont nombreux et composites, modifiant les comportements à l'égard de la surveillance des personnes et révélant dans le même temps les tâtonnements des pouvoirs publics qui peinent à obtenir l'adhésion de l'opinion publique quant à la sécurité des données personnelles. On peut citer l'utilisation des capteurs thermiques afin d'identifier les personnes présentant des symptômes de maladie épidémique et favoriser ainsi leur mise en quarantaine (Singapour), la diffusion d'alertes et le déploiement du réseau de vidéosurveillance pour s'assurer que la population respecte le confinement (Nice) ou encore les partenariats avec le secteur privé aux fins de mieux comprendre l'évolution de la Covid-19 (en Australie, avec les données transactionnelles et en Angleterre avec les données de santé). L'utilisation d'applications « citoyennes » de mise en relation des autorités publiques et des citoyens pour permettre de signaler à ces derniers, en temps réel, qu'ils sont au contact de personnes potentiellement affectées s'est généralisée. Il en est de même de l'usage du « backtracking » qui consiste à utiliser les données personnelles de géolocalisation GPS contenues dans les téléphones des individus testés positifs pour suivre et surveiller leurs mouvements.

- 2 Bien que légaux, et donc rentrant dans le champ d'application du droit européen de la protection des données personnelles², ces outils, qui ont permis de localiser, de suivre et de surveiller les personnes infectées et celles confinées, semblent témoigner de la prééminence d'une vision sécuritaire de la gestion de l'espace public. Dans ce cadre, 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. Or, cet appel à la participation des citoyens, lié à la collecte intensive de données personnelles, peut légitimement nous interpeler. Comment l'entendre dans le cadre des projets de *Smart city* ? Quelles sont les ambiguïtés liées à l'usage même du terme « participation » et qu'impliquent-elles, d'un point de vue juridique, vis-à-vis du consentement éclairé des citoyens et de la protection de leurs données personnelles ? La promotion d'une participation citoyenne pourtant difficilement saisissable (I) met en lumière les ambiguïtés du régime juridique instauré par le Règlement Général sur la Protection des Données (RGPD) quant à la protection des libertés individuelles des citoyens (II).

I. La promotion d'une participation citoyenne pourtant difficilement saisissable

- 3 La participation citoyenne peut être définie comme un « processus d'engagement obligatoire ou volontaire de personnes ordinaires, agissant seules ou au sein d'une organisation, en vue d'influer sur une décision portant sur des choix significatifs qui toucheront leur communauté³ ». Bien qu'elle en soit un préalable, la participation citoyenne ne se résume donc pas à une simple information, voire à une consultation des citoyens à propos de décisions déjà actées qu'il faudrait légitimer. Et l'influence ne peut se contenter d'être seulement un droit à la contestation des mesures envisagées. En écartant les débats quant à la dimension démocratique de la participation citoyenne, celle-ci témoigne d'un pouvoir d'agir « avec », sans que les oppositions ne soient considérées comme une rupture dans la prise de décision. Elle implique un réel engagement des citoyens en amont de la prise de décision, leur permettant d'agir sur ce qui les intéresse et les affecte dans la production de la ville. Cette définition est particulièrement intéressante dans le cadre d'une analyse de la *Smart city* car elle questionne tant la problématique de l'engagement des personnes ordinaires que celle de leur influence dans sa création et dans leur vécu. Elle vient s'opposer à l'idée que les citoyens ne seraient que des « générateurs de données », permettant passivement son fonctionnement⁴.
- 4 Pour mieux comprendre ce dont il est question, il nous faut revenir sur les difficultés de définition de la *Smart city* (A), qui sous-tendent une implication disparate et ambiguë des citoyens (B).

A. D'une technicisation de la ville à l'émergence du « Smart citizen »

- 5 Les difficultés de définition de la *Smart city* sont liées d'une part, à l'hétérogénéité des initiatives mises en œuvre depuis une vingtaine d'années et d'autre part, à la nébulosité du terme, décrit comme un « signifiant flottant qui peut changer de référent chaque fois que nécessaire [et qui] offre un espace flexible et dynamique dans lequel il est possible d'insérer une variété de produits, de pratiques et de politiques⁵ ». Ces référents

sont multiples puisqu'à la prédominance originelle de conceptions « technocentrées⁶ » s'opposent ou se conjuguent désormais des visions mettant en avant l'importance du capital humain dans l'idée que « la technologie ne suffit pas ».

- 6 Théoriquement, l'approche centrée sur la technologie repose sur la présomption selon laquelle les nouvelles technologies de l'information et de la communication permettent automatiquement une ville plus prospère et mieux maîtrisée. Toute transformation technologique est dès lors perçue comme une innovation⁷. Une telle présomption généralement provient d'abord d'acteurs privés, initiateurs ou promoteurs de projets *Smart city*, et est, ensuite, exacerbée par les autorités locales qui utilisent le terme « *Smart city* » comme un label pour valoriser un développement qu'elles affirment durable. Le problème est qu'en répondant aux intérêts propres des uns et des autres, cette mise en avant des bienfaits d'une hyper-technisation de l'espace urbain tend à favoriser un discours d'apparente neutralité qui masque les choix idéologiques qu'elle recouvre. Une telle approche laisse finalement peu de place aux citoyens dès lors que ce qui importe avant tout est le recueil des données qu'ils produisent. *A contrario*, l'approche centrée sur l'humain renvoie à la critique d'un imaginaire représentant la ville vidée de sa substance. Cet imaginaire ne tiendrait compte ni des répercussions des pratiques numériques sur les habitants, ni du fait que ces derniers participent à la fabrique collective de la ville. Condamnant ainsi une « orientation trop technocratique et descendante », cette approche oppose « des formes de gouvernance algorithmique »⁸ à la figure du « *Smart citizen*⁹ ». Une telle optique se retrouve dans la définition donnée par le *Comité européen des régions*, dans un avis du 5 février 2020 :

« Une ville intelligente est un endroit où les réseaux et services traditionnels sont rendus plus efficaces grâce à l'utilisation de la technologie numérique et des technologies de télécommunication au profit des citoyens et des entreprises [...]. Les villes intelligentes doivent associer leurs citoyens à leur démarche, afin qu'ils puissent participer activement à la création de leur habitat local, et que l'initiative humaine, soutenue et étayée par les TIC, ainsi qu'une offre de services de proximité adaptés aux citoyens, peuvent permettre de trouver et d'appliquer des solutions intelligentes et des idées collectives qui améliorent les villes et renforcent leur durabilité [...] »¹⁰.

