Données personnelles
Mesures d'audience : anonymisation et droit à l'information

Par un arrêt du 8 février 2017, le Conseil d'Etat s'est prononcé sur la notion d'anonymisation des données personnelles.

Les données à caractère personnel sont une matière première sensible, et la société JCDecaux l'a appris à ses dépens. Le Conseil d'Etat a rendu un arrêt, le 8 février 2017[1], qui mérite non seulement l'attention des juristes, mais également des acteurs de l'internet des objets, du big data et de la publicité comportementale. Enjeu économique majeur pour tous les acteurs du secteur, et plus ou moins directement, à terme, pour l'ensemble des acteurs économiques, la traditionnelle confrontation entre les libertés publiques et l'intérêt légitime des entreprises cherchant à améliorer leurs services, voire en créer d'autres, se prête ici à un débat inédit à cette échelle juridictionnelle.

Le Conseil d'Etat était saisi d'un recours en annulation d'une délibération de la Commission nationale de l'Informatique et des libertés (Cnil) du 16 juillet 2015[2], ayant refusé d'autoriser la société JCDecaux à mettre en œuvre un traitement de données à caractère personnel qui avait pour finalité de tester une méthodologie d'estimation quantitative des flux piétons sur la dalle de la défense.

Le traitement consistait à installer des boîtiers de comptage Wi-Fi sur les mobiliers publicitaires, qui captaient les adresses des appareils mobiles présents à moins de 25 mètres et dont l'interface Wi-Fi était activée. Plus précisément, l'idée était de quantifier les flux piétons qui fréquentent l'esplanade de la Défense, afin de mieux connaître l'audience des panneaux publicitaires et, partant, de les valoriser auprès des annonceurs. La société JCDecaux faisait ainsi valoir devant la Cnil que « *la valorisation de tout support publicitaire auprès des annonceurs, et ainsi la capacité à vendre des espaces publicitaires et à optimiser leur prix par rapport aux autres supports publicitaires, requiert la connaissance de son audience* ». Le système permettait même d'extrapoler la distance approximative séparant le terminal mobile d'un boîtier, à l'aide de la puissance d'émission du signal Wi-Fi.

Ce traitement était soumis à l'autorisation préalable de la Cnil en vertu de l'article L. 581-9 du code de l'environnement[3], lequel prévoit que tout système de mesure automatique de l'audience d'un dispositif publicitaire, ou d'analyse de la typologie ou du comportement des personnes passant à proximité d'un dispositif publicitaire, est soumis à autorisation de la Cnil.

Saisie de la demande d'autorisation, la Cnil a rendu une délibération particulièrement riche pour refuser à JCDecaux l'autorisation de mettre en œuvre le traitement, qui se voit confirmée par un arrêt du Conseil d'Etat du 8 février 2017 qui fera date.
On passera sur les moyens de légalité externe de la décision, tenant notamment à une prétendue insuffisance de motivation de la décision de la Cnil, pour se concentrer sur la légalité interne, dont le point cardinal était, une fois la légalité même du traitement admise, la question de l'anonymisation des données, dont la non-reconnaissance entraînait l'application des obligations extensives d'information et le droit d'opposition des personnes concernées, ce qui suscite bon nombre d'interrogations pour les acteurs du secteur.

La finalité du traitement jugée légale

L'article 7 de la Loi Informatique et libertés prévoit qu'un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes :

1. le respect d'une obligation légale incombant au responsable du traitement ;
2. la sauvegarde de la vie de la personne concernée ;
3. l'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;
4. l'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;
5. la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire,

sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

En l'espèce, la société JCDecaux n'entendait pas se fonder sur le consentement des personnes dont les données étaient collectées, qui aurait été, on le devine, difficilement envisageable à mettre en œuvre et aurait réduit à néant l'expérimentation. Les autres conditions du texte n'étant à l'évidence pas remplies, restait la condition de « *l'intérêt légitime du responsable de traitement* ».

La Cnil juge la finalité du traitement, selon la formule consacrée, « *déterminée, explicite et légitime* », d'autant que la portée de l'expérimentation était limitée à la fois dans le temps (4 semaines) et dans l'espace. On peut d'ailleurs relever que le caractère expérimental et limité du traitement a certainement joué en faveur de sa légalité, ajouté au fait que la zone en question interdisait d'utiliser des moyens classiques pour connaître l'audience des dispositifs publicitaires. La Cnil avait également relevé qu'aucune décision ne serait prise sur la base de ce traitement à l'égard des personnes concernées, ni qu'il en résulterait un ciblage commercial à leur égard. L'inverse aurait peut être présidé à un refus d'autorisation sur d'autres fondements, en l'absence de consentement des intéressés.

