European Review of Digital Administration & Law - Erdal
2021, Volume 2, Issue 1, pp. 171-187
ISSN 2724-5969 - ISBN 979-12-5994-243-2 - DOI 9791259942432 13

*Le consentement au traitement des données personnelles à l'épreuve de la smart city**

Léonore Cellier
(Ph.D. Student at the University of Lausanne)

Solange Ghernaouti
(Professor at the University of Lausanne)

ABSTRACT So-called smart cities are insidiously developing in our societies. This raises many questions about data protection, particularly when data collection and processing should be based on the consent of the data subject. Therefore, how can a person could freely consent to the processing of his or her data captured by all sorts of connected devices of the smart city (IoT, video surveillance cameras, means of transport, payments, etc.) which are indispensable and have replaced all the means that have prevailed until now? This is particularly the case when the citizen has no other choice than to take public transport or a public road and to submit to the use of information technologies and their suppliers. Is the information given to users is sufficient and relevant? Through the analysis of the consequences of low visibility of data processing, the challenges of the imposed use of technology and the question of the identity of the data processor, this contribution aims to question the possibility of data processing based on the informed consent of individuals in the context of the smart city.

1. *Introduction*

La mise en place de villes intelligentes conduit à une captation des données sur le domaine public et à leur exploitation par le privé sans même que l'individu en ait conscience et encore moins qu'il y ait donné son accord. Si a priori le consentement tel que prévu par le Règlement Général de Protection des Données personnelles (RGPD)[1] semble constituer une garantie à l'information et à la libre volonté de la personne à l'utilisation de ses données pour la ville connectée, l'automatisation et la généralisation des services numériques reflètent en réalité l'absence de consultation du citoyen. La mise en place de ces villes risque de réduire l'autonomie et la liberté des individus et interroge sur la possibilité et la valeur du consentement. Après avoir identifié et décrit les principales caractéristiques du concept de ville intelligente, cet article analyse les conditions de l'expression d'un consentement licite au regard des éléments structurels d'un traitement de données personnelles propre aux villes intelligentes.

2. *Contexte de la ville intelligente et du traitement des données personnelles*

Trois facteurs centraux permettent de qualifier une ville intelligente : la technologie, l'institutionnel et l'humain[2]. Elle vise à une utilisation accrue et intégrée des nouvelles technologies de l'information dans tous les champs d'activité de la ville contribuant à l'optimisation des performances ainsi que du partage et de l'usage des ressources, à la rationalité économique, tout en autorisant l'amélioration supposée de la qualité de vie des citoyens ou encore la fluidité des déplacements par exemple.

Elle se compose d'applications avec des réseaux de capteurs qui analysent l'environnement afin de suivre en continu les actions, d'y réagir et de prendre des décisions dans un temps compatible avec la réalité des évènements et des besoins[3]. L'infrastructure numérique de la ville intelligente, se compose notamment :

- De sources d'informations (usagers) ;
- De capteurs de données des usagers (téléphone, caméra de vidéosurveillance,

* Article submitted to double-blind peer review.

[1] 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 (RGPD).

[2] T. Nam et T. A. Prado, *Conceptualizing Smart City with Dimensions of Technology, People, and Institutions*, dans *The Proceedings of the 12th Annual International Conference on Digital Government Research*, 2011, 286.

[3] D. Cliche, P. Turmel, et S. Roche, *Les enjeux éthiques de la ville intelligente : données massives, géolocalisation et gouvernance municipal*, dans *Ethica*, vol. 20, n. 1, 2016, 223-248, notamment 227.

lecteur de plaque d'immatriculation, objets connectés, QR Code…) ; De réseaux de transmission et de télécommunication (Wi-Fi, Bluetooth, Internet, 4G, 5G...) ;
- D'une infrastructure de traitement des données (stockage (*cloud*), traitements, intelligence artificielle (*big data analytics…*) ;
- Des services (déplacements, visites, loisirs, commerces, administrations) ;
- Des utilisateurs (citoyens, administrateurs...).

Dans le contexte d'une ville intelligente, les traitements de données personnelles trouvent leur fondement dans diverses sources issues de l'art. 6 RGPD (contrat, loi, intérêt public ou intérêt légitime). La condition qui intéresse cette étude est le consentement car s'il est strictement encadré par le RGPD, des abus peuvent facilement en découler. Si pour certains fournisseurs de service, le consentement est le motif le plus global, et le plus susceptible de susciter la confiance des utilisateurs, il est tout de même nécessaire de contrôler le respect de la licéité des traitements de données notamment sensibles pour lequel, le caractère explicite du consentement est requis[4] au regard des dérives et des abus qui peuvent en résulter de manière insidieuse. Le consentement constitue en effet, une condition « fourre-tout » de traitements injustifiables par un « vrai », « solide » motif légal comme la loi ou le contrat. Dans les faits, les traitements basés sur ce motif ne provoquent pas une attention particulière de la part des usagers. Il est donc profitable aux fournisseurs de services de l'employer puisqu'il repose sur la seule responsabilité de l'individu à lire, comprendre et accepter ou non les conditions proposées alors qu'il est intégré dans un système où le temps presse.

Par sa structure même, son déploiement et les services essentiels concernés, la ville intelligente, ne semble pas offrir la possibilité pour un consentement significatif et éclairé du citoyen au traitement de ses données personnelles[5]. De grandes quantités d'informations sont souvent recueillies à son insu et analysées en continue faisant appel au paradigme informatique de traitement massif de données (*Big Data, Big data analytics*). Les domaines d'utilisation des technologies sont variés et concernent en particulier les transports, l'énergie, la communication, la surveillance et la sécurité publique ou encore la gestion de la ville[6]. Il s'agit de services essentiels et indispensables à la vie courante des individus. Cependant, si l'ensemble des avis, émotions, faits et gestes physiques des citoyens sont captés, analysés et numérisés pour rendre une ville plus « performante » il convient de se demander si le citoyen est en capacité de connaitre et de choisir les modalités du traitement de ses données personnelles. Le consentement est-il à ce titre une condition de traitement réellement efficace ? Quels facteurs dans la structure de la ville numérisée défient sa validité ?

3. *Au sujet du consentement aux traitements de données personnelles de la ville intelligente*

Le consentement 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[7]. Il doit en outre être donné pour des finalités spécifiques[8], et est donc valable le temps de l'accomplissement de ces finalités. Lorsque le traitement a plusieurs finalités, le consentement devrait être donné pour l'ensemble d'entre elles[9]. Le consentement peut être retiré à tout moment et il devrait être aussi simple de retirer que de donner son consentement[10]. Le responsable du traitement est censé être capable d'apporter la preuve du consentement[11].

Certains types de traitements propres à la structure de la ville intelligente ne trouvent une justification que dans le consentement. Le Groupe de Travail 29 (G29)[12], préconisait l'invocation principale du consentement pour

[4] L. Edwards, *Privacy, security and data protection in smart cities: a critical EU law perspective*, dans *CREATe Working Paper*, 2015/11, 1, notamment 31.
[5] L. Edwards, *Privacy, security and data protection in smart cities*, 1.
[6] D. Cliche, P. Turmel, et S. Roche, *Les enjeux éthiques de la ville intelligente*, 228.
[7] Art. 4 ch. 11 RGPD.
[8] Art. 6 al. 1 let. a RGPD.
[9] Considérant 32 RGPD.
[10] Art. 7 al. 2 RGPD.
[11] Art. 7 al. 1 RGPD.
[12] Groupe de Travail « Article 29 » sur la Protection des Données (G29), est le groupe de travail européen indépendant qui traitait les questions relatives à la protection de la vie privée et aux données à caractère personnel jusqu'au 25 mai 2018 (avant l'entrée en vigueur du Règlement Général sur la Protection des Données - RGPD) : https://edpb.europa.eu/our-work-tools/article-29-working-party_fr

fonder un traitement de données dans le contexte de l'Internet des objets, peu importe la nature du responsable de traitement (fabricants de dispositifs, plateformes sociales ou de données, prêteurs de dispositifs ou développeurs tiers)[13]. Le Comité Européen de la Protection des Données (EDPB)[14], le recommande également pour les assistants vocaux virtuels, dans la mesure où les responsables de traitement doivent informer les personnes concernées de tout traitement ultérieur, c'est la base la plus adéquate au moment du stockage des données, mais aussi pour une réutilisation postérieure[15]. Cette prescription s'étend à la ville intelligente, étant donné que les traitements de données prévus sont principalement basés sur des objets connectés dans le domaine public[16]. Même dans le cas où un traitement de données serait strictement nécessaire à l'exécution d'un contrat ou des intérêts légitimes du responsable du traitement, le consentement servira nécessairement de motif de licéité à toute fin autre que l'exécution de la demande d'une personne concernée[17]. Dans le cadre du traitement massif de données d'une ville intelligente, il y a tout lieu de prescrire une utilisation unique du consentement, au regard des finalités multiples déterminées au fur à mesure des ambitions commerciales et de la possibilité d'accepter ou non chacune d'entre elles. Cela permettrait en effet, un système où chaque individu paramètre selon sa volonté les usages qu'il souhaite pour ses données personnelles, respectant ainsi au mieux le principe d'autodétermination informationnelle.