- 7 Pratiquement, l'opposition nette entre ces deux approches s'efface devant les objectifs affichés des autorités locales. A cet égard, l'exemple du projet de la métropole dijonnaise est intéressant. S'appuyant sur des indicateurs de performance et des objectifs chiffrés, Dijon Métropole entend rendre plus efficace les services municipaux (régulation et facilitation des déplacements urbains, collecte des déchets, nettoyage de la voirie...) et permettre une meilleure gestion des ressources urbaines (optimisation des consommations d'énergie et d'eau, surveillance de la qualité de l'air...). Cela se matérialise par « l'unification fonctionnelle des services urbains¹¹ ». Les équipements urbains sont désormais connectés et gérés à distance depuis un poste de commandement unique et les données continuellement recueillies proviennent de l'ensemble des capteurs installés par la collectivité. Au cœur de ce projet, la participation citoyenne est encouragée par la création d'outils numériques permettant aux citoyens de signaler, en temps réel et de manière géolocalisée, tout problème survenant sur la voirie publique, y compris des incivilités et des infractions délictuelles et criminelles¹². Les infrastructures connectées et l'utilisation de données ainsi captées doivent donc permettre d'offrir des services adaptés aux besoins et aux attentes des habitants/citoyens. En parallèle, leur implication doit permettre d'ajuster continuellement ces services pour les rendre plus attractifs et performants. L'objectif

affiché étant l'amélioration de leur qualité de vie, les habitants sont ainsi considérés comme placés au cœur de ce dispositif qui promeut leur participation volontaire. Or, bien que le système repose, en partie, sur la « coproduction de données¹³ », il n'est pas certain que l'expression citoyenne soit tout à fait volontaire, ni même tout à fait consciente.

B. D'un difficile traitement des informations à la marginalisation de l'action citoyenne

- 8 En premier lieu, on peut se demander si les habitants/citoyens ont réellement conscience du fait que leur ville est engagée dans un mouvement de transformation et que ces changements vont avoir des répercussions importantes sur la manière dont ils s'approprient l'espace public. Très souvent, les articles de presse ou de revues spécialisées mettent en avant le fait que les citoyens ne savent pas réellement ce qu'est une *Smart city*. Ils n'auraient pas suffisamment de connaissances pour réellement appréhender la manière dont les nouvelles technologies fonctionnent, leurs usages et leurs implications profondes en termes de droits et libertés¹⁴. A cet égard, on peut se demander si les citoyens ont une connaissance des régimes juridiques, au demeurant sectoriels, appréhendant le respect de la vie privée, la protection des données personnelles, etc. On peut même se poser la question de savoir, au regard de leur complexité et de leurs mutations permanentes, s'il est réellement possible de maîtriser les usages technologiques qu'induit le développement d'une *Smart city*. D'une manière plus globale, on s'aperçoit que des difficultés semblables peuvent survenir pour les autorités publiques, encourageant la recherche auprès des tiers, en particulier des consultants externes et plus particulièrement du secteur privé, pour organiser la mise en place d'une *Smart city* - ce qui augmente d'autant le risque d'exclusion des citoyens ordinaires, la *Smart city* devenant une affaire de spécialistes « qui savent ».
- 9 Il se pose ensuite la question du traitement des informations par les citoyens. Ces derniers étant encouragés à participer à la surveillance continue des mouvements de la ville, ont-ils la même perception des dysfonctionnements ou incivilités qu'ils seraient amenés à signaler ? Cette question appelle à avoir une définition commune et claire de ces termes. Pour le dictionnaire Larousse¹⁵, la « civilité », c'est « l'observation des convenances en usage chez les gens qui vivent en société ; politesse, courtoisie ». Si cette définition est considérée comme vieillie par le Larousse lui-même, elle montre que la définition des incivilités est bien difficile, sujette à caution, variable suivant l'âge, la culture des personnes concernées, etc. En effet, si le terme « incivilité » est souvent employé dans les médias pour dénoncer des manquements aux règles du comportement en société, qui resteraient à définir (par qui ? selon quels principes juridiques ?), ces manquements sont par nature très diversifiés (insultes dans la vie quotidienne, atteintes à la décence, nuisances sonores, dégradations de biens publics, etc.) et dépendants de qui les observe. Ils peuvent relever « tout à la fois de comportements perturbateurs qui ne sont pas sanctionnés pénalement et de faits qui constituent des délits¹⁶ » - d'autant que le ressenti d'insécurité des populations peut être très similaire pour un fait pénalement répréhensible que pour un fait qui ne le serait pas. La difficulté est alors de s'accorder sur le contenu des incivilités et sur la manière d'y répondre. A cela, s'ajoute le fait que les acteurs institutionnels, en fonction de leurs champs de compétences, peuvent en avoir une vision tout à fait différente,

selon que l'aspect « prévention » ou l'aspect « répression » domine. Il en est de même pour le terme « dysfonctionnement » qui s'apprécie *a contrario* du « fonctionnement normal ». Or, ce « fonctionnement normal » peut avoir plusieurs sens : l'usuel, ce qui respecte la norme sociale, mais aussi ce qui respecte la norme juridique, etc. Dans la pratique, le problème est le suivant : Ou bien, comme on le dit « nul n'est censé ignorer la loi » et chaque citoyen est capable de parvenir à opérer un tri efficace pour ne signaler que ce qui contreviendrait à la loi ou porterait atteinte à l'ordre public. Ou bien le citoyen ordinaire, n'étant pas juriste de profession, ne connaît pas parfaitement la loi : il risque bien d'encombrer le système par des signalements involontairement inappropriés, qui choquent son propre système de valeurs mais ne sont pas contraires au droit. Tout cela, sans compter la possibilité de dénonciation abusive ou de signalements délibérément malveillants¹⁷. Se pose également la question de 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 tel qu'il est institué à l'article 226-10 du Code de pénal ? Une telle possibilité d'action en justice ne risque-t-elle pas en retour de paralyser toute action citoyenne ?

- 10 A la prise en compte et au traitement de l'information vient s'ajouter la question du degré de participation des citoyens au sein des projets *Smart city*. Quelles que soient les innovations en matière d'applications dédiées, la participation citoyenne semble circonscrite à la seule interface prévue dans l'application ad hoc sur *Smartphone*. Dès lors que les citoyens ne participent ni aux processus décisionnels en tant que tels, ni à la pensée de nouvelles formes d'urbanité, elle apparaît alors bien plus comme un moyen de mieux cibler les interventions des autorités publiques que comme la mise en place d'une nouvelle forme de gouvernance véritablement collaborative. L'analyse des significations composites du terme « *Smart citizen* » témoigne d'une possible permanence des relations verticales et asymétriques entre autorités publiques et citoyens¹⁸. En effet, la marginalisation des capacités d'action du citoyen se produit lorsque son rôle est restreint à celui d'utilisateur ou de consommateur. Dans le premier cas, l'utilisateur est principalement considéré comme un « point de données », c'est-à-dire qu'il est encouragé à fournir des informations relatives à des stratégies de surveillance de l'espace urbain ou de protection de l'environnement, sans « capital politique pour agir »¹⁹. Dans le second cas, en tant que consommateur, le citoyen est invité à utiliser les produits numériques et les services associés mais dans un cadre limité par le choix déjà établi en amont par les fournisseurs de service. Quoi qu'il en soit, dans les deux cas, la participation citoyenne, qu'elle soit passive (surveillance d'une caméra intelligente) ou active (usage de l'application *Smartphone* mise en place pour tel ou tel service), semble se limiter *in fine* à la réception et à la production de données indispensables au bon fonctionnement de la *Smart city*. C'est donc une participation instrumentalisée, qui n'a pour finalité que de permettre au système de fonctionner, sans pour autant agir directement sur sa conception et les enjeux du vivre-ensemble qu'il sous-tend. Par contraste, Kitchin et Cardullo appellent à « une redistribution du pouvoir de ceux qui sont traditionnellement aux commandes vers les citoyens, ce qui permet aux communautés de négocier et de s'engager dans des compromis avec des parties prenantes établies et puissantes, telles que les administrations municipales²⁰ ». Opportunément, un tel partenariat permet également

de garantir l'adhésion des citoyens aux objectifs visés puisqu'ils résulteraient d'une réflexion collective.

