La protection des données personnelles dans l'environnement urbain - De la mesure d'audience publicitaire aux villes intelligentes

Philippe Mouron

La protection des données personnelles dans l'environnement urbain

De la mesure d'audience publicitaire aux villes intelligentes

-

***Revue Lamy Droit de l'Immatériel*, n° 139, juillet 2017, pp. 54-60**

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

Les villes sont-elles vouées à devenir des réseaux sociaux à ciel ouvert ?

La réponse pourrait bien être positive, au vu de la profusion d'objets connectés et de capteurs installés dans les espaces urbains au titre de ce que l'on appelle les « villes intelligentes », ou « *Smart Cities* ». L'utilisation massive des technologies de l'information et de la communication dans les lieux publics permettrait d'améliorer la gestion et le développement de ces espaces, avec de multiples objectifs : meilleure gestion des flux de circulation, de l'enlèvement des déchets et de la salubrité publique, prévention des accidents, des risques environnementaux, rapidité d'exécution des services, prévision accrue des risques pour les populations, management de la sécurité en temps réel,... L'installation de feux de circulation « intelligents », qui pourront adapter leur fonctionnement en fonction de la quantité et du type de véhicules (voitures, vélos, bus, …), en est un bon exemple[1]. Le domaine des transports et de la voirie urbaine est à ce titre l'un des plus prometteurs en la matière[2]. Ces mêmes systèmes permettront sur le long terme de mieux anticiper la planification urbaine. Le secteur privé y trouvera aussi son compte en profitant de ressources non négligeables pour mieux affiner de nouveaux services et de nouvelles formes de publicités. Google tend déjà optimiser ses publicités en ligne en fonction des achats effectués dans les magasins[3]. En général, la finalité

[1] BURGESS K., « Green Light for Traffic Signals that Give Priority to Buses and Bicycles », *The Times*, May 16 2017

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

[3] « Google Helps Advertisers Track Spending in Physical Stores », *The New York Times*, May 23 2017

des villes intelligentes est d'améliorer le cadre de vie dans les métropoles à tous les niveaux, ce qui présente un grand intérêt autant pour les pouvoirs publics que pour les entreprises privées[4]. Néanmoins, les systèmes mis en œuvre au titre de ces projets fonctionneront sur la base de collecte et d'échange automatisés de données qui peuvent provenir des personnes physiques. Des garanties techniques devront donc être mises en œuvre pour limiter les capacités d'identification des personnes.

C'est ce que la Commission nationale de l'informatique et des libertés (CNIL) a fort justement rappelé à l'entreprise JC Decaux. Le traitement litigieux avait pourtant une portée assez limitée, ce qui rend la décision encore plus exemplaire. Précisément, il s'agissait d'un dispositif de comptage des flux de piétons sur la dalle de La Défense. Le traitement était effectué à l'aide de plusieurs boîtiers de comptage wifi, installés sur les mobiliers publicitaires, et censés capter les adresses des téléphones mobiles présents dans un rayon de 25 mètres. Le but était d'établir des statistiques quant au volume de fréquentation, au taux de répétition des mêmes personnes et à leurs déplacements. Le traitement, à vocation expérimentale, n'aurait eu qu'une durée de quatre semaines. L'autorisation d'y procéder sera refusée par la CNIL, dans une délibération du 16 juillet 2015[5], car le procédé d'anonymisation mis en œuvre par JC Decaux se révélait insuffisant pour écarter tout risque de réidentification des personnes. Les données conservant un caractère personnel, une information plus explicite devait de plus leur être transmise. Le Conseil d'Etat, saisi par l'entreprise, a confirmé la décision de la Commission dans un arrêt du 8 février 2017[6].

Cette décision met en relief les difficultés et surtout les risques que présentent les projets des *Smart Cities* pour la protection des données personnelles[7]. Le risque d'identification ou de

[4] BATTY M. et *ali.*, « Smart cities of the Future », *Eur. Phys. J. Special Topics*, n° 214, 2012, pp. 482-486 ; PAN G. et *ali.*, « Trace Analysis and Mining for Smart Cities: Issues, Methods, and Applications », *IEEE Communications Magazine*, June 2013, pp. 124-126

[5] Délibération n° 2015-255 du 16 juillet 2015 refusant la mise en œuvre par la société JC Decaux d'un traitement automatisé de données à caractère personnel ayant pour finalité de tester une méthodologie d'estimation quantitative des flux piétons sur la dalle de La Défense

[6] CE, 10ème et 9ème Ch. Réunies, 8 février 2017, n° 393714, *RLDI*, n° 135, mars 2017, pp. 22-25, note E. Drouard et C. Marolla, *CCE*, avril 2017, pp. 41-42, obs. N. Metallinos