La finalité du traitement a donc été jugée légale par la Cnil, mais ses conditions de mise en œuvre devaient être confrontées aux droits et libertés fondamentaux des personnes dont les données sont traitées sans consentement.

Le traitement pêchait plus en ce que la Cnil a relevé que les données n'étaient pas anonymisées mais seulement « *pseudonymisées* », et que dès lors, la société JCDecaux devait respecter les droits des individus, c'est-à-dire notamment le droit de s'opposer au traitement, et d'être informé de manière satisfaisante des conditions de sa mise en œuvre, sauf à ce que la condition de loyauté du traitement vis-à-vis des personnes concernées fasse défaut.

La distinction entre un dispositif de pseudonymisation et un dispositif d'anonymisation des données personnelles

Anonymisation ou pseudonymisation

La Loi Informatique et libertés[4] ne définit pas l'anonymisation. La Directive n° 95/46 du 24 octobre 1995 indique quant à elle que « *les principes de protection ne s'appliquent pas aux données rendues anonymes d'une manière telle que la personne concernée n'est plus identifiable* », offrant par là un début de définition. Le Règlement général sur la protection des données n° 2016/679, qui entrera en vigueur en mai 2018, n'en donne pas de définition. Tout au plus se contente-t-il de préciser qu'il convient de considérer l'ensemble des moyens « *susceptibles d'être raisonnablement mis en œuvre* » par le responsable de traitement ou toute autre personne pour identifier la personne, pour déterminer si celle-ci est « identifiable« , reconnaissant par là qu'il existe une gradation dans les méthodes employées d'anonymisation.

A l'occasion des débats parlementaires avant l'adoption de la loi dite Lemaire du 7 octobre 2016 « *pour une République numérique* »[5], dont l'un des enjeux est l'anonymisation des données des usagers de services publics appelées à être « *ouvertes* », deux rapporteurs de la Commission des lois du Sénat se sont interrogés sur la protection des données personnelles dans l'open data[6]. Ces travaux résument bien les enjeux de l'anonymisation face au big data, et les différentes techniques existantes.

Les techniques existantes se regroupent autour de deux grands principes : (i) transformer les données pour qu'elles ne se réfèrent plus à une personne désignée, et (ii) généraliser les données de façon à ce qu'elles ne soient plus spécifiques à une personne mais communes à un ensemble de personnes. L'utilisation d'un algorithme de chiffrement, le hachage, la dégradation de l'information par suppression, masquage ou ajout de bruit ou l'agrégation font partie des techniques qui, seules ou combinées, peuvent être mises en place pour tendre vers l'anonymisation.

L'anonymisation peut être définie comme l'opération de suppression de l'ensemble des informations permettant d'identifier directement ou indirectement un individu, contenues dans un document ou une base de données. Mais tout réside dans ce que l'on entend par «*indirectement*».

L'avis du Groupe de travail «*Article 29*» sur la protection des données[7] (G29) développe les trois critères cumulatifs selon lesquels la fiabilité d'une technique d'anonymisation doit être évaluée :

1. l'individualisation : est-il toujours possible d'isoler un individu ?
2. la corrélation : est-il toujours possible de relier entre eux les enregistrements relatifs à un individu ?
3. l'inférence : peut-on déduire des informations concernant un individu ?

Il en résulte (i) qu'un ensemble de données pour lequel il n'est possible ni d'individualiser, ni de corréler, ni d'inférer est a priori anonyme, et (ii) qu'un ensemble de données pour lequel au moins un des trois critères n'est pas respecté ne pourra être considéré comme anonyme qu'à la suite d'une analyse détaillée des risques de ré-identification.

Comme le relève le G29 dans l'avis précité, les techniques d'anonymisation font l'objet de nombreuses recherches, et aucune ne présente d'efficacité certaine. La mesure de leur efficacité est donc une question de degré, de plus ou moins forte probabilité de ré identification, de combinaisons entre différentes techniques pour réduire le risque jusqu'à ce qu'il puisse être considéré comme très résiduel.