- 11 En dernier lieu, la mise en avant d'une participation volontaire, voire même consciente des citoyens, pose la question de leur consentement éclairé. A cet égard, le Comité de la prospective de la CNIL pointe du doigt le manque d'informations claires dont disposent les individus pour consentir au traitement de leurs données à caractère personnel, qualifiant les mécanismes d'information et de consentement « vides de sens ou absents », dès lors que le « volume et la diversité des données collectées rend très compliqué le contrôle de leurs données par les individus, même pour les plus proactifs : lire et comprendre les conditions générales d'utilisation de chacun des services serait trop compliqué et chronophage²¹ ». Le risque est donc que les individus ne sachent pas vraiment ce quoi ils consentent, ni même ce qu'un tel consentement implique dans l'utilisation qui est faite de leurs données présentement ou dans l'avenir. La CNIL s'interroge également sur les risques liés à l'utilisation de capteurs « passifs » qui proviendraient des *Smartphones* des habitants ou des touristes. Elle se demande ainsi : « Ne suis-je pas le seul à pouvoir décider que le *Smartphone* que j'ai acquis soit utilisé, gratuitement et parfois à mon insu pour optimiser des flux ? Puis-je ainsi refuser de « donner mes données au collectif ? Où placer la limite de la notion d'intérêt général dans ce domaine²² ? ». Le problème est similaire à celui du « wifi tracking » dans lequel la captation des données à l'insu des citoyens pose, d'une manière corollaire, la question de la protection des données personnelles recueillies. Il est donc intéressant de se référer à la décision du Conseil d'État du 8 février 2017 confirmant la décision de refus opposée par la CNIL à la société JC Decaux de collecter l'adresse MAC des téléphones mobiles grâce à des boîtiers de comptage wifi installés sur les mobiliers publicitaires dans le quartier de La Défense à Paris²³. Après avoir rappelé qu'il « demeure possible d'individualiser une personne ou de relier entre elles des données résultant de deux enregistrements qui la concernent », le Conseil d'État avait donc considéré que le traitement litigieux « qui a pour objet d'identifier les déplacements des personnes et leur répétition sur la dalle piétonne de La Défense, pendant toute la durée de l'expérience » était bien un traitement de données à caractère personnel dès lors qu'il n'avait pas pour effet de rendre suffisamment anonymes les données pour que la personne concernée ne soit plus identifiable. Si dans le cas présent, la société requérante n'avait pas, contrairement à ce qu'elle avançait, procédé à une anonymisation des données, l'effectivité même de l'anonymisation peut être critiquée²⁴. Cette affaire fait également écho au débat concernant l'application Stop-Covid²⁵ et la confrontation « données centralisées » (position défendue par la France) contre « données décentralisées ».
- 12 L'ensemble de ces quelques observations témoigne de la complexité de la problématique de la participation citoyenne et pose un certain nombre de questions. Quelle forme peut prendre le consentement pour quelles données collectées ? Les garanties qu'offre la législation actuelle sont-elles suffisantes pour garantir un tel consentement ? De manière plus générale, est-ce que le simple fait de se promener en ville (et donc de passer près d'un capteur) vaut consentement ? Est-il possible de refuser de consentir à la captation de données personnelles et quelles sont les implications concrètes pour les citoyens réfractaires ou non connectés ? On peut également se demander si la protection de la vie privée et des données personnelles doit se limiter à la problématique du consentement. La réponse est évidemment non,

puisque se pose la question du traitement ultérieur de ces données, de leur croisement avec des données issues d'autres bases de données, etc.

II. Le citoyen face aux ambiguïtés du RGPD

- 13 La CNIL, lorsqu'elle s'interroge, à juste titre, sur les incertitudes et les possibles déviations liées à l'installation de l'ensemble des technologies précitées, interpelle les autorités étatiques sur la nécessité « produire de nouvelles formes de régulation de la donnée, dans le respect des individus et de leurs libertés²⁶ ». A cet égard, le Règlement Général sur la Protection des Données (RGPD) établit un cadre juridique contrasté : si les garanties quant à l'expression du consentement sont renforcées, la portée de la protection des données à caractère personnel est à relativiser (A). L'exemple de la surveillance par drones est révélateur non seulement du caractère ambivalent d'un consentement librement donné mais également des insécurités juridiques, à l'échelle interne, quant à la protection des données personnelles (B).

A. Les faiblesses d'une nouvelle approche du consentement à l'aune de la Smart city

- 14 Le RGPD a été adopté en 2016 et est entré en vigueur le 1^{er} mai 2018. Il identifie clairement les risques liés à la captation et au traitement des données personnelles²⁷, en mettant l'accent sur la sécurité des données, et consacre le principe d'*accountability* des responsables de traitement des données personnelles. A cet égard, l'article 5 alinéa 1 énonce les grands principes que doivent respecter les traitements de données : traitement des données à caractère personnel de manière licite, loyale et transparente au regard de la personne concernée ; une collecte à des fins déterminées, explicites et légitimes ; minimisation de la quantité de données collectées ; exactitude ; limitation de la conservation ; intégrité et confidentialité. En outre, et c'est là que réside certainement la plus grande innovation, l'alinéa 2 de l'article 5 dispose que « le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté ». Il ne s'agit donc pas seulement de respecter les principes énoncés mais d'être en mesure de démontrer qu'ils sont respectés- la responsabilité du responsable du traitement pouvant dès lors être engagée s'il ne parvient pas à assumer la charge de la preuve.
- 15 Toutefois, l'ambiguïté du RGPD réside dans la notion même de consentement des individus qui est défini comme « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement »²⁸. Cette notion de consentement, pourtant au cœur du droit à la vie privée, apparaît *in fine* biaisée dès lors que l'article 6 du RGDP semble opérer « une évolution radicale dans le cadre de la licéité du traitement de données. Jusqu'alors le consentement était le principe essentiel de tout traitement de données personnelles, il devient aujourd'hui l'exception »²⁹. Pourquoi cela ? Car, hors les cas pour lesquels le consentement doit être recueilli *préalablement* (notamment, en matière de « données sensibles ») énoncés à l'article 9 du RGDP, cet article 6 instaure un double régime de traitement des données personnelles : un traitement avec consentement et un traitement sans consentement.