[7] KITCHIN R., *Getting Smarter about Smart Cities: Improving Data Privacy and Data Security*, Data Protection Unit, Department of the Taoiseach, Dublin, Ireland, 2016, 82p. ; voir également : EDWARDS L., « Privacy, Security and Data protection in Smart Cities : A Critical EU Law Perspective », *Eur. Data Prot. L. Rev.*, Vol. 2, Issue 1, 2016, pp. 28-58 ; HILLER J. S. et BLANKEE J. M., « Smart Cities, Big Data and the Resilience of

réidentification des personnes y est ainsi très important. La diversité des informations collectées et croisées peut révéler un grand nombre de précisions sur leur profil, au-delà de leur localisation. La dimension individuelle va se trouver intimement liée à la dimension collective. La frontière entre la vie publique et la vie privée peut s'en trouver abolie, ce qui renvoie bien à l'image d'un véritable réseau social à l'échelle urbaine. Certains y voient des risques de surveillance généralisée, qualifiant la *Smart City* de véritable « Metropticon », à l'image du Panopticon de Bentham[8]. Si le droit au respect de la vie privée est bien sûr menacé, le droit des données personnelles trouvera bien sûr à s'appliquer à de tels systèmes, qui procèdent de traitements à grande échelle.

S'il est indispensable, comme dans la présente espèce, de garantir le respect des droits des personnes dès le stade des premiers traitements (I), cet impératif de protection devra être pensé à un niveau plus global, au regard des possibilités de réutilisation et de croisement des données qui ont pu être collectées (II).

I. DE L'ANONYMISATION ET DE LA PSEUDONYMISATION DANS UN DISPOSITIF DE MESURE D'AUDIENCE PUBLICITAIRE

Le traitement proposé par JC Decaux devait préalablement être autorisé par la CNIL, sur le fondement de l'article L 581-9 du Code de l'environnement, relatif aux systèmes de mesure d'audience des dispositifs publicitaires[9]. En cela, il devait aussi être conforme aux dispositions de la loi du 6 janvier 1978. Le procédé d'anonymisation des données ayant été jugé insuffisant (A), une information préalable devait normalement être délivrée aux passants (B).

A. L'interprétation stricte du dispositif d'anonymisation des données personnelles

Si le traitement avait une portée assez limitée et semblait conforme à un certain nombre de principes prévus par la loi de 1978 (1), son insuffisance au niveau du dispositif d'anonymisation des données justifie le refus d'autorisation de la CNIL (2).

Privacy », *Hastings L. J..*, Vol. 68, Issue 2, February 2017, pp. 309-356 ; VAN ZOONEN L., « Privacy concerns in Smart Cities », *Gov. Inf. Q.*, Vol. 33, 2016, pp. 472-480

[8] 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

[9] Depuis la loi du 12 juillet 2010 portant engagement national pour l'environnement

1) La portée limitée du traitement de données proposé par JC Decaux

Les mesures d'audience dans un espace ouvert et fortement fréquenté tel que celui de la dalle de la Défense ne pouvaient être effectuées avec des moyens classiques, et notamment reposer sur le consentement des piétons.

Seul restait, de façon dérogatoire, l'intérêt légitime du responsable de traitement, au sens de l'article 7 de la loi de 1978. Celui-ci était bien caractérisé, puisque ces mesures auraient permis d'optimiser les prix des espaces publicitaires, et d'adapter l'affichage en fonction de la fréquentation du site. On relèvera de plus qu'il n'avait alors qu'une visée expérimentale. Il n'empêche que le traitement devait quand même respecter les autres dispositions de la loi et, à travers celles-ci, les droits et libertés des personnes. Les obligations du responsable de traitement prévues par l'article 6 de la loi étaient en grande partie satisfaites. La finalité apparaissait comme explicite, déterminée et légitime au vu des considérations précitées. S'agissant des données collectées, les boîtiers de comptage étaient en mesure de capter les éléments suivants : l'adresse MAC émise par la carte Wi-Fi de tout appareil situé à moins de 25 mètres, l'horaire exact de détection et la puissance d'émission du signal. Cette dernière permettrait d'établir, de façon approximative, la distance entre le boîtier et l'appareil. Il s'agit bien de données pertinentes et adéquates au regard de la finalité précitée. Elles auraient ensuite été transmises à un serveur, à intervalles de deux minutes, pour y être analysées pendant la durée de l'expérimentation, soit un mois, puis supprimées 15 jours plus tard. Là encore, la CNIL estime que la durée prévue était légitime et proportionnée au but poursuivi. De même, les destinataires des données lui apparaissaient clairement identifiés, qu'il s'agisse du personnel de l'entreprise ou de son prestataire.