Aux côtés de l'anonymisation, la pseudonymisation est donc une simple mesure de sécurité, qui a pour objet de réduire la corrélation d'un ensemble de données avec l'identité originale d'une personne donnée. Les deux notions

ne se confondent donc pas (même si en pratique l'opposition entre les deux notions ne peut en aucun cas être considérée comme absolue), et c'est précisément sur la ligne de partage entre les deux que sont fondées la délibération de la Cnil et la décision du Conseil d'Etat.

L'interprétation stricte du Conseil d'Etat de la notion d'anonymisation

En soit, l'adresse MAC d'un terminal mobile identifie une machine, non l'utilisateur, de la même façon qu'une adresse IP. Mais elle n'en demeure pas moins indirectement une donnée nominative, puisqu'elle permet d'identifier une personne si elle est associée à d'autres informations. C'est donc dans sa potentialité de pouvoir d'identification d'un individu qu'il s'agit d'une donnée à caractère personnel.

La société JCDecaux avait pris pour précaution de recourir à une double technique de ce qu'elle estimait de l'anonymisation : les données collectées, transmises toutes les deux minutes à un serveur situé à en Allemagne, étaient tronquées du dernier demi-octet de l'adresse MAC de chaque téléphone, et étaient hachées selon un procédé de chiffrement qui devait en garantir l'anonymisation.

La société JCDecaux soutenait que les procédés mis en place rendaient « *négligeable le risque de pouvoir identifier les personnes en cause, d'autant que la collecte de données se déroule dans le cadre d'une expérimentation limitée dans le temps et pour objet d'améliorer la valorisation de ses panneaux publicitaires, ce qui rend sans intérêt pour elle l'identification des personnes concernées* ». Et de fait, on comprend que la société JCDecaux était, par ce seul traitement, incapable d'identifier un individu à partir de l'identifiant MAC collecté, ou plutôt à partir du résultat cryptographique auquel il parvenait une fois les techniques décrites ci-dessus mises en œuvre.

En revanche, elle était capable de recouper des données sur un même individu, dès lors que le système permettait de repérer le nombre de passages d'une même personne dans la zone en question.

Constatant que la technique utilisée permettait toujours la corrélation et l'inférence, et donc la possible ré-identification des personnes, la Cnil n'y a pas vu la mise en œuvre d'une véritable technique d'anonymisation de nature à contourner les obligations informatives. Elle a donc considéré que « *le procédé présenté ne saurait être qualifié de technique d'anonymisation, notamment du fait que la société JCDecaux est en mesure de rejouer le procédé de chiffrement, cette société utilisant un sel qui lui est propre et connu, et en raison du faible taux de collision proposé* ». Elle relève également que « *pour qu'une solution d'anonymisation soit efficace, elle doit empêcher toutes les parties d'isoler un individu dans un ensemble de données* ». Le Conseil d'Etat n'y trouve rien à redire. Au visa de l'article 2 de la Loi Informatique et Libertés (« *pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne* »), il retient que les données n'étaient de fait pas anonymisées dès lors qu'en l'espèce il demeurait « *possible d'individualiser une personne ou de relier entre elles des données résultant de deux enregistrements qui la concernent* ».

Selon le Conseil d'Etat, les données ne sont donc anonymisées que lorsque l'identification directe ou indirecte de la personne est rendue impossible, que ce soit par le responsable de traitement ou par un tiers, et tel n'est pas le cas lorsqu'il demeure possible d'individualiser une personne ou de relier entre elles des données résultant de deux enregistrements qui la concernent. Il retient que les objectifs mêmes de la collecte des données par la société JCDecaux étaient incompatibles avec une anonymisation des informations recueillies, puisque le procédé visait à mesurer la répétition des passages et à déterminer les parcours réalisés d'un panneau publicitaire à un autre, et donc impliquait d'identifier les déplacements des personnes et leur répétition sur la dalle de la défense.

Dès lors, pour obéir à la condition de loyauté du traitement, il fallait informer les personnes de façon satisfaisante.

