Données personnelles

Les risques liés aux *Smart Cities*[1]

-

***Expertises des systèmes d'information*, n° 422, mars 2017, pp. 103-107**

MOURON Philippe
Maître de conférences HDR en droit privé
LID2MS – Aix-Marseille Université

Les *Smart Cities* sont porteuses de multiples espoirs. Ces « villes intelligentes » tendent à utiliser les ressources que procurent les technologies de l'information et de la communication pour améliorer la gestion et le développement des espaces urbains. L'objectif est de parvenir à un meilleur cadre de vie, une meilleure gestion des flux de population, des services qui peuvent être déployés et des risques environnementaux.

Il serait vain ici de lister tous les projets existants ou à venir, tant leur diversité est grande. Ceux-ci peuvent être regroupés en grands domaines[2]. Le domaine des transports (*Smart Transportation*)[3], et plus généralement des déplacements urbains, a été l'un des premier appréhendé, notamment au titre des systèmes de transport intelligents[4]. Des applications permettront de signaler en temps réel les points d'engorgement et éventuels accidents aux automobilistes et utilisateurs des transports en commun. Le développement prochain de routes et de voitures connectées ou autonomes étendra cette capacité à des espaces non urbains. L'implémentation obligatoire du système *eCall* sur les véhicules à partir de 2018 en constitue

[1] Cet article est la version écrite d'une communication orale présentée lors du colloque *Droit du numérique : Smart Cities, intelligence artificielle et Blockchain*, organisé par l'Association Française de Droit de l'Informatique et de la Télécommunication, organisé à Aix-en-Provence le 2 décembre 2016 ; nous remercions les organisateurs de nous en avoir permis la publication

[2] Voir not. : BATTY M. et *ali.*, « Smart cities of the future », *Eur. Phys. J. Special Topics*, n° 214, 2012, pp. 482-486; GIFFINGER R. et *ali.*, « Smart Cities Profiles », Deliverable 2.1, P.1, introduction, *Planning for Energy Efficient Cities*, May 2014, 7p. ; PAN G. et *ali.*, « Trace Analysis and Mining for Smart Cities: Issues, Methods, and Applications », *IEEE Communications Magazine*, June 2013, pp. 124-126

[3] GLANCY D. J., « Sharing the Road : Smart Transportation Infrastructure », *Fordham Urb. L. J.*, Vol. 41, n° 5, 2015, pp. 1617-1664

[4] Voir not. Directive 2010/40/UE du Parlement européen et du Conseil concernant le cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres modes de transport

déjà un bon exemple[5]. Sur le long terme, ces données intéresseront aussi les pouvoirs publics au niveau des plans de circulation, et leurs permettront de prendre des décisions plus adaptées en fonction de la démographie des transports (*Smart Urban Planning*). D'autres projets garantiront une meilleure gestion des déchets, notamment à travers des poubelles et bornes de tri connectées, qui permettront là encore de mesurer immédiatement les volumes à gérer quartier par quartier. Il en est de même dans le secteur de l'énergie (*Smart Energy*), avec des systèmes d'éclairage public intelligents, lesquels pourront signaler instantanément toute défaillance ou adapter leur intensité à la circulation réelle relevée sur la voirie. La pose de compteurs intelligents aux domiciles des particuliers poursuivra les mêmes finalités d'économie d'énergie, avec une adaptabilité des tarifs. La dimension environnementale, touchant à la santé et la salubrité publiques (*Smart Health*), sera ainsi essentielle dans les *Smart Cities*. On ne saurait non plus négliger l'intérêt de ces projets pour la sécurité publique. Les données recueillies peuvent permettre de dresser des statistiques sur le niveau de délinquance urbaine dans certains secteurs. Leur utilisation pourra contribuer à de meilleures politiques de répression, en facilitant l'identification des auteurs d'infractions. Le développement des véhicules connectés et des systèmes de lecture automatique de plaques d'immatriculation en atteste parfaitement. Au-delà, c'est même la prévention des troubles à l'ordre public et des infractions qui pourra profiter de ces nouvelles technologies (*Smart Security*). Enfin, on peut imaginer la multitude de services commerciaux qui pourront se développer en profitant de ces données, en garantissant une rapidité d'exécution (*Smart Commerce*).