Mais, selon la Commission, le traitement révélait des insuffisances au niveau de la sécurité des données collectées. Les données auraient fait l'objet d'un dispositif rendant impossible toute identification des piétons en cause. Pour cela, les adresses MAC auraient été tronquées au moment de la collecte avant d'être hachées à l'aide d'un sel propre à JC Decaux.

2) L'insuffisance du procédé d'anonymisation des données proposé par JC Decaux

Les garanties de ce procédé, dit de « hachage avec salage », ont notamment été analysées par l'avis du groupe de travail de l'article 29 n° 05/2014 sur les techniques d'anonymisation.

Celles-ci doivent normalement permettre de prévenir tout risque d'individualisation, de corrélation et d'inférence des données qui permettraient de réidentifier une personne[10]. Cette affirmation repose elle-même sur les dispositions de la directive n° 95/46/CE, et notamment son considérant n° 26, selon lequel tous les moyens pouvant « raisonnablement » être mis en œuvre pour identifier une personne doivent être pris en compte. L'idée figure également à l'article 2 de la loi de 1978. Un procédé d'anonymisation n'est considéré comme fiable que s'il est irréversible et qu'il rend impossible tout recoupement ou tout rapprochement d'enregistrements dans un ou plusieurs ensembles de données permettant d'isoler un individu, et d'en déduire des informations. Parmi les différents procédés utilisables, et au vu de cette « grille de lecture », la pseudonymisation apparaît plus comme une mesure de sécurité qu'une réelle technique d'anonymisation. Les personnes dont les données ont été pseudonymisées restent indirectement identifiables, au moins pour le responsable de traitement. Celui-ci peut par exemple être détenteur de la clé de déchiffrement. Il en va de même, comme l'affirme le groupe de travail, pour les fonctions de hachage avec salage[11]. Si celles-ci garantissent une sécurité supplémentaire vis-à-vis des tiers, elles n'empêcheraient pas de calculer la valeur d'origine des données par des moyens raisonnables. De même, elles ne rendent pas impossible toute corrélation, selon la fonction employée.

C'est justement ce qui était reproché à JC Decaux en l'espèce. Afin de sécuriser les données, les adresses MAC collectées étaient censées être tronquées de leur dernier demi-octet, puis complétée par une suite de caractères et soumise à une méthode de « hachage à clé ». Néanmoins, malgré la mise en œuvre de ce procédé, il est apparu que les données propres à un même passant pouvaient être reliées entre elles à chacun de ses passages à proximité de l'un ou l'autre des boîtiers. Autrement dit, il était bien possible d'établir le parcours d'un même individu sur la dalle de la Défense, donc d'en suivre la mobilité dans un lieu public. Les données n'étaient donc pas anonymisées, mais seulement pseudonymisées, au sens de l'avis du G29. Les termes en ont d'ailleurs été repris par la CNIL dans sa délibération, ce qui était soulevé comme un moyen de légalité interne par JC Decaux, cet avis étant dépourvu de valeur normative. Le Conseil d'Etat rejettera le moyen, estimant que la CNIL n'était nullement liée

[10] *Avis n° 05/2014 du groupe de travail de l'article 29 sur les techniques d'anonymisation*, adopté le 10 avril 2014, p. 13

[11] *Avis n° 05/2014 du groupe de travail de l'article 29, op. cit.*, pp. 22-23

par les conclusions de cet avis. Le refus d'autorisation est également confirmé par la juridiction, qui estime que la Commission a dûment pris en compte les facteurs pertinents relatifs au traitement et à ses conséquences, au regard de l'article 2 de la loi de 1978.

Le fait d'écarter tout risque d'identification était essentiel dans le projet de JC Decaux, puisque les données n'auraient alors plus été considérées comme personnelles, ce qui auraient allégé ses obligations.

B. Les conséquences de la qualification de donnée personnelle

La qualification de donnée personnelle (1) emportait un certain nombre de conséquences quant à l'application de la loi du 6 janvier 1978. Ainsi en est-il de la qualité de l'information préalable qui devait être délivrée aux personnes (2).

1) L'attachement à la qualification de donnée personnelle

La distinction technique des procédés d'anonymisation ou de pseudonymisation impacte la qualification juridique de la donnée personnelle.

Celle-ci est classiquement définie par l'article 2 de la loi du 6 janvier 1978 comme « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ». L'étendue de cette notion concourt à garantir le haut degré de protection qui est normalement dû aux données personnelles. Toutes les informations qui conservent un pouvoir identifiant peuvent donc tomber dans cette catégorie, ce qui inclut les données pseudonymisées. A l'inverse, les données anonymisées ne sont considérées comme personnelles que jusqu'à la mise en œuvre d'un procédé d'anonymisation fiable et irréversible[12]. Le caractère identifiant peut même être perçu comme une forme de dérogation dans les dispositions de la loi ou de la directive. Ces deux textes disposent bien que les données ne peuvent être conservées sous une forme identifiante que pour la durée nécessaire à la finalité du traitement, l'anonymat devant s'imposer dans l'hypothèse d'une conservation prolongée, notamment à des fins statistiques, historiques ou scientifiques.