L'obligation pour le responsable de traitement de respecter les droits d'information et d'opposition des personnes concernées en présence d'un dispositif de pseudonymisation

Les textes applicables

L'article 32 I de la Loi Informatique et libertés met à la charge du responsable de traitement des obligations particulièrement contraignantes d'information de la personne auprès de laquelle sont recueillies les données à caractère personnel la concernant :

« I.-La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant :

1. de l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;
2. de la finalité poursuivie par le traitement auquel les données sont destinées ;
3. du caractère obligatoire ou facultatif des réponses ;
4. des conséquences éventuelles, à son égard, d'un défaut de réponse ;
5. des destinataires ou catégories de destinataires des données ;
6. des droits qu'elle tient des dispositions de la section 2 du présent chapitre dont celui de définir des directives relatives au sort de ses données à caractère personnel après sa mort ;
7. le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne ;
8. de la durée de conservation des catégories de données traitées ou, en cas d'impossibilité,

des critères utilisés permettant de déterminer cette durée. Lorsque de telles données sont recueillies par voie de questionnaires, ceux-ci doivent porter mention des prescriptions figurant aux 1°, 2°, 3° et 6°. »

Afin de prendre en compte des situations où l'information extensive peut difficilement être assurée, l'article 32, III et IV de la Loi Informatique et libertés prévoit que III.- Lorsque les données à caractère personnel n'ont pas été recueillies auprès de la personne concernée, le responsable du traitement ou son représentant doit fournir à cette dernière les informations énumérées au I dès l'enregistrement des données ou, si une communication des données à des tiers est envisagée, au plus tard lors de la première communication des données.
Lorsque les données à caractère personnel ont été initialement recueillies pour un autre objet, les dispositions de l'alinéa précédent ne s'appliquent pas ( ) lorsque la personne concernée est déjà informée ou quand son information se révèle impossible ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche.
IV.-Si les données à caractère personnel recueillies sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés, les informations délivrées par le responsable du traitement à la personne concernée peuvent se limiter à celles mentionnées au 1° et au 2° du I.

(...) »

L'article 90 du décret du 20 octobre 2005[8] prévoit enfin que « *le responsable du traitement porte directement à la connaissance des personnes auprès desquelles sont recueillies des données à caractère personnel les informations énumérées au I de l'article 32 de la loi du 6 janvier 1978 susvisée sur le support de collecte ou, à défaut, sur un document préalablement porté à leur connaissance en caractères lisibles. En application du 6° du I du même article, il les informe également, dans les mêmes conditions, des coordonnées du service compétent auprès duquel elles peuvent exercer leurs droits d'opposition, d'accès et de rectification (...)* ».

Un traitement légal, mais ne respectant pas le principe de loyauté

Il résulte de ces textes que les informations à délivrer à la personne concernée sont plus limitées si les données à caractère personnel sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la loi par la Cnil.

En cas d'anonymisation, le responsable de traitement peut se contenter d'informer la personne dont les données sont collectées de son identité (ou celle de son représentant) et de la finalité poursuivie par le traitement.

La société JCDecaux, qui considérait que son traitement faisait l'objet d'une anonymisation, pensait ainsi pouvoir se prévaloir de ces dispositions limitant les obligations d'information des personnes concernées par la collecte des données. Il était ainsi prévu de se contenter d'un panneau d'affichage de format A4 sur les panneaux publicitaires mentionnant le nom du responsable de traitement et la finalité de celui-ci.

Mais le Conseil d'Etat relève que, dès lors que la Cnil avait relevé en amont que les dispositifs mis en oeuvre par JCDecaux n'avaient pas pour effet de rendre anonymes les données, l'information des personnes concernées devait se faire selon les dispositions de droit commun.

En pratique, la nature même du traitement de JCDecaux et ses conditions de mise en œuvre interdisaient de respecter pleinement les obligations d'information dans leur version « extensive« . Les personnes n'avaient à aucun moment la possibilité de faire valoir leur droit d'opposition, et d'une façon générale l'information par affichage n'était guère possible à garantir, du fait notamment de la portée de 25 mètres des bornes installées par la société, qui plus est dans une zone ouverte sans passage obligé dans un espace restreint qui aurait pu les amener à prendre connaissance des informations.

L'impossibilité de se prévaloir de l'exception d'information impossible ou exigeant des efforts disproportionnés : l'enjeu de la collecte directe ou indirecte

JCDecaux aurait-il pu se prévaloir de l'exception d'information impossible ou exigeant des efforts disproportionnés pour le responsable de traitement ? Rarement admise, cette exception fondée sur l'article 32, III 6° a vocation à s'appliquer en cas de collecte « *indirecte* » des données. C'est-à-dire lorsque les données n'ont pas été recueillies auprès de la personne concernée.

C'est l'un des apports importants de l'arrêt du Conseil d'Etat, quelque peu éclipsé par la question de l'anonymisation : dans le cas d'une collecte effectuée depuis le terminal mobile d'une personne, alors même qu'aucun acte volontaire de sa part n'a été consenti, doit on considérer qu'il s'agit d'une collecte ou indirecte ?