Pour toutes ces raisons, les *Smart Cities* représentent un nouveau mode de gouvernance (*Smart Governance*), permettant de mieux comprendre et d'anticiper les problématiques urbaines, à travers des analyses en temps réel, et d'y apporter des solutions garantissant un développement harmonieux[6]. Leur développement nécessitera la collaboration de très nombreux acteurs, qu'il s'agisse des pouvoirs publics, des entreprises, des chercheurs ou encore des habitants eux-mêmes[7]. A ce titre, elles génèrent de multiples problématiques juridiques, qui intéressent notamment la gouvernance des projets, l'urbanisme et l'aménagement, la santé publique. La

[5] Règlement (UE) 2015/758 du Parlement européen et du Conseil du 29 avril 2015 concernant les exigences en matière de réception par type pour le déploiement du système *eCall* embarqué fondé sur le service 112 et modifiant la directive 2007/46/CE

[6] BATTY M., *op. cit.*, pp. 492-496

[7] COSGRAVE E., ARBUTHNOT K. et TRYFONAS T., « Living Labs, innovation Districts and information Marketplaces : A Systems Approach For Smart Cities », *Procedia Computer Science*, Vol. 16, 2013, pp. 668-677

standardisation et l'interopérabilité des données sont aussi au cœur des préoccupations, car elles garantiront la viabilité des projets[8], tout comme les questions de responsabilité[9].

Mais c'est avant tout au niveau du droit des données personnelles que se posent le plus d'interrogations. En effet, dans cette perspective, la dimension individuelle des habitants va se trouver intimement liée à la dimension collective de l'aménagement urbain et des politiques de la ville, en passant par la dimension commerciale des entreprises qui développeront ces nouveaux services intelligents. Celles-ci sont d'autant plus essentielles que ce niveau constitue la base même des projets de *Smart Cities*. Finalement, celles-ci ne font que renouveler des problématiques déjà bien connues, liées à l'internet des objets, au *Big Data* ou au *Cloud Computing*[10]. Toutefois, elles les amplifient pour les porter à l'échelle des aires urbaines, en croisant les intérêts des sphères privées et publiques.

Un rapide tour d'horizon permet de révéler les difficultés que posent de tels projets pour le respect de ces prérogatives et des obligations des responsables de traitements (I). Des solutions juridico-techniques peuvent néanmoins être envisagées afin de garantir cette viabilité des *Smart Cities* (II).

I. Les risques de surveillance de masse dans les *Smart Cities*

Le concept de *Smart Cities* repose sur une interconnexion automatique des fichiers de données (A). Cela remet en cause un certain nombre de principes protecteurs des données personnelles, et réveille la crainte d'une surveillance de masse (B).

A. L'interconnexion technique des fichiers de données nécessaires au fonctionnement des *Smart Cities*

Du point de vue technique, les *Smart Cities* sont vouées à reposer sur un écosystème d'objets connectés (1), organisés dans une structure « bottom-up » de type pyramidal[11] (2).

[8] Voir not. Décision (UE) n° 2016/209 de la Commission du 12 février 2016 relative à une demande de normalisation adressée aux organismes européens de normalisation en ce qui concerne les systèmes de transport intelligents dans les zones urbaines

[9] S'agissant des voitures autonomes, voir : CHOMIAC DE SAS X., « Un droit autonome pour les voitures autonomes », *RLDI*, n° 133, janvier 2017, pp. 52-56, et GOLA R., « L'adaptabilité de la règle de droit face à l'émergence des véhicules connectés et autonomes », *RLDI*, n° 133, janvier 2017, pp. 57-61

[10] EDWARDS L., « Privacy, Security and Data protection in Smart Cities », *Eur. Data Prot. L. Rev.*, Vol. 2, Issue 1, 2016, pp. 28-29 et pp. 44-46

[11] CRENN J.-P., « Les objets connectés décryptés pour les juristes », *Dalloz IP/IT*, septembre 2016, pp. 389-393

1) Un écosystème d'objets connectés comme socle des Smart Cities

Au niveau le plus bas, une multitude de capteurs placés sur des objets connectés, mobiliers ou immobiliers, vont recueillir toutes sortes de données en temps réel[12].