[12] MATTATIA F., *Le droit des données personnelles*, 2ème éd., Eyrolles, Paris, 2016, p. 27

Le potentiel d'identification conditionne donc l'application des dispositifs protecteurs des personnes dont les données sont collectées, soit par référence à leur contenu ou leur nombre, soit de façon temporelle. Cela explique qu'il soit parfois difficile de distinguer les techniques d'anonymisation « pures » des techniques de pseudonymisation, le passage de l'une à l'autre pouvant être établi à l'aune d'un simple détail. Il existerait dès lors une gradation, une sorte d'anonymat relatif[13], la fiabilité du dispositif étant là encore appréciée au regard de l'ensemble des facteurs pertinents[14]. En l'occurrence, il suffit qu'existe un risque de corrélation entre deux informations isolées, comme cela était le cas en l'espèce, pour que la qualification de traitement de données personnelles soit retenue. La traçabilité prend ici le relais de l'identification, puisqu'elle permet quand même d'isoler un individu « anonyme »[15].

Au-delà, le profilage qui peut en être tiré mettra également en cause le respect de la vie privée, là encore sans égard au fait que les données soient pseudonymisées, ou qu'elles proviennent du comportement de la personne dans un espace public.

2) La nécessité de délivrer une information complète aux personnes

La qualification de donnée personnelle ayant été retenue par la CNIL dans l'affaire en cause, le responsable du traitement devait se conformer à un certain nombre d'obligations prévues par la loi de 1978.

Celles-ci auraient pu être sensiblement allégées jusqu'à la mise en œuvre du procédé d'anonymisation, si les données présentaient vraiment ce caractère. L'article 32-IV prévoit en effet une obligation d'information simplifiée lorsque les données font l'objet d'une anonymisation. Celle-ci est limitée à l'identité du responsable de traitement, ainsi qu'à la finalité poursuivie par celui-ci. La CNIL a d'ailleurs pu se faire l'écho de cette dérogation s'agissant de ce type de dispositifs, en rappelant bien qu'elle était subordonnée à l'utilisation d'un dispositif d'anonymisation comportant un fort taux de collision (un identifiant en base

[13] EYNARD J., *Les données personnelles – Quelle définition pour un régime de protection efficace ?*, Michalon, Paris, 2013, p. 48

[14] *Avis n° 4/2007 du groupe de travail de l'article 29 sur le concept de donnée à caractère personnel*, 20 juin 2007, pp. 19-20

[15] EYNARD J., *op. cit.*, pp. 99-109

doit correspondre à un grand nombre de personnes)[16]. Elle était d'autant plus cruciale en l'espèce que le procédé d'anonymisation était censé être mis en œuvre de façon automatique et dès la collecte des données. Cela aurait également délié le responsable du respect des droits d'accès, de rectification et d'opposition.

Tirant les conséquences de la qualification de donnée personnelle, la CNIL constate l'insuffisance des dispositifs d'information prévus par JC Decaux au regard du caractère automatique de la collecte et de l'impossibilité pour les personnes d'exercer les droits précités. Six panneaux d'information étaient voués à être disposés sur les mâts de mobiliers, leur contenu étant limité aux prescriptions de l'article 32-IV. Outre le fait que celui-ci était incomplet, pour les raisons qui viennent d'être évoquées, le nombre et la forme des panneaux apparaissaient clairement insuffisants au regard du nombre de personnes concernées et de la surface de fréquentation. Le refus d'autorisation de la Commission sur ce fondement est également confirmé par le Conseil d'Etat, qui estime que le traitement litigieux devait se conformer aux dispositions de droit commun. Pour autant, on peut se demander par quel autre moyen cette obligation d'information aurait pu être respectée. La multiplication de panneaux lisibles étant exclue dans un tel espace, seul l'envoi de notification par SMS sur les téléphones aurait pu satisfaire cette exigence, au prix du désagrément de leurs propriétaires. La CNIL n'avait d'ailleurs pas manqué de déconseiller ce type de pratiques pour les dispositifs publicitaires intégrant des bornes Bluetooth installés dans les stations de métro[17].