- 16 Si les conditions attachées à l'obtention du consentement ont été renforcées, le consentement n'est qu'une des bases légales prévues par le RGPD en matière de licéité de traitement. En effet, cet article autorise une mise en œuvre de traitements de données à caractère personnel dès lors qu'au moins l'une des conditions suivantes est respectée :
- 17 La personne a consenti au traitement ou le traitement est nécessaire à l'exécution d'un contrat ;
- 18 Le traitement est nécessaire afin de respecter une obligation légale à laquelle le responsable du traitement est soumis ;
- 19 Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
- 20 Le traitement est nécessaire pour l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique ; et enfin,
- 21 Le traitement est nécessaire pour la poursuite d'intérêts légitimes par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.
- 22 En outre, bien qu'il soit expressément indiqué que l'intérêt légitime ne peut être avancé, sauf cas particuliers³⁰ par les autorités publiques dans l'exécution de leurs missions, se pose, néanmoins, la question de sa définition. La CNIL, dans la fiche explicative de ce qu'est un intérêt légitime, n'y apporte pas de réponse, en se bornant à indiquer une méthodologie à appliquer :
- « (i) identification du caractère « légitime » de l'intérêt poursuivi par le responsable du traitement et vérification du caractère « nécessaire » du traitement au vu de cet objectif ; (ii) évaluation des atteintes aux intérêts et droits et libertés des personnes et prise en compte de leurs attentes raisonnables ; (iii) mise en balance de ces éléments et, le cas échéant, prévision de mesures additionnelles³¹ ».
- 23 Le considérant 47 du RGPD n'y apporte également pas de définition, en se limitant à un exemple de ce que pourrait être un intérêt légitime : « dans des situations telles que celles où la personne concernée est un client du responsable du traitement ou est à son service ». Ce considérant précise ensuite que c'est au responsable de traitement de venir justifier lui-même l'existence d'un tel intérêt légitime, en déterminant notamment qu'une « personne concernée peut raisonnablement s'attendre, au moment et dans le cadre de la collecte des données à caractère personnel, à ce que celles-ci fassent l'objet d'un traitement à une fin donnée ». Or, comme le souligne Frédérique Boulanger, « la justification tendant au développement durable et à l'écologie peut être légitime cependant qu'en est-il des traitements de données visant au confort des urbains ? Comment apprécier ce qui permet leur confort ou non³² ? ». A quoi peut-on raisonnablement s'attendre dans le cadre d'un projet « *Smart city* » ? La question est ouverte, d'autant qu'un tel projet ne repose pas uniquement dans les mains des autorités publiques mais concerne un ensemble d'acteurs privés participant à la production de données (entreprises de la sécurité, applications mobiles de suivi...). On peut aussi se demander s'il n'est-il pas problématique de laisser le responsable de traitement déterminer lui-même cet intérêt légitime.
- 24 Par ailleurs, la notion d'*intérêt public* retenue – qui n'est pas la notion d'*intérêt général* au fondement du droit public et justifiant l'existence de régime exorbitant du droit

commun³³ – apparaît difficilement saisissable. Aucune définition précise de ce qui constitue ou non une mission d'intérêt public n'est donnée et la CNIL ne présente que des exemples : « Cette base légale concerne donc en premier lieu les traitements mis en œuvre par les autorités publiques [...] [elle] peut en particulier fonder les traitements tournés vers les usagers de l'autorité publique concernée³⁴ ».

- 25 S'agissant du consentement en tant que tel, les critères de sa validité posent un certain nombre de difficultés lorsqu'ils sont appliqués à un projet « *Smart city* ». En effet, l'article 7 du RGPD dispose non seulement que « le responsable du traitement doit être en mesure de démontrer que la personne concernée a donné son consentement » mais également que la demande de consentement doit être présentée « sous une forme qui la distingue clairement », « compréhensible et aisément accessible, formulée en des termes clairs et simples ». Or, l'ensemble de ces éléments ne sont pas aisément identifiables au regard de la diversité des données collectées, de leur provenance et de leur croisement potentiel. Outre l'imperméabilité des catégories de données³⁵ entre elles, le problème est double. Il concerne d'une part, les risques d'une ré-identification des individus à partir de données agrégées et anonymisées, et d'autre part, la réduction des individus à des données, personnelles ou non, aux fins d'une performance mise en avant sans que l'on sache bien à quoi elle se réfère précisément.
- 26 En outre, comment garantir le caractère éclairé du consentement dès lors que le croisement de données augmente le risque d'une dilution des traitements et des finalités poursuivies et qu'il ne sera pas toujours aisé d'identifier l'identité du responsable de traitement et ces finalités ? Une telle complication est exacerbée par la difficulté de connaître à l'avance les traitements secondaires des données. Les inquiétudes de la CNIL, mentionnées précédemment, témoignent, d'une manière plus générale, des difficultés à satisfaire à la condition d'un consentement éclairé au regard de la complexité d'exercice du droit à l'information. L'opacité d'une collecte massive de données et leur croisement s'oppose à la transparence de l'information, qui doit également être compréhensible et aisément accessible. A cet égard, conformément à l'article 13 du RGPD, la personne concernée doit, au moment où les données sont obtenues, être informée, notamment, de l'identité du responsable de traitement, de la finalité du traitement auquel sont destinées les données à caractère personnel, ou encore des destinataires des données. De plus, l'une des difficultés majeures sera de parvenir à « tracer » les données collectées et utilisées dès lors qu'une personne concernée demandera à exercer ses droits (droit d'accès, droit de rectification, droit à l'effacement, droit à la limitation du traitement, droit d'opposition, droit à la portabilité). Le caractère « librement donné » du consentement interroge également, d'autant que le considérant n° 42 du RGPD vient préciser que le « consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice ». Or, comment définir cette liberté de choix dès lors que l'ensemble du paysage urbain et des espaces publics sont verrouillés par des capteurs recueillant continuellement des données³⁶ ? Cela pose également la question de savoir s'il est même possible de refuser la captation de ces données.

B. La place contestée du consentement à l'aune de la surveillance par drones

- 27 L'usage des drones à des fins de surveillance témoigne des réticences politiques à instituer un cadre juridique véritablement protecteur des droits et libertés, ce qui interpelle, à la lumière d'une légitimation sécuritaire, quant à la place du citoyen dans la « smartification » des villes. Tout d'abord, il est intéressant de mentionner le référé déposé le 4 mai 2020 devant le Tribunal administratif de Paris par la Quadrature et La Ligue des Droits de l'Homme visant à faire cesser le déploiement des drones de la préfecture de Police de Paris en vue de faire respecter les mesures de confinement. Outre l'atteinte au principe de proportionnalité, ces deux associations considèrent que la mobilité des drones porte atteinte au droit au respect de la vie privée en captant des images relevant d'espaces privés et ce « pour un nombre virtuellement infini de finalités, légitimes ou non », d'autant que les citoyens n'ont aucun moyen de donner leur consentement en violation donc des dispositions du RGPD et de la loi de 1978 modifiée³⁷. Le juge des référés du Tribunal administratif de Paris, dans une ordonnance du 5 mai 2020³⁸, a rejeté leur recours au motif que l'ensemble des protocoles mis en place dans la captation des images ne permet pas l'identification d'un individu au sol. En ce sens, le juge considère que :

« Dans ces conditions, même si la préfecture de police a, par ce dispositif, procédé à la collecte, à l'enregistrement provisoire et à la transmission d'images, elle ne peut être regardée comme ayant procédé à un traitement de données à caractère personnel, au sens des dispositions précitées du règlement (UE) 2016/679, de la directive (UE) 2016/680 et de la loi du 6 janvier 1978 [...]. Il n'y a donc pas d'atteinte illégale aux libertés fondamentales que sont le droit à la vie privée et le droit à la protection des données personnelles ».