Celles-ci pourront être collectées directement auprès des personnes, à travers les multiples objets qu'elles emploient au quotidien (smartphones, véhicules,…). S'ajouteront à cela toutes les données collectées par les capteurs implémentés dans les espaces publics. D'autres données pourront encore être volontairement communiquées par les habitants, via des applications comme celles que l'on trouve sur les smartphones (mais qui pourront être étendues à d'autres objets connectés). Enfin, des données publiques, disponibles en *Open data*, pourront aussi participer des projets de *Smart Cities* à des degrés variés. Elles seront ensuite intégrées, analysées et formalisées de façon à entraîner une prise de décision propre à chaque traitement. Celle-ci pourra être automatisée, si le système est à même de renvoyer des informations adéquates aux utilisateurs ; tel serait le cas, par exemple, dans le domaine des transports avec le suivi du trafic et le signalement des accidents, retards,...

Comme nous l'avons relevé, il ne s'agit à ce stade que d'une nouvelle application des possibilités offertes par l'internet des objets[13].

2) La pyramide des traitements comme structure des Smart Cities

Aux niveaux supérieurs, ces mêmes données pourront être analysées pour de nouvelles finalités, y compris en étant croisées et regroupées avec celles qui ont été recueillies par d'autres capteurs.

Des utilités communes à des objets développés de façon séparée pourraient *a posteriori* être découvertes à travers le croisement de leurs données. La plupart de ces usages secondaires n'ont pas forcément été pensés lors de la collecte[14]. Tel est le cas, par exemple, des données de géolocalisation déjà collectées par un certain nombre d'appareils tels que les smartphones, qui peuvent être couplées à d'autres types de données afin d'être mieux contextualisées. Les données relatives à la circulation routière peuvent ainsi être corrélées à celles qui concernent l'utilisation des transports en commun, afin d'examiner les flux existant entre différents quartiers d'une même aire urbaine, en fonction de leur nature (trajets professionnels, de loisirs,…). L'affinage de ces données intéresse également les entreprises au titre de la publicité ; des offres commerciales ciblées peuvent ainsi être délivrées instantanément et *in situ* aux habitants en fonction de leur géolocalisation, leur proximité de certains établissements, leurs habitudes de vie ayant été préalablement analysées. Le recours à des technologies de

[12] PAN G., *op. cit.*, pp. 120-126

[13] PERERA C. et *ali.*, « Sensing as a service model for smart cities supported by Internet of Things », *Trans. Emerging Tel. Tech.*, Vol. 25, Issue 1, 2014, pp. 81-93 ; ZANELLA A. et *ali.*, « Internet of Things for Smart Cities », *IEEE Internet of things Journal*, Vol. 1, n° 1, 2014, pp. 22-32

[14] MAYER-SCHOENBERGER V. et CUKIER K., *Big Data : A Revolution That Will Transform How We Live, Work and Think*, Eamon Dolan, 2013, p. 153

communication sans contact permettra aux objets connectés de communiquer entre eux des informations, ce qui augmentera la rapidité de traitement. Pour cette raison, l'interopérabilité, la standardisation des données et la capacité d'interconnexion des capteurs devront être anticipées dès leur conception. Ce sera même l'un des objectifs de ces projets que de garantir un échange instantané et automatique d'informations, afin d'en extraire une analyse le plus rapidement possible.

Au vu de la diversité des objets connectés et de la nature des données qu'ils peuvent recueillir, des centaines d'utilités pourraient être tirées des traitements secondaires. Les croisements de données peuvent ainsi se multiplier et se hiérarchiser de façon pyramidale, les pouvoirs publics et les entreprises étant intéressés aux niveaux les plus élevés. *In fine,* dans les perspectives les plus lointaines que l'on puisse imaginer, chaque ville pourra être cartographiée instantanément à travers toutes ces séries de traitements qui, au final, seraient absorbées dans un même ensemble. On peut se demander à qui, de tous les acteurs impliqués, appartiennent les données en cause dans ces projets[15]… sans oublier qu'elles incluront une part substantielle de données personnelles.

C'est là qu'un certain nombre d'enjeux juridiques font leur apparition.

B. Les risques des *Smart Cities* au regard de la protection des données personnelles

En dépit de leurs objectifs louables, les projets liés aux *Smart Cities* permettront potentiellement de dresser un véritable réseau social des données à l'échelle d'une ville (1), ce qui met en cause la protection des données personnelles (2).

1) De la réidentification des personnes à la surveillance de masse

Les données recueillies au niveau le plus bas, si anonymes soient-elles au début du traitement, pourront donner lieu à une exploration très précise, et permettre de réidentifier les individus par les multiples croisements dont elles vont faire l'objet[16].