À l'égard des capteurs automatiques de données, les responsables de traitement devraient utiliser les données des utilisateurs non enregistrés dans le système comme ayant donné leur consentement uniquement pour exécuter leurs demandes spécifiques[18], aucun stockage ni quelconque traitement ne devrait avoir lieu sans consentement. Dans la mesure où les dispositifs de traitements de données disposés dans une smart city font un usage accru de profilage à des fins publicitaires, le consentement devrait toujours être recueilli. Cette finalité n'étant en effet jamais considérée comme un service explicitement demandé par l'utilisateur final[19]. Lorsque par ailleurs l'objet connecté de la ville intelligente captera et traitera des données biométriques en vue d'un profilage, il s'agira d'un traitement de données sensibles soumis aux conditions de l'art. 9 RGPD qui nécessitera donc le consentement explicite de la personne concernée[20]. Les responsables de traitement devront alors prévoir une alternative au traitement de données biométriques afin de se conformer à l'art 7 et au considérant 32 RGPD notamment eu égard au caractère libre du consentement[21]. Pour les traitements par vidéo dont les villes intelligentes ont vocation à massivement se doter, le consentement sera utilisé à titre relativement exceptionnel, notamment lorsqu'il s'agit de surveillance systématique puisqu'elle vise un nombre indéterminé de personnes[22]. Le responsable du traitement n'est en effet pas en mesure de prouver qu'une personne déterminée a donné son consentement préalable au traitement[23]. Par ailleurs en cas de retrait du consentement, il est difficile de démontrer que les données personnelles ne sont plus traitées[24].

À l'aide des dernières lignes directrices de l'Union européenne relatives aux technologies dont recèlent et recèleront les villes connectées telles que la reconnaissance faciale, les véhicules autonomes connectés et applications de mobilité, les assistants vocaux virtuels et les dispositifs vidéo, voire des drones, cette étude a vocation à observer la possibilité d'un traitement licite basé sur le consentement dans le cadre d'une ville intelligente. Il s'agit de s'assurer que le citoyen soit suffisamment informé pour être véritablement éclairé au moment du consentement : il doit être parfaitement

[13] G29, *Opinion 8/2014 on the on Recent Developments on the Internet of Things (WP 223)* Adopté le 16 Septembre 2014, 15.
[14] Le Comité Européen de la Protection des Données (EDPB) est un organe européen indépendant qui contribue à l'application cohérente des règles en matière de protection des données au sein de l'Union européenne et encourage la coopération entre autorités de l'UE chargées de la protection des données. Il est institué par le RGPD : https://edpb.europa.eu/about-edpb/about-edpb_fr
[15] EDPB, *Guidelines 02/2021 on Virtual Voice Assistants*, Version 1.0, Adopted on 9 March 2021, §27, 11.
[16] L. Edwards, *Privacy, security and data protection in smart cities*, 18-19.
[17] EDPB, *Virtual Voice Assistants*, §29, 12.
[18] EDPB, *Virtual Voice Assistants*, §29, 12.
[19] EDPB, *Virtual Voice Assistants*, §88, 23.
[20] EDPB, *Virtual Voice Assistants*, §128, 30.
[21] EDPB, *Virtual Voice Assistants*, §128, 30.
[22] EDPB, *Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo,* adoptées le 29 janvier 2020, version 2.0., 9.
[23] EDPB, *Dispositifs vidéo*, 14.
[24] EDPB, *Dispositifs vidéo*, 14.

conscient de l'usage qui est fait des données personnelles et son choix doit être scrupuleusement respecté par les entreprises[25] : il doit être entièrement libre de sa décision. Cependant si dans une ville intelligente le traitement de données est peu visible, l'usage de la technologie inéluctable et le statut du responsable du traitement équivoque, quelle place reste-t-il au consentement libre et éclairé ?

4. *Analyse des problématiques*

4.1. *La faible visibilité, l'invisibilité du traitement*

Dans une ville intelligente, l'ensemble des services sont connectés à des applications et des capteurs qui traitent des données personnelles en temps réel. L'individu est la source des informations qui nourrit la ville numérique. Ce dernier, s'il n'est pas suffisamment averti et éduqué à la protection des données, peut ne pas en avoir conscience. Le confort offert par la ville connectée et l'accès à de nombreux services risquent de primer sur le questionnement lié au contrôle de ses données personnelles qu'il offre gratuitement[26]. L'individu est-il informé de son rôle ? En a-t-il conscience ? Est-il libre de choisir ou non d'être une source d'informations ? Quels sont alors les facteurs de l'opacité du traitement et quelles conséquences emportent-ils sur la licéité du consentement ?

4.1.1. *La convergence du physique et du numérique*

Le premier facteur qui rend invisible le traitement est que dans une ville intelligente, les domaines physiques et numériques sont indistincts. L'utilisateur peut ne pas avoir connaissance du traitement des données effectué par des objets spécifiques tels que les montres intelligentes qui ne sont pas visibles : la plupart ne distinguent pas forcément une montre normale d'une montre connectée, alors qu'elle intègre des caméras, des microphones et des capteurs de mouvement, voire des paramètres physiologiques, qui peuvent transférer des données, qui seront stockées et exploitées, sans qu'elles en soient conscientes, et encore moins sans qu'elles consentent réellement à un tel traitement[27].

D'ordinaire, le consommateur qui navigue sur le Web ou qui installe un objet connecté dans sa maison est en mesure de lire la politique de confidentialité, de choisir s'il y adhère et donc de consentir librement à l'utilisation du service. En revanche, lorsque l'individu verra ses données collectées par une « route intelligente », un tramway ou un « bus intelligent » qu'il sera contraint d'emprunter ou par une poubelle connectée dans laquelle il jettera ses déchets, cette possibilité s'amoindrie[28].

L'utilisateur devrait se voir proposer la possibilité de consentir ou non au stockage de ses données dans ce type d'équipement après avoir reçu des informations claires et complètes sur les finalités du traitement. Il devrait connaître au moins l'identité du responsable du traitement et les finalités du traitement auxquelles sont destinées les données à caractère personnel[29] ainsi que les (types de) données collectées et utilisées, l'existence du droit de retirer son consentement, des informations concernant l'utilisation des données pour la prise de décision automatisée conformément et des informations sur les risques éventuels liés à la transmission des données en raison de l'absence de décision d'adéquation et de garanties appropriées telles que décrites à l'article 46 du RGPD[30].

Si sur Internet, il est relativement aisé de fournir cette information, il est à ce jour difficile de déterminer dans quelle mesure ces exigences légales peuvent s'appliquer aux données collectées à partir de capteurs de différentes sortes dans le « monde réel »[31]. Ce manque d'information constitue un obstacle important à la démonstration d'un consentement valable, car la personne concernée doit être informée[32]. La route connectée devrait-elle être prévoir à son entrée

[25] J.-M. Cheffert, *Respect de la vie privée : quand les approches économique et juridique se rejoignent*, dans C. de Terwangne, E. Degrave, et S. Dusollier (eds.), *Laws, norms and freedoms in cyberspace – Liber Amicorum Yves Poullet*, Bruxelles, Larcier, 2018, 505, notemment 518.

[26] L. Rigollier, *Des données dans la ville : quelles intelligences pour la smart city ? Vers une « culture des données » au sein des collectivités ?*, Master thesis, Ecole d'urbanisme de Paris, Paris, 2016, 48.

[27] G29, WP 233, 7.

[28] L. Edwards, *Privacy, security and data protection in smart cities*, 17.

[29] Considérant 42 RGPD.

[30] EDPB, WP259 rev.01, §64, 14.

[31] L. Edwards, *Privacy, security and data protection in smart cities*,18-19.

[32] G29, WP 233, 7.

une information complète et un formulaire de consentement à remplir éventuellement à son péage ? L'EDPB dénonce le risque qu'un utilisateur ne soit pas même conscient du traitement des données effectué dans son véhicule et recommande de ne pas fonder le traitement sur le consentement dans un tel cas puisque la structure du système fait obstacle à la démonstration d'un consentement éclairé[33].

De même, le consentement doit être librement donné, en ce sens que la personne concernée doit disposer d'une véritable liberté de choix ou être en mesure de refuser ou de retirer son consentement sans subir de préjudice[34]. En outre, lorsque le consentement n'a pas été obtenu, le responsable du traitement devrait rendre les données anonymes avant de les réutiliser ou de les partager avec d'autres parties[35]. Si dans le monde numérique il est (normalement) aisé de renoncer à l'activation des *cookies*, dans le monde physique il en va tout autrement. Comment alors garantir que le conducteur qui refuse que l'équipement Bluetooth de sa voiture soit détectable par l'ensemble des capteurs routiers ait effectivement la possibilité de circuler sans être traqué ?

À première vue, dans de tels systèmes, les garanties conventionnelles du consentement de la législation européenne sur les données personnelles, fonctionneront difficilement comme des garanties pour la vie privée des consommateurs[36]. Cela est d'autant plus vrai que ces systèmes opaques sont automatisés. Cela soulève la question de l'identification du traitement des données par l'informatique portable, qui pourrait être résolue en envisageant une signalisation appropriée qui serait réellement visible par les personnes concernées[37].

4.1.2. *L'injonction du temps réel*

La personne concernée a besoin d'accéder au service de manière instantanée, même si elle est consciente du risque présenté par l'acceptation du traitement, ses conséquences pourraient advenir dans le futur, elle se contraint donc à accepter[38]. Ce dernier, mêlé au volume d'informations, empêche la personne concernée de consentir de manière éclairée et libre. Un individu qui doit se déplacer et qui décide d'entrer sur une route connectée ou de prendre un bus connecté pour se rendre sur son lieu de travail est généralement contraint par le temps et par le fait qu'il n'a pas d'itinéraire alternatif valable. Ainsi, il n'accorde pas forcément d'énergie et de temps à la lecture des informations, à leur compréhension quant à l'usage et au traitement de ses données personnelles.