- 28 Le juge des référés se fonde sur l'article 4 du RGPD qui vient définir la notion de « données à caractère personnel » comme « toute information se rapportant à une personne physique identifiée ou identifiable [...] » pour en déduire que « dans la mesure où l'usage dans un cadre de police administrative n'autorise pas à identifier des individus mais seulement à prévenir des troubles à l'ordre public, la présence d'un traitement de données aurait été en soi écartée »³⁹. Ce raisonnement est critiquable en ce qu'il repose sur les engagements de la Préfecture de Police⁴⁰ et non sur des facteurs objectifs tel que le préconise le RGPD. En effet, le juge des référés ne cherche pas à déterminer si, en fonction de « l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement » (considérant n° 26), les caractéristiques techniques des drones permettent, effectivement ou non, d'identifier les personnes concernées. Ceci apporte donc un élément de réponse quant à la possibilité de refuser la captation de données dans la rue. Toutefois, en appel, se conformant à l'analyse technique requise, le juge des référés du Conseil d'État écarte ce raisonnement et soutient que les données susceptibles d'être collectées par le traitement litigieux doivent bien être regardées comme revêtant un caractère personnel. Il explicite ainsi qu'il :

« ... résulte de l'instruction que les appareils en cause qui sont dotés d'un zoom optique et qui peuvent voler à une distance inférieure à celle fixée par la note du 14 mai 2020 sont susceptibles de collecter des données identifiantes et ne comportent aucun dispositif technique de nature à éviter, dans tous les cas, que les informations collectées puissent conduire, au bénéfice d'un autre usage que celui actuellement

pratiqué, à rendre les personnes auxquelles elles se rapportent identifiables » (Considérant 16).

- 29 Le Conseil d'État considère ainsi que ce ne sont pas tant les caractéristiques propres aux drones qui importent, que l'absence d'une barrière technique qui préviendrait toute collecte et tout enregistrement d'images permettant l'identification des personnes filmées si elles étaient utilisées pour un autre usage que celui pratiqué. Autrement dit, c'est l'absence d'une garantie technique qu'une captation de données identifiantes serait effectivement neutralisée qui implique la qualification de traitement de données à caractère personnel. Peu importe que la Préfecture de police ait, dans sa doctrine d'emploi, annoncé une absence d'enregistrement des images captées ou n'autorise pas les drones à se rapprocher des personnes. Le juge des référés réfute également l'argument selon lequel « le visionnage en temps réel des personnes filmées fait en tout état de cause obstacle à ce qu'elles puissent être identifiées » (considérant 16). Dès lors qu'il s'agit d'un traitement des données à caractère personnel pour le compte de l'État, le juge des référés constate l'obligation de conformer à l'article 31 de la loi Informatique et Libertés n° 78-17 du 6 janvier 1978 modifiée qui impose un encadrement réglementaire, après avis motivé et publié de la CNIL. Constatant l'absence d'une telle réglementation, il en conclut que :

« Compte tenu des risques d'un usage contraire aux règles de protection des données personnelles qu'elle comporte, la mise en œuvre, pour le compte de l'État, de ce traitement de données à caractère personnel sans l'intervention préalable d'un texte réglementaire en autorisant la création et en fixant les modalités d'utilisation devant obligatoirement être respectées ainsi que les garanties dont il doit être entouré caractérise une atteinte grave et manifestement illégale au droit au respect de la vie privée » (Considérant 18).

- 30 Le Conseil d'État reprendra cette logique dans une décision du 22 décembre 2020⁴¹ à propos de la surveillance par drones des rassemblements de personnes, en soutenant que :

« Dès lors que les images collectées par les appareils sont susceptibles de comporter des données identifiantes, la circonstance que seules les données traitées par le logiciel de floutage parviennent au centre de commandement n'est pas de nature à modifier la nature des données faisant l'objet du traitement, qui doivent être regardées comme des données à caractère personnel » (Considérant 7).

- 31 En refusant de considérer que la seule présence d'un dispositif de floutage après collecte d'images captées par drones suffise à les disqualifier comme traitement de données à caractère personnel, le Conseil d'État établit clairement qu'à défaut de cadre légal⁴², la surveillance par drones ne peut être réalisée sans la présence d'un dispositif technique de nature à rendre impossible l'identification des personnes filmées. Cette position du Conseil d'État sera suivie par la CNIL⁴³.
- 32 Afin de pallier le vide juridique, la proposition de loi n° 3452 relative à la sécurité globale a créé un régime juridique visant à « autoriser les services de l'État concourant à la sécurité intérieure et à la défense nationale et les forces de sécurité civile à filmer par voie aérienne pour des finalités précises ». La proposition de loi disposait ainsi que les images pouvaient être transmises en temps réel au poste de commandement du service concerné, sans que ne puissent toutefois être visualisées les « images de l'intérieur des domiciles ni, de façon spécifique, celles de leurs entrées ». Une liste, exhaustive mais d'ampleur considérable, indiquait l'ensemble des finalités d'un traitement de données.