Les données de géolocalisation, tout comme celles qui relèvent d'applications mobiles permettront d'affiner très précisément les profils des habitants, ainsi que leurs habitudes de déplacement, de consommation et de comportement dans l'espace urbain[17]. Le croisement avec des données issues des réseaux sociaux sera à ce titre particulièrement utile, dès lors qu'elles reflètent en elles-mêmes les habitudes de vie d'un individu. Elles permettront également de mieux connaître ses relations sociales. La présence physique de plusieurs personnes en un même lieu pourra ainsi être relevée à travers les données physiques collectées par les capteurs,

---

[15] EDWARDS L., *op. cit.*, pp. 33-34

[16] OHM P., « Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization », *UCLA Law Review*, Vol. 57, Issue 6, 2010, pp. 1701-1777

[17] GLANCY D. J., *op. cit.*, p. 1658

et être recoupées avec ces données relationnelles. A défaut, elles serviront quand même pour tracer des relations éventuelles entre personnes qui ne se connaissent pas forcément. Cela explique aussi que celles qui n'utilisent pas d'objets connectés ou d'applications de géolocalisation pourraient quand même être réidentifiées dans la masse des données traitées. Chaque habitant pourra être « suivi » malgré lui en parcourant la ville, loin de l'anonymat que la foule pouvait garantir dans les grands ensembles. La frontière entre la vie privée et la vie publique s'en trouve abolie. Celle-ci deviendrait un véritable « Metropticon »[18], où chacun serait surveillé sans le savoir avec une précision microscopique. Ces traitements pourraient révéler un important potentiel discriminatoire, en ce qu'il permettrait de remonter le parcours de populations entières issues d'un même quartier.

Certains auteurs craignent même les réactions des gouvernements et pouvoirs publics locaux qui disposeront de ces informations, et pourront mettre en œuvre des politiques fondées sur la surveillance de masse avec un fort potentiel discriminatoire ou « paternaliste »[19].

2) Le droit des données personnelles confronté aux Smart Cities

Ces conséquences interrogent sur la conformité de ces traitements automatisés à la loi du 6 janvier 1978.

Les droits des personnes dont les données sont collectées sont ainsi menacés, pour des raisons logiques. Le respect du droit au consentement préalable, des droits d'accès et de rectification, ainsi que du droit d'opposition à la poursuite du traitement s'avère peu compatible avec les objectifs des *Smart Cities*, qui exigent une rapidité d'exécution et de croisement des données. Cela est d'autant plus vrai au regard des multiples traitements secondaires, parfois non prévus à l'origine, qui s'ajouteront à ceux effectués directement auprès des personnes, et qui auront parfois pour effet de les réidentifier. Cela justifierait pourtant d'obtenir un nouveau consentement, avec le risque que les responsables invoquent un intérêt légitime leur permettant de passer outre. Ces mêmes difficultés se posent au niveau du respect des obligations qui sont mises à leur charge. Tel est le cas de l'information préalable qui doit être communiquée aux personnes dont les données sont collectées, y compris de façon indirecte, en leur indiquant notamment les types de données utilisées, les finalités poursuivies, ou encore l'identité des responsables de traitements. La multitude de capteurs qui pourront être déployés, la multiplication et la mutualisation des traitements *a posteriori*, pour des nouvelles finalités, rendent bien illusoire cette information dès le stade de la première collecte. Du moins, elle nécessiterait des efforts disproportionnés à ce stade, ce qui permettrait d'en exonérer les responsables selon la loi. Cela interroge également sur le respect du principe de proportionnalité, ou de « minimisation », selon lequel les collectes doivent être limitées aux

[18] FINCH K. et TENE O., « Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town », *Fordham Urb. L. R.*, Vol. 41, Issue 5 (October 2014), pp. 1581-1616

[19] FINCH K. et TENE O., *op. cit.*, pp. 1595-1606 (évoquant l'exemple d'escalators « intelligents » qui pourront cesser de fonctionner selon la corpulence de l'utilisateur, l'invitant à plus d'efforts !)

seules données qui sont nécessaires aux finalités prévues. En admettant que ce principe soit respecté au premier niveau, les croisements ultérieurs dont elles peuvent faire l'objet pour de nouvelles finalités Cette considération intéresse aussi la durée de conservation des données, qui doit normalement être limitée. Or l'intérêt que présentent les usages secondaires explique qu'elles puissent être enregistrées pour des durées dépassant celle du premier traitement. Encore une fois, ces risques avaient déjà été identifiés au niveau des objets connectés[20]. Enfin, le recours à des systèmes de *Cloud Computing* interroge aussi sur les garanties à mettre en œuvre lorsque les données seront stockées hors d'un Etat de l'Union européenne.