4.1.3. *Des traitements automatisés indiscernables*

Deux types traitements de données peuvent être distingués : celui où les données sont produites de manière volontaire pour une finalité déterminée par exemple si la personne utilise l'application « *fix my street* » et envoie des informations sur l'état de la ville dans un but de gestion ou le cas de données enregistrées passivement dans le cadre d'un service annexe, par exemple avec une localisation de l'individu à travers un outil cartographique ou d'un navigateur web[39]. Les données sont dans les deux cas à disposition du responsable du traitement mais dans le premier cas la personne concernée aura sciemment et de son propre chef envoyé des informations précises alors que dans le deuxième, la personne concernée pourrait ne pas avoir conscience d'avoir produit une telle information qui pourra être réutilisée à foison. Dans ce deuxième exemple, il s'agit d'un abandon de données par la personne plutôt que d'une cession, en ce sens qu'elles sont plus laissées que transmises mais n'apparaissent pas pour autant comme des données volées[40].

Dans la ville intelligente, l'ensemble des traitements envisagés sont tellement intégrés

[33] EPDB, *Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications* adoptees le 9 mars 2021, version 2.0, §50, 14.
[34] Considérant 42 RGPD.
[35] G29, WP 233, 21.
[36] L. Edwards, *Privacy, security and data protection in smart cities*,17.
[37] G29, WP 233, 7.
[38] R. Neisse, G. Baldini, G. Steri, Y. Miyake, S. Kiyomoto, et A. R. Biswas, *An Agent-based Framework for Informed Consent in the Internet of Thing*, in *IEEE 2nd World Forum on Internet of Things (WF-IoT)*, Milan, 2015, doi: 10.1109/WF-IoT.2015.7389154, 789-792, notemment 789.
[39] M. Saujot et T. Erard, *Les innovations de la ville intelligente au secours de la ville durable ? Décryptage à partir des enjeux de données*, dans *Working Papers*, n. 2/15, Paris, Iddri, 2015, 7.
[40] A. Rouvroy et T. Berns, « *Gouvernementalité algorithmique et perspectives d'émancipation » Le disparate comme condition d'individuation par la relation ?*, dans *Réseaux*, 2013/1, n. 177, DOI : 10.3917/res.177.0163, 163-196, notamment 169.

qu'ils deviennent invisibles. Ils sont instantanés et permanents si bien qu'ils sont indiscernables. Pourtant, un consentement passif n'est pas valable, il ne doit pas être présumé par l'inaction[41].

Avec la captation de données par des caméras, un consentement valable est encore plus difficile à mettre en œuvre. Le responsable de traitement devrait s'assurer que chaque personne concernée pénétrant dans la zone surveillée a donné son consentement, mais le seul fait de pénétrer dans ladite zone ne suffit pas à caractériser une déclaration ou un acte positif clair de volonté[42]. Il en va ainsi également pour les véhicules connectés. En effet, si le consentement du conducteur principal est obtenu lors de l'achat et de la mise en activité du véhicule, il en va différemment pour le conducteur occasionnel ou passager, le consentement parait difficile à obtenir lorsqu'il s'agit d'un véhicule d'occasion, loué ou emprunté[43] notamment du fait de la passivité du traitement. Cette problématique s'étend aux voitures partagées en libre-service, qui tendent à se développer de plus en plus dans ce modèle de ville.

Si des données biométriques sont traitées à des fins d'identification, le responsable du traitement doit veiller à ce que chaque modèle intermédiaire réalisé à la volée avant d'obtenir un résultat de concordance soit supprimé[44]. Les modèles créent pour être enregistrés ne doivent être conservés que pour atteindre une finalité spécifique et ne devraient ni être stockés ni archivés[45].

Dans le cas où le système de surveillance avait vocation à créer de la publicité ciblée, le responsable du traitement devrait obtenir le consentement préalable de toutes les personnes concernées. Ce système serait illicite s'il filmait des passants sans leur consentement[46]. Le comité européen dénonce l'installation de ces systèmes dans des zones non contrôlées et rappelle que le consentement explicite des personnes devrait toujours être requis s'agissant de traitement dont la finalité est l'identification de personnes[47].

4.1.4. *Utilisation postérieure des données personnelles*

À l'ère du *Big Data*, la plupart des utilisations secondaires innovantes n'ont pas été imaginées au moment où les données sont collectées pour la première fois. Le maximum de données est récolté et conservé par défaut[48], la personne concernée n'a souvent pas conscience qu'un traitement de données personnelles la concernant a lieu car les données personnelles qu'elle a pu confier à un moment T sont réutilisées a posteriori sans qu'elle en soit informée. La structure du *Big Data* fait que les données sont collectées en masse sans être forcément exploitées dans l'instant mais elles sont conservées pour des usages ultérieurs. La valeur de la donnée n'est pas apparente au moment de la collecte et au moment où la personne concernée donne son consentement[49]. Elles sont quelconques et dispersées[50]. Les services étant souvent structurés par une utilisation future et non anticipée de la donnée personnelle[51].

Cette caractéristique de la collecte de données personnelles est contraire aux art. 5 al. let. b et 6 RGPD qui exigent que le consentement soit donné pour des finalités déterminées, explicites et légitimes. En effet, les données sont déliées de toute connaissance véritable des finalités recherchées par la collecte, c'est-à-dire des usages auxquels elles donneront lieu une fois corrélées à d'autres données[52]. Pourtant, l'EDPB préconise que le responsable du traitement demande pour chaque nouvelle finalité, un nouveau consentement et offre la possibilité aux personnes concernées d'en refuser certaines[53].

[41] E. Politou, E. Alepis, et C. Patsakis, *Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions*, dans *Journal of Cybersecurity*, vol. 4, Issue 1, 2018, 1–20, notemment 7.
[42] EDPB, *Dispositifs vidéo*, §46, 14.
[43] EPDB, *Connected vehicles*, 14.
[44] EDPB, *Dispositifs vidéo*, §78, 19.
[45] EDPB, *Dispositifs vidéo*, §78, 19.
[46] EDPB, *Dispositifs vidéo* 20.
[47] EDPB, *Dispositifs vidéo*, 20.
[48] A. Rouvroy et T. Berns, *« Gouvernementalité algorith-mique et perspectives d'émancipation » Le disparate comme condition d'individuation par la relation ?*, 69.
[49] E. Politou, E. Alepis et C. Patsakis, *Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions*, 5.
[50] A. Rouvroy et T. Berns, *« Gouvernementalité algorith-mique et perspectives d'émancipation » Le disparate comme condition d'individuation par la relation ?*, 169.
[51] E. Politou, E. Alepis et C. Patsakis, *Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions*, 5.
[52] A. Rouvroy et T. Berns, *« Gouvernementalité algorith-mique et perspectives d'émancipation » Le disparate comme condition d'individuation par la relation ?*, 169.
[53] EDPB, *Connected vehicles*, §53, 14.

Le consentement initial ne légitimera jamais un traitement ultérieur, car le consentement doit être informé et spécifique pour être valide[54]. Cela donne lieu à une évacuation ou au minimum à un voilement de toute finalité, et à une minorisation de l'implication du sujet, et donc du consentement pouvant être donné à cette communication d'informations : toute forme d'intentionnalité semble donc se mouvoir[55].

Afin de compenser cette lacune, la planification à l'avance de l'ensemble des finalités futures et réutilisation possibles et probables est une solution mais elle entre en contradiction avec le mode de développement de l'économie numérique et des applications du *Big Data* et de l'intelligence artificielle. En effet, le responsable de traitement ne sait pas à l'avance quelles données l'intéresseront. De même, la personne concernée ne sait pas dans le futur quelles informations elle acceptera de délivrer et pour quelle finalité. Par ailleurs cette solution risque de mener à l'acceptation de finalités trop générales comme c'est le cas avec Facebook par exemple qui, lors de l'inscription sur le réseau, prévoit l'utilisation postérieure de données personnelles à des finalités de recherche. Or, ni la personne concernée, ni Facebook ne sait par avance quelles recherches spécifiques seront menées. Le consentement ne peut donc être éclairé. Une autre solution serait de donner un nouveau consentement à chaque réutilisation mais cela semble bien trop complexe et onéreux pour le responsable du traitement[56]. Quant à la possibilité de fonder le traitement sur l'intérêt légitime du responsable du traitement, cela paraît intéressant si le modèle économique de la donnée est accepté. L'exploitation des informations des individus pour faire marcher les affaires de chaque entreprise devrait alors être considérée comme un besoin. Les individus devraient sciemment accepter de livrer leur vie privée pour prétendre à un service gratuit. Néanmoins, cette possibilité fait risquer des abus notables avec une opacité accrue compte tenu des difficultés de contrôle et de la délégation au responsable du traitement de la tâche de trouver l'équilibre entre intérêts commerciaux et droits fondamentaux[57].