- 33 Ces dispositions ont été censurées par le Conseil constitutionnel⁴⁴. Mettant en garde contre le caractère particulièrement intrusif d'une surveillance par drones, eu égard aux potentialités d'une captation d'images très importantes de personnes, en tout lieu - sans que leur présence ne soit détectée - et dans un vaste périmètre, le Conseil considère que le régime juridique ainsi institué n'est pas suffisamment assorti de garanties particulières de nature à sauvegarder le droit au respect de la vie privée. D'une part, d'un point de vue technique, le caractère potentiellement indétectable des drones implique une captation sans que les personnes concernées n'en soient informées, allant ainsi à l'encontre des dispositions du RGPD. D'autre part, le recours aux drones est insuffisamment circonscrit, notamment en matière de police administrative, et ce d'autant que l'autorisation délivrée par l'autorité administrative compétente n'était assortie d'aucune « limite maximale, exceptée la durée de six mois lorsque cette autorisation est délivrée à la police municipale, ni aucune limite au périmètre dans lequel la surveillance peut être mise en œuvre ». Il en est de même pour l'autorisation donnée à la police municipale d'user de ces drones pour « assurer l'exécution de tout arrêté de police du maire, quelle que soit la nature de l'obligation ou de l'interdiction qu'il édicte, et de constater les contraventions à ces arrêtés ».
- 34 Ainsi, le Conseil constitutionnel, s'il ne s'oppose pas en tant que tel à la surveillance par drones et même la légitime en reconnaissant qu'elle répond « aux objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions », conclut à l'inconstitutionnalité desdites dispositions, dès lors que « le législateur n'a pas assuré une conciliation équilibrée entre les objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions et le droit au respect de la vie privée ». Néanmoins, à la suite de cette censure, le gouvernement a déposé un nouveau projet de loi relatif à la responsabilité pénale et à la sécurité intérieure réintroduisant un cadre juridique, supposément plus strict, pour l'usage de la surveillance par drones. Adopté en première lecture par l'Assemblée nationale le 23 septembre 2021, ce projet de loi est vivement critiqué par la Défenseure des Droits, notamment en ce que l'autorisation de surveillance est confiée aux seules autorités préfectorales, sans contrôle par une autorité indépendante du pouvoir exécutif, ni préalablement à l'octroi d'une telle autorisation, ni *a posteriori* pour son renouvellement. En outre, aucun recueil de consentement des personnes filmées n'est prévu ; seule une information serait garantie⁴⁵, sauf « quand les circonstances l'interdisent ou que cette information rentrerait en contradiction avec les objectifs poursuivis. Or, l'on peut se demander ce que signifie exactement l'expression « quand les circonstances l'interdisent » car, contrairement aux caméras fixes, les mouvements perpétuels des drones rendent, techniquement, l'information difficile d'accès.
- 35 La surveillance par drones catalyse ainsi les risques de déviance, en violation du principe de protection des données et du respect de la vie privée, et les craintes qu'induit l'usage de ces nouvelles technologies par les autorités publiques⁴⁶. A cet égard, la CNIL pointe également du doigt l'avènement d'une vision préventive⁴⁷ de la sécurité. Cette vision préventive serait couplée à l'utilisation de technologies de sécurité intelligentes devant aider les opérateurs, à partir des données collectées et suivant un algorithme, d'une part à identifier automatiquement des comportements suspects, et d'autre part à prédire des tendances ou évolutions du système. Or, non seulement ces modèles prédictifs peuvent véhiculer des informations qui pourraient se

révéler « fausses⁴⁸ » mais il est également à craindre que leur usage influence le comportement et les opinions des habitants, dévoyant alors leur participation tout en « renforçant les préjugés et en stigmatisant certains segments de la population⁴⁹ ». L'ensemble de ces craintes font apparaître un décalage important entre la figure d'un citoyen surveillé dans le but de maintenir l'ordre public et celle d'un citoyen, acteur de la *Smart city* et co-décisionnaire. Ce décalage est d'autant plus problématique que les desseins politiques ainsi affichés se confrontent à la perte de contrôle des autorités publiques sur les données, liée à l'intensification du volume des données collectées et à l'opacité précédemment mentionnées.

Conclusion

- 36 Nos observations confirment le caractère particulièrement ambigu de la participation citoyenne au sein des projets *Smart city*, d'autant que la difficile protection des données à caractère personnel et le caractère précaire du consentement se conjuguent au souhait des politiques de mettre en place une surveillance accrue des mouvements de la ville. Les droits et libertés des citoyens peuvent en être affectés, comme en témoignent les atteintes au respect de la vie privée qu'implique l'usage non encadré des drones. Il en est de même, bien que non mentionnée par le Conseil constitutionnel, de la liberté d'expression des citoyens. Le risque de telles atteintes est accentué par la collecte massive et continue de données qu'induit le développement d'un projet « *Smart city* », particulièrement à l'égard de l'information et du consentement des citoyens qui ne doivent pas être vidés de toute substance, intentionnellement par un cadre juridique biaisé ou en raison des problèmes induits par l'usage même d'une technologie mal maîtrisée (opacité à propos du fait que des données sont engendrées et sur la finalité de celles-ci, réutilisation des données à d'autres fins auxquelles elles sont destinées, inférence...). Si la participation citoyenne ne peut se résumer au consentement, elle est rendue d'autant plus compliquée que l'obtention d'un consentement librement donné, préalable et éclairé est entravée par les difficultés qu'ont les citoyens à connaître ce à quoi ils acquiescent. Et toute démarche volontariste vient se confronter à la logique instituée par le RGPD : soit le responsable de traitement se fonde sur l'une des bases légales permettant de passer outre le consentement ; soit le fait de donner son consentement, quand son obtention est obligatoire pour le responsable de traitement, est pratiquement automatique. Ou plus précisément, les contours d'un refus de consentir au traitement de données à caractère personnel ne sont pas clairs, comme c'est le cas dans l'espace public.

NOTES

1. Voir, par exemple, Ayyoob SHARIFI, Amir Reza KHAVARIAN-GARMIR, Rama Krishna REDDY KUMMITHA, 2021, « Contributions of Smart City Solutions and Technologies to Resilience against the COVID-19 Pandemic: A Literature Review », *Sustainability*, vol. 13, n° 8018, doi.org/10.3390/su13148018.