De façon plus générale, la sécurisation des fichiers est également mise en cause. Les risques d'atteintes sont d'autant plus élevés en raison de leur interconnexion. Une seule intrusion malveillante, à un point du réseau, suffirait pour accéder à l'intégralité de celui-ci, ou du moins avoir des répercussions à grande échelle. Un simple bug informatique, altérant les données traitées, pourrait aussi impacter tous les autres traitements, et fausser finalement l'ensemble des analyses qui en sont tirées. La vulnérabilité des objets connectés contre les attaques informatiques, et les risques qu'ils génèrent à l'égard de la vie privée, ont déjà pu être dénoncés[21]. Ils prennent désormais de nouvelles proportions à l'échelle des *Smart Cities*. Enfin, cette vulnérabilité peut aussi être relevée au niveau de leur consommation énergétique. Une panne d'électricité, même localisée, pourrait stopper le fonctionnement d'un certain nombre de capteurs (et avec eux de traitements). Au-delà de l'intégrité des données et du respect de la vie privée, c'est la sécurité physique des personnes qui pourrait ainsi être mise en cause. Tel serait le cas, par exemple, avec la défaillance ou le piratage d'un système de traitement des données de circulation routière, dont les automobilistes seraient dépendants. Derrière les prouesses techniques, on ne doit pas oublier que les services que rendront les *Smart Cities* intéressent des personnes et des situations bien réelles.

Leur avenir ne sera viable qu'au prix de garanties protectrices des prérogatives et droits extrapatrimoniaux dont les citoyens disposent sur leurs données. Une « *Smart Privacy* »[22] est à construire…

---

[20] DE SILGUY S., « Les objets connectés, un risque pour la protection de nos données personnelles », *RLDC*, n° 119, octobre 2014, pp. 66-69 ; FOREST D., « Qui a peur de l'"Internet des objets" ? », *RLDI*, n° 54, novembre 2009, pp. 45-46 ; EDWARDS L., *op. cit.*, pp. 41-42

[21] Voir not. : Groupe de travail « article 29 » sur la protection des données, avis 8/2014 sur les récentes évolutions relatives à l'internet des objets, adopté le 16 septembre 2014

[22] FINCH K. et TENE O., *op. cit.*, pp. 1606-1615

II. La nécessité de penser une « *Smart Privacy* » pour les *Smart Cities*

Le règlement européen du 27 avril 2016 sur la protection des données personnelles prévoit de nouvelles obligations à l'égard des responsables de traitements qui seraient particulièrement adaptées pour le développement des *Smart Cities*. Tel est le cas des principes dits de « *Privacy by Design* » et « *Privacy by Default* » (A). D'autres obligations peuvent s'avérer particulièrement pertinentes pour la transparence des traitements de données (B).

A. *Smart Cities, Privacy by Design* et *Privacy by Default*

Le renforcement des droits des personnes sur leurs données ne fait pas disparaître les limites auxquelles va se heurter leur exercice dans les *Smart Cities* (1). La solution se doit d'être de même nature que le problème : technique. C'est l'un des objectifs qui peut être atteint avec les deux principes précités (2).

1) Les limites aux droits des personnes dans l'environnement technique des Smart Cities

Les droits des personnes sur leurs données sont certes renforcés et enrichis de nouvelles prérogatives, telles que le droit à l'effacement ou à la portabilité des données.