4.1.5. *Captation de toutes les données personnelles, quid des personnes non-consentantes ?*

Les personnes consentantes peuvent-elles fournir des données qui affectent ensuite les personnes non-consentantes ? Tout objet manipulateur d'émotions ou d'opinions générales ne devrait-il pas être interdit ? Même en refusant de participer aux systèmes les données sont captées et les comportements sont orientés par des algorithmes. Les traitements de données dans une smart city ont lieu de manière passive et généralisée, c'est-à-dire que la personne concernée en effectuant de simples activités quotidiennes nourrit le système de ses informations personnelles car les capteurs sont automatiquement activés sur la voie publique. C'est notamment le cas de la vidéosurveillance. Lorsqu'un individu marche dans la rue, il n'a aucune idée que ses faits et gestes peuvent être captés. Il a beau être réfractaire au système, son identité peut figurer dans des bases de données. Par exemple, si je refuse d'accéder à mon lieu de travail par le système de surveillance biométrique d'entrée dans mon établissement, je n'en serais pas moins sur l'ensemble des vidéos dès lors que celui-ci est activé en permanence. Aussi, à l'instar du cas de l'application *RadarApp* utilisée sur les réseaux sociaux rapportée dans l'étude de Politou, Alepis et Patsakis[58], mes données collectées à travers mes trajets dans les transports publics pourraient être réutilisées afin d'alerter mes proches sur ma santé mentale, sans mon consentement, et cela donc à mon insu.

Par ailleurs, les personnes réfractaires peuvent être en relation avec des personnes « connectées », et risquent malgré elles que leurs données soient traitées par leur intermédiaire et sans leur consentement.

Afin d'éviter ces dérives, les paramètres de traitement ne devraient être activés qu'à l'initiative de l'utilisateur, et non par une analyse permanente des données captées par la

[54] EDPB, *Connected vehicles*, §53, 14.
[55] A. Rouvroy et T. Berns, *« Gouvernementalité algorith-mique et perspectives d'émancipation » Le disparate comme condition d'individuation par la relation ?*, 169.
[56] L. Edwards, *Privacy, security and data protection in smart cities*, 22.
[57] S. Ghernaouti, *How Digital Ecosystem and Practices increase the Surveillance System's Performance and Generate New Risks for Human Rights*, dans *GNLU Law and Society Review*, vol. 2, 2020, 16-38, notamment 17.
[58] E. Politou, E. Alepis et C. Patsakis, *Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions*, 6.

technologie notamment en ce qui concerne la vidéosurveillance ou la biométrie[59].

Cela pose de nombreuses questions en termes de protection des données car le RGPD ne s'appliquera pas dans tels cas. Le consentement devrait pourtant être demandé dans tous les cas. L'existence des traitements devrait être signalée et la possibilité de ne pas en faire partie proposée systématiquement.

À l'égard des assistants vocaux électroniques, l'EDPB a mis en garde du fait qu'ils peuvent accidentellement capturer l'audio de personnes qui n'avaient pas l'intention d'utiliser le service[60]. Par exemple, si une personne appelle une amie « Alexia » à côté de l'assistant vocal Amazon « Alexa », l'assistant peut s'activer et traiter ses données personnelles. Or, il est très peu probable qu'une activation accidentelle puisse être interprétée comme un consentement valide, les données collectées accidentellement doivent donc être supprimées[61].

Par ailleurs, même si la personne concernée retire son consentement ou refuse le traitement, il est prouvé que des risques de ré-identification dans certains modèles d'apprentissage automatique existent[62]. Le responsable du traitement est tout de même tenu de supprimer les données personnelles qui ne pourraient pas être légalement utilisées. Les responsables du traitement et les sous-traitants doivent utiliser des modèles capables de perdurer en cas de retrait du consentement et appliquer des mesures d'atténuation pour ramener le risque de réidentification à un seuil acceptable[63]. Des études montrent cependant que des attaques par reconstruction et par inférence d'appartenance peuvent être réalisées, ce qui permet aux attaquants de récupérer des informations sur les personnes qui ont retiré leur consentement[64]. Par ailleurs, le seuil acceptable n'étant pas défini, le risque ne peut être contrôlé par l'individu.

4.2. *L'inévitable utilisation de la technologie face à l'inexistence d'alternatives*

La composante technique nécessaire au fonctionnement de la ville intelligente est la technologie. Il s'agit des technologies incorporées aux infrastructures, des capteurs, mais aussi des technologies possédées par les individus. La ville intelligente ne peut exister sans, et par ricochet le citoyen ne peut vivre dans la ville sans détenir cette technologie. Ce caractère obligatoire pose des questions essentielles quant à la liberté du consentement. Cela est d'autant plus fondamental qu'une fois imposée, la technologie a ensuite le pouvoir de diriger et de contrôler les comportements individuels[65]. Le citoyen est-il en mesure de refuser cette technologie ? Existe-t-il des alternatives réalistes au traitement de données personnelles par ces technologies ? Dans une ville optimisée technologiquement, que faire des personnes allergiques réfractaires, inaptes au numérique ?

4.2.1. *L'injonction de posséder des équipements*

En Chine, il n'est plus possible de se déplacer sans son smartphone qui conditionne l'accès à l'ensemble des services. L'occident n'est pas loin d'une telle injonction qui se trouve augmentée avec les villes intelligentes et la situation de pandémie et de crise sanitaire. Ce n'est pas tant le smartphone qui est en cause, mais la manière dont il est devenu le vecteur indispensable d'une économie numérique basée sur l'exploitation des données et à la réalisation des activités de la vie quotidienne qui doit être questionnée. En Suisse par exemple, l'accès à de nombreux restaurants a été conditionné par le téléchargement de l'application « Social Pass » afin de lutter contre la pandémie du Covid-19 en traçant les potentielles contaminations. De même, pour favoriser les applications mobiles et la « transition numérique », les Transports publics lausannois ont mis fin à l'achat de tickets de transport vers le conducteur, et les bornes d'achat des tickets ne reçoivent que des pièces de monnaies. L'individu qui se trouve sans pièce et sans smartphone ne peut donc entrer dans le transport, la carte bleue n'étant pas admise. Certains lieux n'autorisent l'accès qu'à condition d'être connecté pour suivre l'activité d'une personne. Il en va ainsi du parc d'attraction Super Nintendo World au Japon[66]. Pour participer à la ville intelligente,

[59] EDPB, *Virtual Voice Assistants*, §132, 30-31.
[60] EDPB, *Virtual Voice Assistants*, §30, 12.
[61] EDPB, *Virtual Voice Assistants*, §30, 12.
[62] EDPB, *Virtual Voice Assistants*, §101, 25.
[63] EDPB, *Virtual Voice Assistants*, §101 et 102, 25.
[64] EDPB, *Virtual Voice Assistants*, §103, 26.

[65] E. Sadin, *L'intelligence artificielle ou l'enjeu du siècle, anatomie d'un antihumanisme radical*, Paris, L'échappée, 2018, 37-68.
[66] https://objetconnecte.net/visiteurs-super-nintendo-world-bracelets-connectes-mario/.

le citoyen doit posséder des équipements électroniques et les technologies associées. L'accès aux services dépendra de l'acceptation d'utiliser des applications mobiles dont la vocation première est commerciale[67]. Le citoyen ne pourra s'en passer car l'exécution du service dépendra de la participation et de la détention du système. Même lorsque le numérique ne conditionne pas l'accès au service, de nombreuses incitations, des récompenses et des formes indirectes de punitions (systèmes de *bonus, malus*) sont créées pour convaincre l'individu d'en faire usage, cela associé à un discours marketing exacerbant le rôle de bon citoyen servant l'intérêt général[68]. Ce dernier aspect est largement mis en avant dans le cadre de la lutte contre la pandémie pour convaincre l'usager d'installer et d'utiliser l'application de traçage des contacts comme SwissCovid[69].

Y aura-t-il une place quelque part pour les migrants du numérique, pour ceux qui ont une phobie du mobile ou qui souffrent d'addiction numérique, de surmenage digital (digital intox) ou qui souffrent de l'exposition aux ondes électromagnétiques ? Cette problématique semble peu prise en compte dans la manière d'implémenter les technologies dans les villes. La 5G a par exemple fait l'objet d'oppositions virulentes pour des raisons sanitaires et environnementales. Ces contestations n'ont toutefois pas suffi à faire restreindre les déploiements partout en Suisse[70]. Dans ce même sens, des antennes ont été installées contre l'avis d'un maire en France[71]. Si ce phénomène ne touche pas directement le consentement au traitement de données, il démontre tout de même que l'imposition des technologies aux citoyens, étapes par étapes, sans un choix réel, et ces technologies ont vocation finale à considérablement augmenter les traitements de données personnelles.

4.2.2. *Un traitement multimodal incontrôlable*

La technologie est la pièce maîtresse et omniprésente de la ville intelligente. Chacun doit l'utiliser sans pour autant qu'elle soit paramétrable selon ses choix spécifiques. Par défaut et par sa conception, l'objet numérique connecté (conçu sans « security by design » ni « privacy by default ») prélèvera le maximum de données le plus souvent possible, ce qui est, a priori, contraire au principe de minimisation des données (art. 5 al. 1 let. c RGPD). Si la personne accepte d'utiliser un smartphone pour quelques finalités définies, elle doit en réalité s'attendre à un ensemble de traitements bien plus larges que ceux prévus initialement. Face à cette ouverture des possibles, il est illusoire de moduler les traitements selon des finalités strictes. Dans l'internet des objets, la possibilité de renoncer à certains services ou fonctionnalités est d'avantage un concept théorique qu'une alternative réelle[72]. Pour la technologie implémentée dans la ville intelligente, il est impossible d'imaginer comment en temps réel, une personne pourra définir quelles informations personnelles la concernant peuvent être traitées ou non et pour quelles finalités. Le responsable du traitement devrait proposer un *opt-in* distinct pour chaque finalité, afin de permettre aux utilisateurs de donner un consentement spécifique pour des finalités spécifiques[73], mais cela semble illusoire dans la réalité. Par exemple, si un titre de transport sur smartphone pour un trajet d'un seul arrêt (2 minutes) implique un consentement au traitement des données de géolocalisation, d'achat, de comportement à des fins de marketing, de stockage pour faciliter les usages suivants, mais aussi à des fins de gestion des fichiers sur les clients, la personne concernée aura difficilement le temps de lire, de comprendre et d'accepter ou refuser les différents traitements. La solution la plus simple est d'accepter le traitement comme lorsque l'on accepte les *cookies* sur Internet, par lassitude de décocher l'ensemble des finalités proposées.