Aussi, pour cette raison, le refus de la Commission d'autoriser le traitement proposé par JC Decaux a pu être jugé particulièrement sévère, en ce qu'il enserre ces dispositifs dans des limites techniques trop étroites, assimilables à une logique de « tout ou rien »[18]. On notera cependant que la CNIL a entretemps autorisé un autre dispositif de mesure d'audience publicitaire, dont le procédé d'anonymisation a été jugé conforme à l'avis du G29[19]. Il était

[16] Voir le communiqué « Mesure de fréquentation et analyse du comportement des consommateurs dans les magasins », 19 août 2014

[17] *29ème rapport d'activité 2008*, La Documentation Française, Paris, 2009, p. 50

[18] METALLINOS N., « "Unique dans la foule" : l'impossible anonymisation de l'analyse des flux piétons », *CCE*, juin 2016, pp. 36-38 ; voir également : DROUARD E. et MAROLLA C., « Anonymisation et internet des objets : une "première" du Conseil d'État qui fera date » *RLDI*, n° 135, mars 2017, pp. 22-25

[19] Délibération n° 2017-145 du 09 mai 2017 autorisant la société *Retency* à mettre en œuvre à titre expérimental un traitement automatisé de données à caractère personnel ayant pour finalité la mesure d'audience et de fréquentation de dispositifs publicitaires au sein de la gare SNCF de Dijon

établi que le responsable du traitement ne pouvait lui-même rejouer les procédés de chiffrement, et donc réidentifier les personnes, ce qui lui permettait de s'en tenir à une information simplifiée sous la forme d'affiches. Au vu de cette deuxième décision, la Commission invite à exclure toute faculté d'identification pour ce type de traitements, celle-ci étant disproportionnée au regard de leur finalité.

Il est vrai que ceux-ci sont voués à faire partie d'un ensemble de traitements beaucoup plus vaste dans l'environnement des villes intelligentes, où le risque d'identification est latent.

II. DE LA MESURE D'AUDIENCE PUBLICITAIRE AUX VILLES INTELLIGENTES

Les difficultés que présente l'affaire JC Decaux illustrent parfaitement les interrogations que posent les villes intelligentes pour la protection des données personnelles (A). La décision de la CNIL se comprend peut-être mieux dans ce contexte, bien qu'elle ne lève pas toutes les incertitudes (B).

A. De l'anonymisation à la réidentification des personnes dans les villes intelligentes

Comme nous l'avons indiqué, les projets de *Smart Cities* investissent tous les champs d'activité des espaces urbains, et reposent sur l'analyse de données qui leurs relatives. En cela, il ne s'agit que d'une nouvelle application de l'internet des objets[20], des techniques de *Big Data*[21] et d'intelligence artificielle. L'image de la pyramide décrit aisément le schéma prospectif de ces villes intelligentes. Une multitude de traitements de données pourront s'y superposer (1), augmentant les risques de réidentification des personnes (2).

1) La pyramide des traitements de données

Les projets déployés par les villes intelligentes peuvent être initialement isolés les uns des autres. Leur mutualisation présente pourtant d'importantes potentialités. La capacité de

[20] 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

[21] HILLER J. S. et BLANKEE J. M., *op. cit.*, pp. 314-316 ; MARINO L., « Le Big Data bouscule le droit », *RLDI*, n° 99, décembre 2013, p. 57

croisement des données qu'ils auront collectées permettra de leur découvrir de nouvelles utilités à des degrés variés.

Tous les traitements qui seront mis en œuvre pourront s'organiser dans une structure verticale[22], et même pyramidale. Les données collectées à un niveau donné pourront être agrégées et réutilisées au niveau supérieur. Au niveau le plus bas, les nombreux capteurs embarqués sur les objets connectés, qu'ils soient mobiliers ou immobiliers, tels que les dispositifs publicitaires, vont collecter toutes sortes de données en temps réel[23]. Certaines de ces données proviendront directement des personnes, soit de façon automatique à travers leurs propres objets (smartphones, véhicules,…), soit de façon volontaire, à travers des applications de partage d'informations. Elles pourront aussi être enrichies par les données publiques, disponibles en *Open data*. Tous ces ensembles pourront dans un premier temps être analysés pour entraîner une prise de décision propre à chaque traitement, celle-ci pouvant même être automatisée.

Mais ces mêmes données pourront par la suite être réutilisées pour de nouvelles finalités, en étant croisées avec celles qui relèvent d'autres traitements. Ces usages secondaires n'auront pas forcément été anticipés au premier niveau[24]. Pour reprendre le cas des transports et de la voirie, les données collectées par un feu de circulation intelligent pourront être contextualisées à l'aide d'autres données de circulation, provenant d'autres objets, d'autres lieux, publics ou privés, pour mieux analyser les flux par zones, par type de trajets (professionnels, loisirs,…) ou par type de transports (individuels, collectifs). En fonction des circonstances de temps et de lieu, cela aidera à mieux prévenir les risques d'engorgements, d'accidents, et garantir une meilleure sécurité publique. Cet affinage permettra aussi aux entreprises de délivrer des offres commerciales personnalisées de façon instantanée en fonction de la situation des personnes. Là encore, tout cela pourra être effectué de manière automatisée, grâce à la capacité d'échanges des objets connectés. Un très grand nombre d'utilités pourra ainsi être tiré des traitements secondaires. Les croisements peuvent se multiplier et se hiérarchiser, les pouvoirs publics et les entreprises étant intéressés aux niveaux les plus élevés.