Si ces droits seront théoriquement opposables aux traitements mis en œuvre par les *Smart Cities*, ils se heurtent néanmoins aux mêmes difficultés techniques que celles qui ont été précédemment relevées. Le texte laisse d'ailleurs certaines latitudes aux responsables de traitements à ce niveau. Par exemple, si le consentement préalable doit être donné d'une façon « éclairée et univoque » (art. 4, § 11), et en respectant certaines exigences en termes de présentation (art. 7), il n'est pas exclu qu'il puisse être donné de façon implicite, et résulter d'un simple « comportement » de la personne (cons. n° 32)[23]. Le fait de ne pas avoir paramétré les capteurs et objets connectés, et donc de les laisser échanger des informations avec d'autres capteurs situés dans les lieux publics, pourrait-il être considéré comme manifestant le consentement de la personne dans l'environnement d'une *Smart City* ? De même, si le devoir d'information préalable a été précisé par le règlement, y compris dans les cas où les données ne sont pas collectées directement auprès des personnes (art. 13 et 14), sa mise en œuvre reste toujours aussi incertaine au vu des potentialités que présentent les usages ultérieurs. En fait, la dilution des données dans la masse des traitements mis en œuvre reste le principal effet pervers à enrayer, car elle met en cause même l'objet même de ces droits.

Aussi, la solution devrait davantage se porter sur le renforcement des obligations des responsables de traitements, à la fois sur le plan juridique et technique.

[23] METALLINOS N., « Les apports du règlement général relatif à la protection des données personnelles sur les conditions de licéité des traitements », *Dalloz IP/IT*, décembre 2016, pp. 588-591

2) La nécessaire mise en œuvre d'une solution juridico-technique dans l'environnement des Smart Cities

C'est à ce niveau que le règlement présente un apport significatif pour les *Smart Cities,* en cherchant à responsabiliser davantage les concepteurs quant au respect du droit des données personnelles.

Tel est le cas avec les principes dits de « protection des données dès la conception » (*Privacy by Design*) et de « protection des données par défaut » (*Privacy by Default*), visés à l'article 25 du règlement. Selon le premier de ces principes, le responsable du traitement doit prévoir, dès la conception de celui-ci, des mesures techniques et organisationnelles, « telles que la pseudonymisation », qui garantissent le respect des droits des personnes et des autres obligations mises à sa charge. La minimisation de la collecte est également exigée au titre du second principe, dans la continuité du principe de proportionnalité. *In fine*, l'article 25 obligera à prendre en compte la protection des données personnelles tout au long du cycle de vie des technologies, au stade même de la création, et non seulement à celui de la commercialisation[24]. Les capteurs, objets connectés et leurs interfaces de communication devront ainsi être conçus en fonction de toutes les contraintes légales, et notamment celles qui sont prévues par le règlement. C'est ainsi, par exemple, que la sécurisation des données (art. 32) et la limitation de leur durée de conservation (art. 5) devront être garanties par des dispositifs techniques, lesquels font d'ailleurs l'objet d'autres attentions dans le règlement. Cette exigence se situe donc en amont des traitements, et permettra certainement de mieux les anticiper. La rencontre entre les standards techniques et juridiques suppose de sensibiliser davantage les concepteurs et ingénieurs chargés de la création de ces produits, y compris au stade de leur formation. L'innovation est quand même de taille dans le secteur, car on constate trop souvent que ces objets ont été développés par des techniciens peu au fait du droit qui leur est applicable[25]. C'est une première mission « civilisatrice » qui doit continuer d'être menée, confortant une approche globale des *Smart Cities*, à la fois technique, économique et juridique.

Au-delà de ces aspects, qui intéressent les responsables de traitements, la mise en œuvre de l'article 25 doit se traduire par la mise à disposition d'outils concrets au profit des personnes, afin qu'elles puissent prendre le contrôle de leurs données. C'est à ce niveau que le renforcement des prérogatives individuelles prend tout son sens, mais jette aussi un défi technique. S'il est certain, sur la base du principe de *Privacy by Default*, que les traitements effectués devront s'efforcer d'être anonymes, et se limiter à de simples informations brutes, les risques de réidentification exigeant quand même que la personne soit dûment informée de l'existence et de la teneur des traitements. Mais comment garantir une parfaite information des usagers quant aux traitements déployés à l'échelle des *Smart Cities*, ainsi que l'exercice de leurs droits ? La multiplication des points d'accès à l'information par des moyens clairs et simples

[24] DARY M. et BENAISSA L., « *Privacy by Design* : un principe de protection séduisant mais complexe à mettre en œuvre », *Dalloz IP/IT*, octobre 2016, pp. 476-480