En France, deux lycées publics ont mis en place un dispositif de contrôle d'accès aux

[67] D. Cliche, P. Turmel, et S. Roche, *Les enjeux éthiques de la ville intelligente : don-nées massives, géolocalisation et gouvernance municipal*, 238.
[68] S. Ghernaouti, *Trou noir & données de santé*, dans *Blog – Le Temps*, 2020, disponible sous : https://blogs.letemps.ch/solange-ghernaouti/2020/09/27/trou-noir-donnees-de-sante/.
[69] L. Cellier et S. Ghernaouti, *SwissCovid, un dispositif médical ?*, dans *Jusletter*, 22 Mars 2021, disponible sous: https://jusletter.weblaw.ch/juslissues/2021/1060/-swisscovid_-un-dispo_2a825b49d2.html__ONCE&log-in=false, 26.
[70] https://www.lematin.ch/story/pres-de-3000-antennes-5g-activees-en-suisse-123577519701.
[71] https://france3-regions.francetvinfo.fr/occitanie/la-5g-poursuit-son-deploiement-en-occitanie-malgre-les-contestations-1940035.html.
[72] G29, WP 223, 7.
[73] EDPB, *Virtual Voice Assistants*, §90, 24.

bâtiments par comparaison faciale et de suivi de trajectoire. La Commission Nationale de l'Informatique et des Libertés (CNIL) consultée par la région PACA avait rendu un avis défavorable sur ce projet vu le risque majeur pour la vie privée et les libertés individuelles et sa contradiction au principe de minimisation de données[74]. Ces risques ont été jugés disproportionnés par rapport au besoin et au but recherché de sécurisation et fluidification des entrées notamment face à des mineurs. Constituant des données sensibles, le traitement de données biométriques est en principe interdit. Il n'est autorisé que sur la base du consentement explicite de la personne concernée[75]. Sur ce motif, le système de reconnaissance faciale a été installé dans les deux lycées, en dépit de la position de la haute autorité. Les tribunaux ont alors été saisis par des associations de parents d'élèves et d'enseignants, mais aussi par la Quadrature du net[76]. Le 27 février 2020, le tribunal administratif de Marseille annule alors l'autorisation de la région permettant aux lycées d'exploiter les systèmes d'accès biométriques[77]. La région s'est notamment vu reprocher de ne pas avoir prévu de garanties suffisantes en vue d'un consentement libre et éclairé de la part des lycéens ou de leurs représentants légaux[78]. Le système étant appliqué de façon générale et sans exception, aucun refus ni retrait du consentement ne serait réellement possible puisqu'il impliquerait de ne pas être accepté dans l'établissement[79]. Par ailleurs, il n'est pas possible de paramétrer une caméra fonctionnant à tout moment pour prendre en compte les refus de certains.

Même si les dispositifs prévoient des moyens de refuser, ils sont techniquement presque impossibles à mettre en œuvre. La CNIL a estimé par exemple que la possibilité de faire non de la tête pour refuser un traitement de données à une caméra de reconnaissance faciale à Paris, dans la station de Châtelet-les-Halles, est une solution « peu praticable dans les faits et difficilement généralisable […] qui fait porter une charge trop importante sur la personne[80] ».

4.2.3. *Un coût indirect et caché porté par le citoyen/consommateur*

L'injonction d'innovation technologique s'inscrit dans une logique d'optimisation et de rationalisation économiques basées sur l'exploitation des données captées gratuitement (mais dont le coût est porté par l'utilisateur via notamment l'achat de son objet connecté (téléphone, montre, ordinateur, …) et son abonnement télécom et par le temps passé à produire des données)[81]. Dans les lieux publics, le coût du Wi-Fi « gratuit » est à la charge de la société, c'est-à-dire du service public tandis que les bénéfices de la connectivité sont généralement pour le secteur privé qui en maîtrise les usages. Le citoyen paye pour l'ensemble de la mise en place, du développement et de la maintenance de la ville intelligence. Dans la ville de Marseille, par exemple, le financement du projet d'expérimentation de vidéosurveillance coûte aux collectivités locales, à la ville et en partie à l'Union européenne 1,8 millions d'euros, qui sont donc prélevés par l'impôt. Il paye également le coût de l'obsolescence programmée et celui de la pollution engendrée par l'ensemble des traitements de données et infrastructures déployées.

Si le service est gratuit, c'est que l'individu est le produit ou alors qu'il le paye par le biais d'impôts. Le fait de rendre gratuit le service fait immerger le modèle économique où les personnes nourrissent le système pour financer la smart city. Cela passe par un consentement invisible et l'objectif de faire passer un temps connecté le plus élevé possible aux personnes[82].

[74] Commission Nationale de l'Informatique et des Libertés (CNIL), *Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position*, 2019, disponible sous : https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position.

[75] Art. 9 RGPD.

[76] La Quadrature du Net, *Reconnaissance faciale : un recours pour faire barrage à la surveillance biométrique*, 2019, disponible sous : https://www.laquadrature.net/2019/02/19/reconnaissance-faciale-un-recours-pour-faire-barrage-a-la-surveillance-biometrique/.

[77] Tribunal Administratif de Marseille (TA), 9ème Chambre, Arrêt du 27 Février 2020, req. n. 1901249, disponible sous : https://www.dalloz-actualite.fr/document/ta-marseille-27-fevr-2020-req-n-1901249.

[78] TA Marseille, Arrêt du 27 avril 2020, Considérant 12, 5.

[79] A. Fitzjean ó Cobhthaig, *Recours du 14 février 2019*, 24, disponible sous : https://www.laquadrature.net/wp-content/uploads/sites/8/2019/02/Recours-D%C3%A9lib%C3%A9ration-14.12.18.pdf.

[80] https://www.lesnumeriques.com/vie-du-net/la-cnil-dit-non-aux-cameras-intelligentes-de-chatelet-les-halles-et-cannes-n151675.html

[81] S. Ghernaouti, *Cyberpower, crime conflict and security in cyberspace*, Lausanne, EPFL Press, 2013, 14.

[82] Laboratoire d'Innovation Numérique de la CNIL, *La*

La personne concernée devrait être informée lors du traitement de ses données personnelles, au moment de donner son consentement, que ses informations financent le système. Il serait intéressant également de savoir à quel montant se chiffre le bénéfice rapporté par une personne pour un traitement précis.

Par ailleurs, la dépendance envers le privé est très dangereuse car elle soumet l'argent public à la contrainte d'être injectée dans le domaine privé, pour lutter contre l'obsolescence des infrastructures. Ce mécanisme de verrouillage technologique[83] provoque un emprisonnement des individus comme de l'État à la contrainte de mettre à jour des systèmes dont seule une entreprise en a l'aptitude, et donc de supporter le coût de ces ajustements. Cela provoque un affaiblissement du secteur public au bénéfice d'acteurs privés, éventuellement d'origine étrangère, générant une perte de souveraineté préjudiciable à l'État.

4.2.4. *L'imposition d'une surveillance*

L'eldorado numérique s'est transformé à l'insu des personnes, en économie de la surveillance de masse et de la surveillance personnalisée. Le marketing du consentement pour se laisser déposséder de ses données et se faire surveiller informatiquement est très efficace[84]. L'injonction d'utiliser les technologies et de passer par des services numériques a pour conséquence majeure de créer de manière insidieuse et indirecte une surveillance généralisée à laquelle il n'est plus concevable d'échapper. Cela passe notamment par des dispositifs de reconnaissance faciale[85] ainsi que de la vidéo surveillance[86] dont il faut se méfier[87]. Les caméras de surveillance dans les villes de Marseille en sont des exemples, Eda, membre de la Quadrature du Net dénonce qu'à Marseille il est impossible de circuler sans être filmé : « il n'y a aucun trajet possible où je pouvais ne pas être repérée par ces caméras, dans ma ville je suis donc surveillée en permanence »[88]. Une cartographie a d'ailleurs été mise en place pour montrer par ville les dispositifs existants[89].

L'ensemble des faits et gestes sont captés par les technologies du numérique si bien qu'il n'est plus possible de distinguer l'identité personnelle physique et l'identité numérique. Le monde virtuel ne permet plus de se cacher[90]. Il est en effet possible désormais dans des lieux publics (aéroports, centres commerciaux, …) de relier l'identification d'un smartphone (possible grâce à l'usage du Wi-Fi), à une personne se déplaçant dans une zone de vidéosurveillance.

Ces ensembles d'innovations engendre donc la perte de l'anonymat[91] qui risque de découler ensuite sur une confiscation de la liberté d'aller et venir et un système proche du Crédit Social Chinois. À Toronto par exemple, le Conseil municipal a été mis en garde du risque que la société Alphabet (Google) utiliserait des algorithmes pour suivre et influencer le comportement des résidents[92]. À terme, cela mènerait donc au contrôle des individus[93].