---

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

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

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

Dans l'absolu, une ville pourra être cartographiée en temps réel, tout comme la vie privée de ses habitants, avec une précision microscopique.

2) Le risque global de réidentification des personnes

Le croisement potentiel des informations constitue la menace la plus importante pour le droit au respect de la vie privée et la protection des données personnelles. En effet, il augmente le risque de réidentification, aux niveaux supérieurs des traitements de données.

Celles qui sont recueillies au premier degré seront le plus souvent dérisoires, soit par leur quantité soit par leur qualité. Tel était le cas pour le système proposé par JC Decaux, les données collectées étant somme toute assez limitées, indépendamment de leur pseudonymisation[25]. On sait cependant qu'une seule corrélation ou une seule inférence entre deux données, issues du même ensemble ou de deux ensemble séparés, suffit pour qu'une personne soit considérée comme identifiée. Si anonymes et isolées que puissent être les informations issues de chaque traitement, les utilités secondaires permettront *a posteriori* de reconstituer un profil très précis des habitants, donc de les réidentifier[26]. Cela est d'autant plus vrai au regard de la diversité de ces informations et de leur provenance. On rappellera que certaines d'entre elles pourront être communiquées volontairement. Les données de géolocalisation (*check in*) tout comme les avis postés par les internautes sur les lieux qu'ils fréquentent seront autant d'éléments venant enrichir celles qui ont été collectées automatiquement pour établir leurs habitudes de vie[27], ou même leurs relations sociales. La présence de plusieurs personnes en un même lieu pourra ainsi être aisément établie ; celles qui ne seraient pas utilisatrices de ces applications pourraient quand même être « happées » dans le filet des croisements de données. Il faut ajouter à cela les données ouvertes, qui seront de plus en plus accessibles, et permettront encore davantage de préciser le profilage des individus[28]. Comme l'a relevé le groupe de travail de l'article 29, le risque de réidentification

[25] METALLINOS N., *ibid.*

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

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

[28] EDWARDS L., *op. cit.*, p. 45

est toujours susceptible d'augmenter avec les progrès des technologies de l'information et de la communication[29].

De ce risque de réidentification découle la crainte d'une nouvelle forme de surveillance de masse à l'échelle urbaine. Tout habitant pourrait être suivi à son insu, renonçant à l'anonymat traditionnel de la foule, à travers la collecte et le croisement automatisés de ses données[30]. Celles-ci pourront se retrouver entre les mains des pouvoirs publics ou d'entreprises privées pour toutes sortes de finalités. Ces traitements pourront révéler un important potentiel discriminatoire, puisqu'ils permettraient de cloisonner les populations par quartiers, par comportements, par trajets,... Certains auteurs craignent même les réactions paternalistes des gouvernements et pouvoirs publics qui disposeront d'une telle somme d'informations[31]. On ne peut également s'empêcher de penser aux risques que présentent ces systèmes en termes de sécurité. Une défaillance informatique ou physique, un piratage des données, ou une intrusion malveillante pourrait avoir des répercussions considérables, mettant en cause jusqu'à la sécurité physique des habitants[32]. Ces dangers, propres aux objets connectés[33], prennent eux aussi des dimensions beaucoup plus inquiétantes.

Ces considérations techniques interrogent sur l'application du droit des données personnelles.

B. Les incertitudes des villes intelligentes pour la protection des données personnelles

La sévérité de la CNIL se comprend peut-être mieux à la lumière de ce contexte. Elle prouve cependant qu'il est difficile d'assurer un parfait respect des droits des personnes dès le niveau des premiers traitements, ceux-ci se révélant finalement incompatibles avec plusieurs des principes prévus par la loi (1). Le règlement européen relatif à la protection des données personnelles apportera quelques outils qui seront certainement utiles pour penser cette protection de façon plus globale (2).