[25] EDWARDS L., *op. cit.*, p. 51

(par exemple à travers des QR codes implantés sur les objets connectés) est bien sûr envisageable. Il en serait de même avec des systèmes de notifications ou d'alertes, qui se mettraient en marche à chaque connexion et échange d entre capteurs. Toutefois, ces mécanismes risqueraient d'avoir un effet extrêmement fastidieux pour l'utilisateur, obligé de se connecter de manière répétitive. Il serait alors aisé de profiter de sa lassitude et de son inertie pour passer outre. La solution idéale serait de développer un système unique, centralisant l'ensemble des informations afférentes aux traitements mis en œuvre[26]. Cela permettrait à l'utilisateur de paramétrer à l'avance ses préférences pour tous ses objets connectés. Ceux-ci seraient dès lors configurés de façon permanente, donc y compris dans leurs interactions avec d'autres capteurs et objets, qui peuvent être placés dans des lieux publics. Le consentement de la personne pourrait alors être clairement exprimé, et conditionner la mise en œuvre d'une pluralité de traitements. Au-delà, le même système devra lui permettre d'exercer son droit d'opposition, par exemple si elle ne souhaite pas être « traquée » dans certains lieux, ou certains déplacements. Elle exercerait alors un véritable droit au « silence des puces » lui permettant de se déconnecter de l'environnement réseau à tout moment[27]. L'exercice de ce droit pourrait bien sûr être différencié selon le type de traitement, voire même être rendu impossible, par exemple si celui-ci est nécessaire dans un but de sécurité publique (art. 23).

L'ambition est forte, mais il reste à concevoir un tel système, avec la capacité d'être embarqué, ce qui pourrait prendre la forme d'une application mobile. La gestion des données personnelles serait ainsi totalement décentralisée. Dans un mouvement de « Self Data », il appartiendrait aux individus de s'en soucier directement[28]. De ce point de vue, la *Smart City* s'apparente bien à un réseau social, dès lors que les personnes devront paramétrer à l'avance le partage de leurs informations !

B. Les autres obligations prévues par le règlement intéressant les *Smart Cities*

D'autres obligations générales à la charge des responsables de traitement pourront efficacement être mises en œuvre dans le cadre des *Smart Cities*. Tel est le cas avec l'encadrement des usages secondaires (1) et les exigences relatives à la transparence des traitements de données (2).

1) La compatibilité des traitements secondaires avec le consentement initial de la personne

La centralisation des informations auprès de l'utilisateur fournira une base juridique à la pyramide des traitements qui seront mis en œuvre dans les *Smart Cities*.

---

[26] EDWARDS L., *op. cit.*, pp. 54-55

[27] Communication du 18 juin 2009 de la Commission au Parlement européen, au Conseil, Comité économique et social européen et au Comité des régions - L'internet des objets : un plan d'action pour l'Europe /* COM/2009/0278 final

[28] ZOLYNSKI C. et *ali.*, « La *Privacy by Design* : une fausse bonne solution aux problèmes de protection des données personnelles ? », *LP*, n° 340, juillet-Août 2016, pp. 401-402

Si le consentement de la personne devra être recherché dans la mesure du possible, le règlement n'a pas exclu quelques assouplissements pour les usages ultérieurs de données. L'article 6 § 4 vise spécifiquement la situation où des données vont être traitées pour une autre fin que celle de leur collecte initiale, et sans le consentement de la personne. Un test de compatibilité devra ainsi être respecté, afin de vérifier les liens existants entre les finalités du premier et du second traitement, le contexte dans lequel les données ont été collectées, la nature de celles-ci et les conséquences que pourraient avoir le nouveau traitement. Enfin, ce test exige du responsable qu'il mette en œuvre des garanties à l'égard des données, lesquelles peuvent inclure le chiffrement ou la pseudonymisation. A défaut, le consentement de la personne devra à nouveau être recherché. C'est là une dérogation importante en faveur du *Big Data*[29], mais qui sera aussi utile pour les *Smart Cities*.

Il reste à savoir comment seront appréciés les liens entre les finalités des traitements, ce qui ne sera pas une mince affaire au titre de leur potentielle diversité.

2) Un renforcement de la transparence des traitements de données

Le règlement tend également à renforcer la sécurité et la transparence des traitements de données. Outre les exigences de l'article 24, plusieurs mesures intéressant les projets de S*mart Cities* devront ainsi être respectées.