Le projet de filmer les individus dans les transports publics afin de surveiller le respect des mesures anti-covid illustre bien cette problématique. Même un réfractaire figure dans les bases de données car il est impossible de ne pas être filmé et si l'on recoupe ses

plateforme d'une ville - Les données personnelles au Coeur de la fabrique de la smart city, in *Cahiers IP Innovation & Prospective*, n. 5, 2017, 19.

[83] D. Cliche, P. Turmel, et S. Roche, *Les enjeux éthiques de la ville intelligente : don-nées massives, géolocalisation et gouvernance municipal*, 238.

[84] S. Ghernaouti, *Mobility pricing & Contact tracing*, dans *Blog – Le Temps*, 2020, https://blogs.letemps.-ch/solange-ghernaouti/2020/05/02/mobility-pricing-contact-tracing/.

[85] https ://www.laquadrature.net/2019/10/15/reconnaissance-faciale-dans-les-lycees-debat-impossible/.

[86] https://www.laquadrature.net/2020/01/20/safe-city-a-marseille-premier-recours-contre-la-videosurveillance-automatisee-de-lespace-public/.

[87] https://www.laquadrature.net/2019/06/21/le-vrai-visage-de-la-reconnaissance-faciale/.

[88] https://www.franceculture.fr/emissions/lsd-la-serie-documentaire/a-lere-de-la-surveillance-numerique-34-d-ans-les-allees-de-la-safe-city entre 06:40 et 07:13.

[89] https://technopolice.fr/villes/.

[90] D. Cliche, P. Turmel, et S. Roche, *Les enjeux éthiques de la ville intelligente : don-nées massives, géolocalisation et gouvernance municipal*, 234.

[91] M. Dieuzeide et C. Coulée, S*mart cities: quelles sont les principales menaces ?*, Master thesis, Louvain School of Management, Université catholique de Louvain, Louvain, 2018, 28, disponible sous : http://hdl.handle.net/2078.1/; Laboratoire d'Innovation Numérique de la CNIL, *La plateforme d'une ville - Les données personnelles au Coeur de la fabrique de la smart city*, 13.

[92] https://www.zdnet.fr/actualites/smart-city-la-ville-futuriste-the-line-redefinira-t-elle-la-megalopole-de-demain-39918193.htm.

[93] S. Breux et J. Diaz, *La ville intelligente : origine, définitions, forces et limites d'une expression polysémique Institut national de la recherche scientifique*, Montréal, Centre Urbanisation Culture Société, 2017, disponible sous : http://espace.inrs.ca/id/eprint/4917, 21.

données envoyées par un téléphone portable, la déduction de sa présence à bord et de son identité sont facilitées. Si dans ce cas précis, les raisons sanitaires justifient cette exploitation, il risque par ce type de système de généraliser la surveillance vidéo pour des motifs entrant moins dans l'intérêt public mais « vantés » comme tels (sécurité, efficacité des services, mise en relation…).

4.2.5. *Le préjudice du réfractaire*

Les réfractaires aux traitements de données risquent de s'exclure du fait d'une fracture entre ceux qui ne veulent pas et ceux qui veulent participer au système[94]. Ainsi par exemple, l'étudiant qui ne souhaite pas utiliser l'informatique se risque à être exclu des plateformes pédagogiques où les ressources d'apprentissage sont mises à disposition, des listes de communications par mail, des groupes de discussion en lignes, etc.

Ce sont les réfractaires qui devront payer un coût supplémentaire pour passer par un service « normal ». En sus des réfractaires, les personnes qui n'ont pas les finances ou les compétences d'utiliser la technologie se trouveront en marge[95]. Ces ensembles de facteurs créeront des inégalités qui ne doivent pas être négligées dans l'offre du service[96]. Pourtant, pour garantir la liberté du consentement, les utilisateurs ne devraient pas être pénalisés économiquement ni avoir un accès dégradé aux capacités de leurs appareils s'ils décident de ne pas utiliser l'appareil ou un service spécifique[97].

Si accéder à un service physique nécessite de payer un coût supplémentaire, le consentement ne peut être considéré libre car la personne concernée subit un préjudice financier du fait de son refus. Or, si elle veut éviter le préjudice financier, elle n'a pas d'autre choix que d'accepter. Ce type de configuration est contraire au considérant 42 du RGPD qui considère le consentement non librement donné si la personne concernée n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice.

Dans l'affaire des lycées marseillais, l'absence de liberté du consentement tenait notamment dans le fait que le réfractaire au système ne pouvait véritablement refuser sans subir de préjudice puisque cela lui aurait valu un rejet de l'établissement[98], mettant alors à mal son droit fondamental à l'éducation. L'acceptation du traitement de données biométriques n'est pourtant pas nécessaire à la mise en œuvre de la scolarisation. Le préjudice qui en découlait était donc sans rapport avec le traitement. Même si un contrôle classique avait été maintenu en parallèle, cette alternative aurait été préjudiciable aux réfractaires puisque les temps d'attente auraient été plus importants et des formalités supplémentaires auraient pu s'ajouter[99]. Ces désagréments, renforcés par un manque de moyens humains pour mener les contrôles d'accès auraient eu pour effet d'exercer une contrainte indirecte sur les élèves afin d'obtenir leur consentement[100].

Lorsque le traitement basé sur le consentement porte sur des données biométriques, une solution alternative sans contrainte ni coût supplémentaire devrait être proposée. Si le service sert à l'authentification d'individu, l'alternative sert notamment aux personnes incapables d'utiliser le dispositif ou pour des cas de dysfonctionnement[101]. La France mis en place un système d'accès au service public en ligne via l'application de reconnaissance faciale ALICEM dont le caractère non-libre du consentement été dénoncé du fait de l'absence d'alternative pour les usagers[102]. Le recours[103] a toutefois

[94] D. Cliche, P. Turmel, et S. Roche, *Les enjeux éthiques de la ville intelligente : don-nées massives, géolocalisation et gouvernance municipal*, 240.
[95] M. Dieuzeide et C. Coulée, S*mart cities: quelles sont les principales menaces ?*, 21.
[96] S. Breux et J. Diaz, *La ville intelligente : origine, défi-nitions, forces et limites d'une expression polysémique Institut national de la recherche scientifique*, 24 ; M. Dieuzeide et C. Coulée, S*mart cities: quelles sont les principales menaces ?*, 21.
[97] G29, WP 223, 23.
[98] A. Fitzjean ó Cobhthaig, *Recours du 14 février 2019*, n. 108, 24.
[99] A. Fitzjean ó Cobhthaig, *Recours du 14 février 2019*, n. 108, 24.
[100] A. Fitzjean ó Cobhthaig, *Recours du 14 février 2019*, n. 109, 24.
[101] EDPB, *Dispositifs vidéo*, 21.
[102] Commission nationale de l'informatique et des libertés, *Délibération n°2018-342 du 18 octobre 2018 portant avis sur projet de décret autorisant la création d'un traitement automatisé permettant d'authentifier une identité numérique par voie électronique dénommé « Application de lecture de l'identité d'un citoyen en mobilité» (ALICEM) et modifiant le code de l'entrée et du séjour des étrangers et du droit d'asile demande d'avis n°18008244*, disponible sous : https://www.legifrance.gouv.fr/download/pdf?id=JQDkiVqbiPoVpbHfpdweSZcrPSXYo-T8chbNahjpRk0.
[103] A. Fitzjean Ó Cobhthaigh, *Recours du 15 juillet 2019*, disponible sous : https://www.laquadrature.net/wpcontent/uploads/sites/8/2019/07/1084951458_DECR_ALICEM_REQ.pdf.

été rejeté par le Conseil d'État, le dispositif « France Connect » permettant une authentification de substitution, le refus d'utiliser ALICEM impliquait seulement de renoncer soit à un niveau de protection renforcé contre l'usurpation d'identité, soit à une démarche en ligne au profit d'une démarche physique[104]. Le système d'authentification via France Connect ne permet pas de détenir une protection contre l'usurpation d'identité suffisante, donc potentiellement un préjudice pourrait être causé à l'administré, le contraignant possiblement à tout de même opter pour la solution ALICEM l'alternative d'un passage à un service physique équivalent n'est pas sans incidence pour l'intéressé. La fracture numérique provoquée par un traitement « traditionnel » et un traitement numérique pourrait par exemple faire advenir un désavantage disproportionné car le traitement traditionnel est menacé de devenir obsolète, long et coûteux pour les personnes concernées, notamment pour les personnes âgées.

4.3. *Sur l'identité du responsable du traitement*

Dans le cadre d'une ville intelligente, la multiplicité des acteurs impliqués dans le traitement des données personnelles pose problème. Qui est le responsable du traitement des données personnelles ? Comment donner un consentement libre à chacun des acteurs impliqués alors qu'ils ne sont pas annoncés ? Le modèle de la gouvernance par des algorithmes se développe. À partir de l'ensemble des données confiées par les citoyens, des décisions politiques peuvent être prises. Seulement le citoyen a-t-il consenti de manière éclairée à cet usage de ses informations personnelles ? Est-il libre ou non de participer à ce système ?

4.3.1. *Un public se diluant dans le privé au détriment de l'intérêt général*

Les infrastructures qui à l'époque appartenaient à l'État, sont désormais et seront à l'avenir entre les mains du privé. Cela implique que l'infrastructure publique et les services publics passent par le traitement de données par du privé. Les données sont exploitées par des privées mais elles sont collectées sur le domaine public. Les données transitent sur des dispositifs privés alors que l'infrastructure est officiellement confiée au public : les dispositifs sont de la propriété et du contrôle étatique[105]. L'État fera appel dans à un ensemble d'acteurs technologiques qui seront donc responsables du traitement des données ou alors sous-traitants. Cela créer un problème de détermination du responsable de traitement[106]. De nombreuses études dénoncent le risque de privatisation du secteur public[107] en ce qu'elle risque de laisser prendre possession de l'avenir de la ville aux acteurs privés[108].