2. Daniel VENTURA, « Coronavirus et 'suivi de localisation' : le Comité européen de la protection des données en première ligne », *Dalloz Actualité*, 10 avril 2020, <https://www.dalloz-actualite.fr>.
3. Pierre ANDRE, avec la collaboration de P., MARTIN et G., LANMAFANKPOTIN, « Participation citoyenne », In CÔTE, L., SAVARD, J.-F (dir.), *Le Dictionnaire encyclopédique de l'administration publique*, 2012, www.dictionnaire.enap.ca
4. Catherine NGUYEN, Hélène BLEUS, Jonas VAN BOCKHAVEN, *Le Guide pratique de la Smart city – Tome 2*, Smart city Institute, 2018, pp. 18-21.
5. Jathan SADOWSKI, Franck A., PASQUALE, « The Spectrum of Control: A social theory of the smart city », *First Monday*, vol. 20, n° 7, 2015, <https://firstmonday.org/article/view/5903/4660>.
6. A cet égard, plusieurs modèles se dessinent : la « ville internet » qui a la particularité d'être entièrement planifiée et pilotée par des algorithmes et l'internet des objets ; la ville « fluide » qui, à l'image de Singapour, repose sur une plate-forme gouvernementale de données ouvertes visant à moderniser et optimiser l'ensemble des services publics, tout en reposant sur l'idée d'une influence réciproque entre le pouvoir central et la collectivisation des comportements citoyens ; ou encore la ville « adaptative », à l'image des projets français qui repose sur la transformation des « acteurs traditionnels des métiers de l'urbain. In Jean-François SOUPIZET, « La smart city : mythe et réalité », *Futuribles*, vol. 1, n° 434, 2020, pp. 49-65.
7. Voir, par exemple, les analyses d'Antoine PICON, « L'avènement de la ville intelligente », *Sociétés*, vol. 2, n° 132, 2016, pp. 9-24 ; de Vito ALBINO et al., « Smart Cities : Definitions, Dimensions, Performance and Initiative », *Journal of Urban Technology*, vol. 22, n° 1, 2015, pp. 3-21 et de Michel LUSSAULT, « L'allégorie de la Smart city », *Tous urbains*, vol. 3, n° 23, 2018, pp. 14-16.
8. Rob KITCHIN, Paolo CARDULLO, « Being a 'citizen' in the smart city: Up and down the scaffold of smart citizen participation », *GeoJournal*, vol. 84, n° 1, 2019, pp. 1-13.
9. Pour une analyse critique de l'ambiguïté du terme « Smart citizen », voir, par exemple Albert VANOLO, « Smartmentality: the Smart City as Disciplinary Strategy », *Urban Studies*, vol. 51, n° 5, 2014, pp. 883-898; Jennifer GABRYS, « Programming Environments: Environmentality and Citizen Sensing in the Smart City », *Environment and Planning D: Society and Space*, vol. 32, n° 1, 2014, pp. 30-48.
10. COMITÉ EUROPÉEN DES RÉGIONS, *Avis du Comité européen des régions – Villes intelligentes : de nouveaux défis pour une transition équitable vers la neutralité climatique – Comment mettre en œuvre les ODD dans la vraie vie ?*, 5 février 2020, 20202/C39/17).
11. DIJON MÉTROPOLE, Just Dijon, OnDijon, *Dijon métropole met en service un projet inédit de Smart city en France*, Dossier de presse, 11 avril 2019, 20 p.
12. Nous discuterons plus loin du concept d'« incivilité ».
13. Mathieu VIDAL, « Quels habitants et usagers de la ville intelligente ? Éléments de prospective », In Emmanuel EVENO, Jean-Jacques GUIBBERT (dir.), « Villes intelligentes 'par le bas'. Entre chercheurs, experts et acteurs associatifs », *Les Cahiers des Ateliers de dialogue Recherche-Action-Expertise (ADIRAE)*, n° 5, 2016, p. 42.
14. Voir, par exemple, Viktor WEBER, *Smart cities must pay more attention to the people who live in them*, World Economic Forum, 16 avril 2019, <https://www.weforum.org/agenda/2019/04/why-smart-cities-should-listen-to-residents/>; Emilie SCOTT, *The trouble with informed consent in Smart cities*, International Association of Privacy Professionals, 28 février 2019, <https://iapp.org/news/a/the-trouble-with-informed-consent-in-smart-cities/>.
15. LAROUSSE, « Civilité », <https://www.larousse.fr/>.
16. Éric MAUREL, « Infractions pénales et incivilités. Une réponse diversifiée », *Les Cahiers dynamiques*, vol. 4, n° 53, 2011, p. 28.
17. De la Saint Barthélémy à l'Occupation, en passant par la Révolution Française, l'histoire regorge de cas de dénonciations malveillantes, souvent entre voisins.

18. Rob KITCHIN, Paolo CARDULLO, « Being a 'citizen' in the smart city: Up and down the scaffold of smart citizen participation », *GeoJournal*, *op.cit.*
19. *Ibid.*, p. 8.
20. Kitchin et Cardullo prennent l'exemple de Barcelone qui a « donc cherché à re-politiser la ville intelligente et à déplacer sa création et son contrôle des intérêts privés et de l'État vers la base, les mouvements civiques et l'innovation sociale ». *Ibid.*, p. 14.
21. CNIL, « La plateforme d'une ville. Les données personnelles au cœur de la fabrique de la smart city », *Cahiers IP Innovation & Prospective*, n° 5, 2017, p. 14.
22. *Ibid.*, p. 25.
23. CE, 10^{ème}-9^{ème} chambres réunies, 8 février 2017, n° 393714. Voir, à ce propos, Philippe MOURON, « La protection des données personnelles dans l'environnement urbain – De la mesure d'audience publicitaires aux villes intelligentes », *Revue Lamy Droit de l'Immatériel*, n° 129, 2017, pp. 54-60.
24. CNIL, *L'anonymisation des données, un traitement clé pour l'open data*, 2019, <https://www.cnil.fr/en/node/114427>.
25. L'échec relatif de cette application tient en partie à la crainte de la centralisation des données – l'effet « *Big brother* » si bien décrit par Georges Orwell (Orwell, 1949).
26. CNIL, « La plateforme d'une ville. Les données personnelles au cœur de la fabrique de la smart city », *op.cit.*, p. 49.
27. Voir le Considérant n° 75 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
28. Article 4 du RGPD.
29. Clémence CODRON, *La surveillance diffuse : entre Droit et Norme*, Thèse de doctorat de Droit, Université du Droit et de la Santé – Lille II, 2018, 571 p.
30. CNIL, *La mission d'intérêt public : dans quel cas fonder un traitement sur cette base légale*, 2019, <https://www.cnil.fr/fr/la-mission-dinteret-public-dans-quels-cas-fonder-un-traitement-sur-cette-base-legale>.
31. CNIL, *L'intérêt légitime : comment fonder un traitement sur cette base légale*, 2019, <https://www.cnil.fr/fr/les-bases-legales/interet-legitime..>
32. Frédérique BOULANGER, « La difficile protection des données personnelles au sein de la smart city », *IREDIC*, 6 décembre 2017, <http://www.iredic.fr/2017/12/06/la-difficile-protection-des-donnees-personnelles-au-sein-de-la-smart-city/>.
33. Nous pouvons souligner que la notion même d'intérêt général est difficilement définissable, le Conseil d'État se référant à la « *capacité des individus à transcender leurs appartenances et leurs intérêts pour exercer la suprême liberté de former ensemble une société politique* », Conseil d'État, *Réflexions sur l'intérêt général - Rapport public 1999*, Étude annuelle, <https://www.conseil-etat.fr/ressources/etudes-publications/rapports-etudes/etudes-annuelles/reflexions-sur-l-interet-general-rapport-public-1999>.
34. CNIL, *La mission d'intérêt public : dans quel cas fonder un traitement sur cette base légale*, *op.cit.*
35. Voir à ce propos l'analyse de Liesbet Van Zoonen qui identifie deux grands types de collecte, eux-mêmes divisés en deux, en fonction de la perception des individus sur ces données : la collecte de données personnelles à des fins de service et à des fins de surveillance et la collecte de données impersonnelles à des fins de service et à des fins de surveillance. In Liesbet VAN ZOONEN, « Privacy concerns in smart cities », *Government Information Quarterly*, vol. 33, n° 33, 2016, pp. 472-480.
36. Dans sa thèse, Clémence CODRON prend l'exemple des applications mobiles : « *Certaines applications mobiles, spécialement des jeux, demandent à accéder à la fois au répertoire téléphonique, à*

l'appareil photo, aux coordonnées de localisation, aux données techniques (réseau de télécommunication et wifi), alors même que certaines de ces fonctionnalités n'ont clairement pas d'effet dans le cadre de cette application. Si l'utilisateur refuse l'accès à ces données, l'usage de ces applications est impossible. Le consentement librement donné réside-t-il alors dans le choix d'utiliser et/ou dans le choix de ne pas utiliser cette application ? ». In Clémence CODRON, *La surveillance diffuse : entre Droit et Norme*, op. cit., p. 318.