---

[29] *Avis n° 05/2014 du groupe de travail de l'article 29*, *op. cit.*, pp. 9-10

[30] HILLER J. S. et BLANKEE J. M., *op. cit.*, pp. 323-325 ; KITCHIN R., *op. cit.*, pp. 30-38

[31] FINCH K. et TENE O., *op. cit.*, pp. 1595-1606

[32] ELMAGHRABY A. S. et LOSAVIO M. M., « Cyber Security Challenges in Smart Cities : Safety, Security and Privacy », *JAR*, Vol. 5, 2014, p. 496 ; KITCHIN R., *op. cit.*, pp. 39-46

[33] *Avis n° 8/2014 du groupe de travail de l'article 29 sur les récentes évolutions relatives à l'internet des objets*, adopté le 16 septembre 2014

1) Le difficile respect des droits des personnes et des obligations des responsables de traitements

Comme cela a pu être relevé, le traitement mis en œuvre par JC Decaux semblait incompatible avec l'exigence d'une information suffisante à délivrer aux personnes ainsi qu'avec le respect de plusieurs de leurs droits. Mais c'est là une caractéristique courante des projets développés au titre des villes intelligentes.

La recherche du consentement préalable et la possibilité d'exercer les droits d'accès, de rectification et d'opposition sont bien peu compatibles avec ces projets. Ceux-ci reposent sur la rapidité d'exécution, voire l'instantanéité, des traitements de données. Tel était bien le cas avec le système de mesure d'audience publicitaire, qui ne pouvait raisonnablement se fonder sur le consentement des milliers de personnes fréquentant la dalle de La Défense. Le recours à une action positive de l'utilisateur, s'il a pu être utilement exigé dans certaines hypothèses comme les dispositifs d'affichage publicitaire installés dans les métros (*cf. supra.*), paraît difficilement envisageable dans les espaces publics ouverts. La règle étant la même pour tous les autres types de traitements, il faudrait alors envisager l'envoi systématique de notifications aux habitants, les informant de leur mise en œuvre et leur laissant la possibilité d'y consentir ou de s'y opposer ultérieurement. Cela serait d'autant plus difficile à mettre en œuvre qu'il faudrait tenir compte des traitements secondaires, dont on rappelle qu'ils ne seront pas toujours connus au moment de la première collecte. Là encore, il y a fort à parier que l'intérêt légitime des responsables de traitement soit trop facilement invoqué pour s'affranchir du consentement des personnes, ce qui interroge sur la portée de cette dérogation.

Il en est de même avec la nécessité d'informer les personnes de l'existence de ce traitement secondaire, normalement prévue par l'article 32-III de la loi. Comme nous l'avons vu, un premier traitement qui serait anonyme (au bon sens du terme) pourrait cesser de l'être si on le croise avec un autre, dès lors qu'apparaît le risque de réidentification. Quelle sera alors la qualité de l'information à délivrer au sens de l'article précité ? Comment communiquer correctement l'identité des nouveaux responsables de traitements, et les nouvelles finalités qui sont poursuivies, notamment lorsque celles-ci sont « découvertes » *a posteriori* ? Des doutes similaires pèsent sur le respect des principes de proportionnalité et de limitation de la durée de traitement. Quand bien même les données collectées au premier degré seraient parfaitement adéquates à une finalité donnée, les utilités secondaires qui peuvent en être tirées vont justifier

la superposition de nouveaux traitements, augmentant le stock d'informations à traiter. Il sera dès lors plus intéressant de conserver ces données bien au-delà de la durée nécessaire aux premières finalités. Le potentiel qu'elles représentent servira le développement rapide de nouveaux services. Là encore, il ne s'agit que d'une nouvelle expression de tendances qui avaient déjà été relevées pour les objets connectés[34], tout comme les risques pour la sécurité des données.

Ces quelques exemples des risques que présentent les villes intelligentes peuvent justifier l'intransigeance de la CNIL à l'égard du dispositif de mesure d'audience publicitaire que souhaitait mettre en œuvre JC Decaux de façon expérimentale. Sa décision peut donc être considérée comme un exemple, un signal adressé aux entreprises et aux pouvoirs publics leur rappelant la nécessité de garantir un haut degré de sécurité pour les données, ce qui passe aussi par une minimisation des risques d'identification dès le premier degré.

2) Les solutions du règlement européen pour la protection des données personnelles dans les villes intelligentes

La protection des données personnelles dans l'environnement urbain pose donc un important problème en termes de faisabilité technique. Le futur règlement général relatif à la protection des données[35] fournit à ce titre des pistes de solutions, tout en laissant certaines latitudes utiles aux responsables de traitements.