Cette structure pose une difficulté de mise en œuvre de la liberté du consentement car l'opérateur public contraint en quelque sorte de passer par un traitement de privé. Cette problématique future est déjà bien présente. À Nice par exemple, les entreprises Thalès et Engie-Inéo, déploient des systèmes de surveillance intelligents sur l'ensemble du territoire, et pourraient prendre possession du contrôle de la sécurité de la ville grâce à une cartographie en temps réels des faits et gestes des citoyens[109]. De même dans l'affaire des lycées français, les élèves n'avaient pas d'autres choix que d'accepter de livrer leurs informations biométriques à un privé pour accéder aux locaux et de bénéficier de leur droit fondamental à l'éducation.

Les entreprises exercent par cette implémentation une influence considérable sur les politiques publiques[110]. Le risque de conflits d'intérêts est grandissant [111] comme celui de s'écarter des besoins de la population et de l'intérêt public car les entreprises

[104] Conseil d'État, Décision N° 432656 du 04 Novembre 2020, https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2020-11-04/432656.

[105] D. Cliche, P. Turmel, et S. Roche, *Les enjeux éthiques de la ville intelligente : don-nées massives, géolocalisation et gouvernance municipal*, 237.

[106] L. Edwards, *Privacy, security and data protection in smart cities*, 2.

[107] D. Cliche, P. Turmel, et S. Roche, *Les enjeux éthiques de la ville intelligente : don-nées massives, géolocalisation et gouvernance municipal*, 237; S. Breux et J. Diaz, *La ville intelligente : origine, définitions, forces et limites d'une expression polysémique Institut national de la recherche scientifique*, 22.

[108] S. Breux et J. Diaz, *La ville intelligente : origine, défi-nitions, forces et limites d'une expression polysémique Institut national de la recherche scientifique*, 22.

[109] https://www.laquadrature.net/2018/07/06/nice-smart-city-surveillance/.

[110] Cliche, P. Turmel, et S. Roche, *Les enjeux éthiques de la ville intelligente : don-nées massives, géolocalisation et gouvernance municipal*, 237.

[111] M. Dieuzeide et C. Coulée, *Smart cities: quelles sont les principales menaces ?*, 28.

agissent dans une logique de profit[112]. Ainsi que le dénonce Ghernaouti : « Leurs produits commerciaux sont en passe de devenir des invariants indispensables à la gestion publique. Les Google, Apple, Facebook, Amazon, Microsoft, ou encore Palantir (géant américain de l'analyse des données, en lien avec des agences de renseignement américains et dont une partie du financement initial est issu de la CIA) par exemples, ne cessent de développer des partenariats avec diverses entreprises locales et autorités de par le monde. Les opérateurs téléphoniques sont également très présents sur le marché du contrôle sécuritaire du fait de leur maitrise des données de géolocalisation. Les technologies, services et données de géolocalisation et de navigation constituent des enjeux économique et géopolitique majeurs, y compris dans leur indissociable dimension de la maitrise de l'espace et des satellites, à des fins civiles et militaires.[113] »

4.3.2. *L'intervention de nombreux tiers dans le traitement des données*

Le traitement de données personnelles dans une ville intelligente est d'autant plus opaque qu'il est effectué par différents opérateurs dont la personne concernée ne soupçonne pas même l'existence. Une multitude de parties prenantes sont impliquées dans les processus de captation et d'analyse des données personnelles. Pour un tram connecté, certains capteurs seront attribués à une entreprise, le tram en lui-même par une autre et la responsabilité finale à un service de l'État. L'ensemble des données captées sur le tram transiteront vers ces entreprises, mais encore d'autres chargées par exemple de la sécurité, de l'analyse des données, de publicité. Un fort nombre d'organisations s'échangent nécessairement les informations et parfois même d'autres tiers seront impliqués. Il conviendrait d'informer la personne concernée de l'identité du responsable du traitement pour chaque traitement envisagé afin de garantir un consentement éclairé. Il est toutefois compliqué de connaitre le responsable du traitement et de savoir à qui sont communiquées les données et pour quelles finalités. Cette information semble très difficile à donner puisque comme vu précédemment au moment T, il n'est pas possible de déterminer qui aura un regard et un usage des données pour chaque finalité. Le G29 a mis en garde sur la nécessité d'un consentement éclairé dans ce contexte avec l'Internet des objets où il soulignait que des multiples parties prenantes peuvent avoir accès à des informations sensibles stockées sur les terminaux[114]. L'exigence de consentement existe donc non seulement à l'égard du responsable du traitement mais aussi du fabricant du dispositif ainsi que toutes les parties prenantes qui ont un accès aux données brutes stockées dans les infrastructures[115]. Cette exigence va de pair avec celles de la détermination préalable des finalités du traitement : si d'autres professionnels accèdent aux données, la finalité doit le prévoir explicitement afin de s'assurer qu'elles soient traitées dans un but précis[116].

Chaque partie prenante à l'internet des objets et donc par extension à la ville intelligente doit s'assurer que la personne concernée a effectivement consenti au stockage et/ou à l'accès, après avoir obtenu du responsable du traitement des informations claires et complètes sur, entre autres, les finalités du traitement[117]. Par exemple, si le coureur d'un stade connecté utilise sa montre sportive pour charger des données de séances de sport, le fabriquant de la montre doit obtenir le consentement de l'utilisateur pour obtenir le graphe créé par le stade sur la montre et l'enregistrer sur ses serveurs. En qualité de fabricant, il ne devrait pas traiter de données du consommateur puisque la personne concernée a décidé de créer son profil de sport uniquement dans le stade connecté.

Lorsque des données sont envoyées à un partenaire commercial à partir d'un objet connecté, celui-ci devient à son tour responsable de traitement. Dès lors, il devrait systématiquement demander un nouveau consentement à la personne concernée. Dans le cadre d'un véhicule connecté, l'EDPB

[112] Cliche, P. Turmel, et S. Roche, *Les enjeux éthiques de la ville intelligente : don-nées massives, géolocalisation et gouvernance municipal*, 238.
[113] S. Ghernaouti, *Mobility pricing & Contact tracing*.
[114] G29, WP 223, 14.
[115] G29, WP 223, 14.
[116] L. Cellier et S. Ghernaouti, *An interdisciplinary approach for security, privacy and trust in the electronic medical record: A pragmatic legal perspective*, in *IEEE International Conference on E-health Networking, Application & Services (HealthCom)*, 2019, 2.
[117] G29, WP 223, 14.

recommande par exemple l'utilisation d'un dispositif logique ou physique ou la possibilité de cocher une case à chaque nouveau traitement envisagé par la voiture[118].

Même si le tiers privé n'est pas responsable ni sous-traitant, sa participation au processus pose question car il a une vue d'ensemble sur le système alors que le citoyen lui n'est pas en capacité de déterminer quels traitements sont effectués sur ses informations. Avec l'application SwissCovid, par exemple, l'implication de Google et Apple dans le processus de fabrication et de maintenance du dispositif ne permet pas une totale confiance dans un projet pourtant public[119]. Le G29 a souligné à ce propos que de nombreux capteurs sont exposés dans les API afin de faciliter le développement d'application mais souvent, les demandes d'autorisation faites par des tiers développeurs d'applications n'affichent pas suffisamment d'informations pour que le consentement de l'utilisateur soit considéré comme spécifique et suffisamment éclairé, donc valable[120].

En cas de refus ou de retrait du consentement, l'ensemble des acteurs de la chaîne de traitement devrait être informée et agir en conséquence pour stopper tout traitement. Les méthodes devraient être aussi conviviales que possible[121]. Or, il semble compromis dans une *smart city* de réussir à obtenir la transparence de tous les processus en direct alors que pour le monde de l'internet les politiques de confidentialité sont déjà toutes inintelligibles et si volumineuse qu'elles ne permettent pas aux personnes concernées de s'informer efficacement.

Par ailleurs, les données sont également utilisées par des tiers à l'étranger sans que cela ne soit vraiment prévu et su par l'utilisateur. Aux USA, le Cloud Act permet au gouvernement de réquisitionner toutes les données qu'il souhaite aux entreprises situées sur son sol, sans justification ni notification à apporter à la personne concernée mais simplement pour un motif général de sécurité nationale. À ce titre, le consentement ne devrait pas être invoqué lorsque les transferts sont récurrents, massifs ou structurels[122]. Une ville connectée en Europe devrait donc éviter dans la mesure du possible les technologies étrangères. Or, il est bien connu que les GAFAM et autres entreprises américaines sont largement préférées pour des projets de grande envergure à l'instar de l'utilisation du Microsoft Azure Cloud pour l'hébergement des données de santé des Français[123] ou la participation de Google et Apple dans le dispositif SwissCovid.

4.3.3. *Un privé en situation de monopole ou de quasi-monopole, un abus de position dominante ?*

Les citoyens pourraient ne plus pouvoir se passer de certaines entreprises de la ville intelligence. Ce serait notamment le cas de celles qui obtiennent le mandat d'exécution d'une tâche fondamentale qui deviennent alors indispensables[124]. Ce privé est en situation de monopole ou de quasi-monopole. Du fait de l'exécution d'un service public, il est en situation de position dominante étant donné qu'aucun autre concurrent n'est capable de fournir une prestation de service public définie par la loi. Reste à savoir si le responsable de traitement abuserait de sa position dominante. Puisque la personne concernée dépend de celui-ci pour bénéficier d'un service public ou d'un service essentiel, elle n'a pas d'autres choix que d'accepter les conditions du traitement de données personnelles. Il s'agit donc d'un abus de dépendance économique qui ne dispose pas de solution équivalente.