La désignation de responsables conjoints (art. 26), ainsi que l'encadrement strict de la sous-traitance (art. 28 et 29) permettront normalement d'éviter la divagation ou le croisement de fichiers non conformes aux exigences du règlement. A cela s'ajoute la nécessité de tenir un registre des activités de traitement, consignant l'ensemble des informations afférentes à celles-ci (catégories de données, durée de conservation, finalités,…), ainsi que les opérations ayant été effectuées à l'égard d'un fichier de données, qu'il s'agisse du responsable principal ou d'un sous-traitant (art. 30). La coopération dans la tenue des informations est également prévue (art. 31). Cette mise en œuvre du principe d'*Accountability* se traduit par un régime basé sur une plus grande responsabilité des responsables de traitement, ce qui semble être la solution la plus adaptée à l'environnement des *Smart Cities*. S'agissant de la sécurité, l'article 33 obligera ces mêmes responsables à signaler toute faille aux autorités nationales de contrôle, dans de très brefs délais, si celle-ci est susceptible de porter atteinte à des fichiers de données personnelles. Ils devront également en rendre compte devant les personnes concernées, selon l'article 34, à moins qu'ils aient mis en œuvre des mesures techniques ou organisationnelles limitant l'impact de cette faille dans l'immédiat ou dans l'avenir.

Enfin, l'article 35 impose la nécessité de mettre en œuvre des études préalables à chaque nouveau type de traitements. Celles-ci sont notamment rendues obligatoires si les opérations vont porter sur le profilage d'individus pour la prise de décision automatisée, ou la surveillance systématique à grande échelle d'une zone accessible au public. Il est précisé qu'une seule étude

[29] METALLINOS N., *op. cit.*, p. 591

pourra couvrir une pluralité de traitements, l'objectif étant de mesurer les risques que ceux-ci présentent pour les droits et libertés des personnes, ainsi que les garanties techniques à mettre en œuvre afin de respecter les obligations prévues par le règlement. C'est là un dispositif particulièrement pertinent pour l'avenir des *Smart Cities*, alors même que la plupart de leurs utilités restent à découvrir.

****

Le règlement européen offre donc un certain nombre de garanties qui pourront être utilement mises en œuvre dans les villes intelligentes, propres à garantir une certaine transparence vis-à-vis des utilisateurs. C'est là un élément déterminant au vu du caractère potentiellement intrusif de ces projets. Quand bien même leur utilité serait grande, et leurs garanties suffisantes, la réticence psychologique de la population à se laisser « ficher » de la sorte est un facteur à prendre en considération.

Aussi, il est déjà proposé d'aller plus loin pour parer ce risque. La participation et la responsabilisation des habitants pourraient ainsi être encouragées en recourant à des modèles d'innovations ouvertes. Tel serait le cas avec des applications leur permettant d'alimenter eux-mêmes les données à traiter. La collecte de données au niveau le plus bas pourrait ainsi reposer sur la collaboration active des usagers. Cela serait un complément utile au mouvement d'ouverture des données publiques. Cette participation des utilisateurs finaux pourrait être encore plus active, et reposer sur la création collaborative des outils, interfaces et applications, notamment à travers les activités des laboratoires vivants[30]. Ceux-ci pourraient être développés sur la base de modèles *Open Source* ou *Open Hardware*. Ces pratiques peuvent renforcer la confiance des habitants d'une *Smart City*. Ils seront plus à mêmes d'en contrôler le fonctionnement et le développement, ce qui semble d'autant plus logique qu'ils en constituent le socle fondamental. De plus, elles s'insèrent dans la continuité du mouvement précité de « Self Data », en donnant aux personnes les moyens d'un parfait contrôle de leurs données et de leur environnement. Les *Smart Cities* ne peuvent donc reposer exclusivement sur les initiatives des pouvoirs publics et des entreprises privées. Elles doivent aussi se nourrir des initiatives citoyennes.

Plus qu'intelligentes, les villes du futur se doivent d'être démocratiques et ouvertes.

[30] FINCH K. et TENE O., *op. cit.*, pp. 1609-1611 ; SCHAFFERS H. et ali., « Smart Cities and the Future Internet : Towards Cooperation Frameworks for Open Innovation », *The Future Internet - Future Internet Assembly 2011: Achievements and Technological Promises*, Springer, 2011, pp. 431-445; SCHUURMAN D. et ali., « Smart ideas for Smart Cities: Investigating Crowdsourcing for Generating and Selecting Ideas for ICT Innovation in a City Context », *Journal of Theoretical and Applied Electronic Commerce Research*, Vol. 7, Issue 3, December 2012, pp. 49-62