Sur le plan technique, les principes 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, présent un certain intérêt. En effet, il semble indispensable d'intégrer la protection des données en amont, dès le développement des systèmes[36], ce afin de garantir techniquement les obligations du responsable de traitement et l'exercice de leurs droits par les personnes. Des outils concrets pourraient être développés afin qu'elles puissent contrôler

[34] 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

[35] 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

[36] 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

directement leurs données. Ce serait là un moyen de responsabiliser également les personnes, dans un mouvement de « *Self Data* »[37]. L'implémentation de points d'accès à l'information par des moyens techniques, tels des QR codes apposés sur les objets connectés, ou le recours à des applications pour smartphones pourraient à ce titre être envisagés. Cela conforterait l'approche « positive » de l'utilisateur, et écarterait les désagréments liés à l'envoi répétitif de notifications ou d'alertes. Le défi reste quand même important au vu du nombre de traitements secondaires qui pourront être mis en œuvre. Il faudrait concevoir un système centralisé, regroupant l'ensemble des informations relatives aux traitements[38], et permettant de paramétrer à l'avance les objets connectés de l'utilisateur. Ce système lui permettrait aussi de s'opposer à certaines collectes, notamment dans certains lieux ou situations. Le droit au « silence des puces » avait de la même façon été suggéré pour les objets connectés[39]. L'efficacité de ces dispositifs pourrait néanmoins rester illusoire. L'utilisateur peu enclin à consulter une information trop détaillée et fastidieuse pourra s'en remettre à un paramétrage par défaut[40]. De même, on sait que les personnes partagent plus volontiers leurs données lorsque les gains du traitement sont immédiats ou présentés comme tels[41]. C'est là l'effet du *Privacy Paradox*.

Les risques sont d'autant plus avérés que certaines libertés seront laissées aux responsables de traitement par le règlement. Tel est le cas au niveau du consentement préalable, qui peut être recueilli de façon implicite, en fonction d'un « comportement » de la personne[42]. L'absence de paramétrage des objets connectés pourrait être interprétée comme un tel comportement. On relèvera que l'intérêt légitime du responsable de traitement reste une dérogation au principe du consentement préalable (art. 6 f)), posant les mêmes difficultés d'interprétation[43]. De même, le règlement prévoit d'autres assouplissements qui intéresseront les usages secondaires des données. L'article 6 § 4 prévoit ainsi un test de compatibilité, qui devra être respecté dans tous

[37] 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

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

[39] 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

[40] KITCHIN R., *op. cit.*, pp. 37-38

[41] VAN ZOONEN L., *op. cit.*, p. 474

[42] 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

[43] EDWARDS L., *op. cit.*, p. 43

les cas où des données vont être utilisées pour une nouvelle finalité sans le consentement de la personne. Le responsable est censé tenir compte des liens existants entre les finalités du premier et du second traitement, du contexte de leur collecte et des conséquences de cette réutilisation en fonction de la nature des données. Le respect de certaines garanties y est encore exigé, tel que le recours à la pseudonymisation. Cette dérogation, qui favorise l'utilisation de techniques de *Big Data*, trouvera un terrain d'application privilégié avec les villes intelligentes. Enfin, des incertitudes demeurent également au niveau du devoir d'information préalable. Celui-ci est visé par l'article 14 du règlement spécialement dans les cas où les données ne sont pas collectées directement auprès des personnes. Si le contenu de cette obligation apparaît assez substantiel dans son principe, le paragraphe 5 en dédouane pourtant le responsable de traitement lorsque la fourniture des informations « se révèle impossible ou exigerait des efforts disproportionnés », à charge pour lui de prendre « des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles ». La recherche d'équilibre est louable, mais pose les mêmes difficultés d'interprétation que celles de l'affaire JC Decaux, s'agissant de l'équilibre entre l'intérêt légitime du responsable de traitement et le respect des droits et libertés des personnes.

Quand bien même l'exigence de minimisation de la collecte, qui découle du principe de *Privacy by Default*, serait respectée au niveau des premiers traitements, les risques liés à la réidentification demeurent importants au vu de ces dérogations.

****

Il est certain que la solution à ces difficultés ne peut résider qu'en une adéquation des standards technologiques et juridiques. Puisque le risque d'identification est dépendant de l'évolution des techniques, celles-ci doivent aussi évoluer pour mieux l'écarter. C'est peut-être l'une des vertus du principe de *Privacy by Design* que de pousser à anticiper ces risques, ce qui invite à sensibiliser jusqu'aux concepteurs des systèmes de traitement. Cela est d'autant plus vrai que ceux-ci sont souvent peu informés du cadre juridique applicable à ces produits[44]. Au-delà, il serait essentiel d'impliquer directement les personnes, ce qui passe par une forme d'éducation

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

au droit des données personnelles[45]. Certains vont jusqu'à suggérer de les intégrer dans le fonctionnement même des villes intelligentes, en développant notamment des systèmes d'innovations ouvertes[46], afin d'en renforcer la légitimité[47]. Le droit et la technique ne seraient alors que les moyens d'un nouveau mode de vie urbaine.

[45] KITCHIN R., *op. cit.*, p. 53

[46] 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

[47] HILLER J. S. et BLANKEE J. M., *op. cit.*, pp. 334-336