Cette situation d'abus de position dominante rejoint l'interdiction du considérant 43 du RGPD selon lequel le consentement ne peut être librement donné si dans une situation de déséquilibre de la relation la personne concernée n'est pas en mesure de choisir librement. Par la position de prestataire unique, la personne concernée n'a en effet pas d'autre choix que d'accepter le traitement. Elle subira donc un préjudice en cas de refus ou de retrait de son consentement (contrairement à ce qui est prévu au considérant 42). Si la personne concernée ne peut plus bénéficier d'un service essentiel, ou public, elle se verra, en effet, privée de l'exercice d'un autre droit, ou alors de ses

[118] EDPB, *Connected vehicles*, 25.
[119] L. Cellier et S. Ghernaouti, *SwissCovid, un dispositif médical ?*, 15.
[120] G29, WP 223, 12.
[121] G29, WP 223, 22.
[122] L. Edwards, *Privacy, security and data protection in smart cities*, 26.
[123] https://www.cnil.fr/fr/la-plateforme-des-donnees-de-sante-health-data-hub.
[124] T. Braun, B. C.M. Fung, F. Iqbal, et B. Shah, *Security and privacy challenges in smart cities*, dans S*ustainable Cities and Society*, vol. 39, 2018, 499-507, notamment 504.

finances.

Cette situation de monopole peut conduire à des situations semblables à celle interdite par l'art. 7 al. 4 RGPD qui interdit de lier l'exécution du contrat à l'obtention d'un consentement qui n'est pas nécessaire à l'exécution du contrat. Il s'agirait par exemple d'une situation où l'exploitant prévoit de manière générale que l'utilisateur de la route connectée doit accepter que ses données personnelles soient utilisées à des fins de publicité ciblée alors que son passage sur la route ne nécessiterait a priori qu'un traitement à des fins d'autorisation d'accès et à la limite la surveillance du respect des règles autoroutières.

5. *Éléments de conclusion et conséquences pour le consentement*

À travers la recherche et l'identification des caractéristiques de la ville intelligente et la confrontation aux exigences d'un consentement licite, l'analyse permet de conclure que ce motif n'est pas approprié à la structure des traitements. Les cas étudiés, les exemples illustratifs et les exigences de l'EDPB (European Data Protection Board) inquiètent sur les implémentations insidieuses de technologies. D'une part, l'information est totalement illusoire à cause du manque de transparence du traitement et d'autre part, il n'existe pas de réelles alternatives aux traitements de données qui sont automatisés forçant le choix de l'individu.

Le volume et la diversité des données personnelles collectées rendent quasiment impossible de garantir un réel contrôle de la personne concernée[125]. Les transferts de données sont multiples, instantanés et continus, ils s'opèrent, sur de nombreux systèmes et dispositifs[126], entre plusieurs acteurs ce qui limite la qualité d'un consentement éclairé.

Lire et comprendre les conditions générales d'utilisation de chacun des services serait trop compliqué et chronophage[127]. Ce facteur constitue un des enjeux pour la numérisation d'une ville en accord avec un consentement licite. Les traitements de données personnelles étant très nombreux dans la ville connectée, l'utilisateur risque de se perdre dans les informations à lire et finalement décider de les ignorer. Nombreuses sont les études montrant que les politiques de confidentialités sont si volumineuses, s'étendant sur de multiples pages que l'utilisateur les accepte par défaut sans les lire[128].

Si le responsable du traitement a pris le temps d'établir une information conforme au RGPD, claire et complète, où le responsable du traitement est identifié, les finalités détaillées ou même le droit de retrait du consentement est annoncé, il est tout de même à redouter que la personne concernée risque de ne pas comprendre les implications du traitement. Il peut être assez difficile pour un utilisateur non-expert de comprendre comment les données personnelles seront utilisées ou si elles seront anonymisées[129]. Les explications sont souvent laborieuses car elles ne tiennent pas compte du contexte de l'utilisation du service, de la langue parlée ou encore des règles juridiques propres à chaque pays[130].

L'article ne traite pas de la question du consentement des mineurs, qui mérite un développement à part entière mais la structure de la ville connectée amène à se demander comment le consentement d'un parent peut être donné conformément à l'article 8 du RGPD alors même que les traitements sont passifs et généralisés ? Lorsque les traitements numériques ont lieu dans le monde physique, l'authenticité de l'accord parental question cruciale sur le web[131], parait encore plus nécessaire. Si même pour un adulte les mécanismes de consentement sont illusoires dans le monde physique, comment imaginer qu'une personne mineure puisse être à l'abri de la captation permanente de son image et de

[125] Laboratoire d'Innovation Numérique de la CNIL, *La plateforme d'une ville - Les données personnelles au Coeur de la fabrique de la smart city*, 14.
[126] Laboratoire d'Innovation Numérique de la CNIL, *La plateforme d'une ville - Les données personnelles au Coeur de la fabrique de la smart city*, 14.
[127] Laboratoire d'Innovation Numérique de la CNIL, *La plateforme d'une ville - Les données personnelles au Coeur de la fabrique de la smart city*, 14.
[128] R. Neisse, G. Baldini, G. Steri, Y. Miyake, S. Kiyomoto, et A. R. Biswas, *An Agent-based Framework for Informed Consent in the Internet of Thing*, 1.
[129] R. Neisse, G. Baldini, G. Steri, Y. Miyake, S. Kiyomoto, et A. R. Biswas, *An Agent-based Framework for Informed Consent in the Internet of Thing*, 1.
[130] R. Neisse, G. Baldini, G. Steri, Y. Miyake, S. Kiyomoto, et A. R. Biswas, *An Agent-based Framework for Informed Consent in the Internet of Thing*, 1.
[131] L. Cellier et S. Ghernaouti, *General Comment on children's rights in relation to the digital environment*, Haut-Commissariat des Nations Unies aux droits de l'homme, 2020, disponible sous : https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx, 4.

ses informations personnelles ?

Le consentement donné dans un contexte général de ville intelligente ne peut pas être vraiment éclairé. En effet, même si un responsable du traitement a effectué son devoir légal, la structure de la ville intelligente (ou même de l'Internet) ne permet pas à chaque personne de donner pour chaque traitement un consentement éclairé. Les politiques de confidentialité sont par ailleurs très souvent non modulables en ce sens qu'elles sont générales, le consentement n'est donc pas granulairement proposé, c'est-à-dire qu'il n'y a pas la possibilité de choisir quel traitement accepter ou refuser. À ce titre, le consentement est présumé ne pas pouvoir être donné librement puisqu'un consentement distinct ne peut pas être donné à différentes opérations de traitement des données à caractère personnel bien que cela soit approprié dans le cas d'espèce[132]. En outre la personne concernée n'a pas d'autre alternative réaliste que d'accepter le traitement, la seule autre option étant alors de renoncer au service[133]. Cependant dans la ville intelligente, il est impossible de vivre sans être connecté en permanence, car il n'existe pas d'alternative valable. Il semble impossible de s'opposer à la numérisation et aux traitements de données qu'elle implique. Le consentement en l'état semble d'avantage être passif qu'explicite, il est donné par lassitude ou par absence de choix. L'économie biface des données qui consiste à une entreprise qui exploite massivement des données en échange d'un service gratuit tend à s'étendre à la ville numérique avec la même asymétrie. La nouveauté est que le service offert est essentiel, indispensable au citoyen. Il n'y a donc plus de possibilité de refuser. L'asymétrie dans la relation ne permet pas à la personne concernée de consentir librement, puisqu'elle n'a pas les pouvoirs de connaitre et de paramétrer les traitements qui la concernent.

Les principes de « *privacy by design and by defaut* » et de transparence semblent ignorés et contournés par le modèle économique actuel. Une transparence efficace signale non seulement l'existence d'une menace pour les droits du destinataire, mais aussi son ampleur. Un consentement éclairé nécessite également une volonté d'être informé de la part de la personne concernée. La liberté tient aussi dans le besoin de contrôler et s'approprier les modalités de traitement. Un consentement collectif pourrait constituer une piste d'une acceptation plus libre et informée des traitements de données personnelles de la ville intelligente.

Par ailleurs, la numérisation de la ville, pensée et réalisée de manière analogue à la numérisation des entreprises, favorise-t-elle l'épanouissement des individus et contribue-t-elle au bien vivre ensemble, à leur bonheur et à leur santé ? Est-il souhaitable de vivre dans un espace public (place de jeu, ...) géré comme une entreprise[134] ? Ces questions montrent à quel point l'information et la liberté du choix de la personne concernée à l'ère de la généralisation du numérique constituent le défi de demain.

[132] Considérant 43 RGPD.

[133] R. Neisse, G. Baldini, G. Steri, Y. Miyake, S. Kiyomoto, et A. R. Biswas, *An Agent-based Framework for Informed Consent in the Internet of Thing*, 1.

[134] S. Ghernaouti, *De quelles villes numériques voulons-nous ?…et qui le décide pour nous ?*, dans *Blog - Le Temps*, 2018, disponible sous : https://blogs.letemps.ch/solange-ghernaouti/2018/09/25/de-quelles-villes-numeriques-voulons-nous-et-qui-le-decide-pour-nous/.