37. Marc REES, « Confinement : les droits de la préfecture de police de Paris attaqué en justice », *NextInpact*, 4 mai 2020, <https://www.nextinpact.com/>.

38. TA Paris, ord., 5 mai 2020, n° 20006861/9.

39. Bastien LE QUERREC, « Le Conseil d'État ouvre l'espace aux drones », *RDLF*, n° 81, 2020, <http://www.revuedlf.com/droit-administratif/le-conseil-detat-ouvre-lespace-aux-drones-ce-ord-18-mai-2020-association-la-quadrature-du-net-et-ligue-des-droits-de-lhomme-n440442-n440445/>.

40. Pour appuyer sa décision, le juge des référés soutient ainsi que « *S'il résulte de ce qui a été dit au point précédent que, lorsqu'ils sont utilisés dans un cadre judiciaire, les appareils sont capables d'identifier les individus, il n'est pas non plus établi ni soutenu que les appareils auraient été utilisés dans un tel cadre, depuis le début du confinement* » - la Préfecture de police de Paris assumant le fait d'identifier un individu dans ce cadre judiciaire « *que ce soit en flagrance, en préliminaire ou au titre d'une instruction* », précisant toutefois que « *dès la fin de la mission, les images sont supprimées de la carte mémoire. Elles ne font l'objet d'aucun recoupement avec des fichiers de police* ».

41. Conseil d'État, 10^{ème} – 9^{ème} chambres réunies, 22/12/2020, n° 446155.

42. A noter que le Conseil d'État, sollicité au titre de ses fonctions consultatives par le Premier ministre au sujet de l'usage de dispositifs aéroportés de captation d'images par les autorités publiques a rendu le 20 septembre 2020 un avis explicitant clairement que cette captation relève non plus du pouvoir réglementaire mais bien des « *matières réservées au législateur par l'article 34 de la Constitution, celui-ci pouvant seul, en fixant les éléments principaux, définir les conditions permettant d'assurer la conciliation entre le respect de la vie privée et la sauvegarde de l'ordre public, comme il l'a fait pour la vidéoprotection et les caméras individuelles. Le Conseil d'État estime donc qu'il est nécessaire de fixer un cadre législatif d'utilisation des caméras aéroportées par les forces de sécurité et les services de secours* ». Dans CE, « Avis relatif à l'usage de dispositifs aéroportés de captation d'images par les autorités publiques », 20 septembre 2020, n° 401214.

43. CNIL, *Délibération de la formation restreinte n° SAN-2021-003 du 12 janvier 2021 concernant le ministère de l'intérieur*.

44. CC, Décision n° 2021-87 DC du 20 mai 2021 – Loi pour une sécurité globale préservant les libertés.

45. DEFENSEUR DES DROITS, *Avis du Défenseur des droits n° 21-12, 2021*.

46. Voir, à ce propos, le numéro très complet de Sciences et Actions sociales (2019) : *Normes, déviations et nouvelles technologies : entre régulation, protection et contrôle*.

47. GICAT, *Safe city*, Rapport réalisé par le GICAT et la FIEEC, en liaison avec le CoFIS, 2017, 41 p.

48. Ce risque fait écho au célèbre film hollywoodien *Minority Report* (tiré du roman de Philip K. Dick) dans lequel un système centralisé est censé détecter les crimes avant qu'ils ne soient commis, le héros joué par Tom Cruise, pourtant chargé d'arrêter ces futurs criminels, étant lui-même victime du système. Voir, également, à propos de la gestion de la crise sanitaire : Benoit DUPONT, « Covid-19 : les dérives possibles de surveillance des données personnelles », *The Conversation*, 29 mai 2020, <https://theconversation.com/covid-19-les-derives-possibles-de-surveillance-des-donnees-personnelles-139443> ; David LYON, « The coronavirus pandemic highlights the need for a surveillance debate beyond 'privacy' », *The Conversation*, 24 mai 2020, <https://theconversation.com/the-coronavirus-pandemic-highlights-the-need-for-a-surveillance-debate-beyond-privacy-137060>.

49. Rob KITCHIN, « Getting smarter about smart cities: Improving data privacy and data security », Data Protection Unit, Department of the Taoiseach, Dublin, 28 janvier 2016, 82 p. In

Regis CHATELLIER, « Smart privacy dans la smart city », CNIL, *Cahiers IP Innovation & Prospective*, op.cit., pp. 13-14.

RÉSUMÉS

Si la définition même des *Smart cities* est relativement complexe, l'ambition première apparaît relativement clairement : une plus grande efficacité d'intervention des services municipaux dans la gestion de l'espace public (régulation et facilitation des déplacements urbains, collecte des déchets, nettoyage de la voirie...) et une administration simplifiée visant à faciliter la vie quotidienne des usagers et une meilleure gestion des ressources urbaines (optimisation des consommations d'énergie et d'eau, surveillance de la qualité de l'air...). L'amélioration de la qualité de vie des habitants/citoyens au sein des *Smart cities* conduit à ce que leur participation soit mise en avant par leurs promoteurs. Les citoyens sont considérés comme étant au cœur du dispositif en tant que bénéficiaires et usagers des infrastructures et services publics optimisés par de nouvelles technologies. Ils le sont également en tant qu'acteurs participant pleinement à la modernisation de l'action publique et à la production subséquente de données. C'est ainsi moins la figure unique d'un *Big Brother* qui est promue que celle de leur participation volontaire, qu'elle soit véritablement consciente ou non. Or, cette dimension participative n'est pas sans ambiguïté et interroge l'efficacité du régime juridique de protection de la vie privée, des données personnelles recueillies et du droit à un consentement libre et éclairé.

Although the very definition of Smart cities is relatively complex, the primary ambition is relatively clear: greater efficiency of municipal services in the management of public space (regulation and facilitation of urban travel, waste collection, street cleaning, etc.) and simplified administration aimed at facilitating the daily life of users. There is also a better management of urban resources (optimization of energy and water consumption, air quality monitoring, etc.). The improvement of the quality of life of the inhabitants/citizens within Smart cities leads to their participation being put forward by their promoters. Citizens are considered to be at the heart of the system as beneficiaries and users of infrastructures and public services optimized by new technologies. They are also considered as actors fully participating in the modernization of public action and in the subsequent production of data. It is thus less the unique figure of a "Big Brother" that is promoted than that of their voluntary participation, whether it is truly conscious or not. However, this participatory dimension is not without ambiguity and questions the efficiency of the legal regime of protection of privacy, of the personal data collected and of the right to free and informed consent.

INDEX

Mots-clés : smart city, participation citoyenne, RGPD, consentement, protection des données personnelles

Keywords : smart city, citizen participation, RGPD, consent, personal data protection

AUTEUR

ADÈLE DE MESNARD

Adèle de Mesnard est Docteure en droit de l'Université Jean Moulin Lyon 3, Chercheur associée à l'Institut de Droit de l'Environnement (CNRS - UMR 5600 - EVS - IDE).