De façon sibylline, le Conseil d'Etat vient poser qu' « *alors même que cette collecte ne nécessite aucune intervention des personnes concernées, elle a néanmoins le caractère d'une collecte directe de données personnelles* ».

Un précédent arrêt du Conseil d'Etat du 23 mars 2015[9] avait donné pour indication qu'une collecte était qualifiée d'indirecte lorsque les données avaient fait l'objet de deux traitements successifs, par deux responsables de traitement différents. Rien de tel dans le cas de JCDecaux, où non seulement la collecte ne nécessitait aucune intervention ou acte volontaire de la personne concernée, mais surtout ne concernait pas des données ayant fait l'objet de deux traitements successifs.

Partant, l'exception d'information impossible ou exigeant des efforts

disproportionnés ne pouvait s'appliquer, et le Conseil d'Etat considère que la Cnil n'a pas commis d'erreur de droit sur ce fondement.

Un renforcement de la protection des données personnelles par le Conseil d'Etat, et beaucoup d'interrogations

La solution, dans sa sévérité, invite à s'interroger : comment utiliser le Big Data en garantissant l'anonymisation des données lorsqu'une entreprise utilise ce type d'outils statistiques ?

Si l'on considère qu'une personne est identifiable par un hypothétique croisement subséquent de données la concernant, alors même que le responsable de traitement est incapable de remonter à l'identité d'une personne à partir des seules données de son terminal (qui plus est faisant l'objet, comme en l'espèce, de mesures techniques avancées de hachage et de chiffrement), on peut penser que ce type d'expérience n'est pas prêt d'être validé juridiquement.

La décision est d'autant plus sévère que le traitement lui-même était jugé licite, et qu'on voit difficilement comment la société JCDecaux aurait pu garantir l'information et le droit d'opposition des personnes dans des conditions satisfaisantes, compte tenu des conditions de mise en œuvre du traitement.

En pratique, sauf à recourir à un dispositif d'anonymisation totale, dont on peine à penser, dans des cas similaires, qu'il puisse être mis en œuvre tout en assurant par ailleurs au responsable de traitement de pouvoir trouver une quelconque utilité aux données collectées, il paraît donc très difficile de pouvoir mener à bien ce type d'expérimentation compte tenu de la sévérité dans l'appréciation de l'anonymisation.

Car c'est bien d'utilité qu'il s'agit. L'expérimentation de JCDecaux, comme tout procédé similaire a évidemment pour vocation de conférer aux données une utilité économique : ici, mesurer l'audience de panneaux publicitaires pour les valoriser auprès des annonceurs, ou dans d'autres cas de mesurer les déplacements d'un client dans un magasin, les trajets effectués et heures de fréquentation, l'intérêt porté aux promotions mises en avant, le temps de fréquentation, etc.

En poussant plus loin, tout type de traitement ayant pour finalité de mesurer un déplacement, sa fréquence, sa durée dans le temps, renseignera inévitablement sur le comportement d'une personne, et par inférence, autoriserait selon cet arrêt du Conseil d'Etat une possible ré-identification interdisant de le considérer comme anonyme.

Ce nouvel « or *numérique* » que représente la donnée, notamment dans des contextes de publicité comportementale et plus généralement afférent aux acteurs des objets connectés, se heurte donc frontalement à des exigences légales et réglementaires de plus en plus contraignantes, dont l'arrêt du Conseil d'Etat est sans conteste une manifestation éclatante de la rigueur à laquelle les acteurs économiques sont confrontés.

Jean-Guy de RUFFRAY
Avocat associé
Cabinet Altana

Notes

1 CE, 10ème et 9ème ch. réunies, 8 février 2017, n° 393.714

2 Délibération n° 2015-255 du 16 juillet 2015 refusant la mise en oeuvre par la société JCDecaux d'un traitement automatisée de données à caractère personnel ayant pour finalité de tester une méthodologie d'estimation quantitative des flux piétons sur la dalle de la Défense (demande d'autorisation n° 1833589)

3 L. 581-9 du code de l'environnement : "Dans les agglomérations, et sous réserve des dispositions des articles L. 581-4 et L. 581-8, la publicité est admise. Elle doit toutefois satisfaire, notamment en matière d'emplacements, de densité, de surface, de hauteur, d'entretien et, pour la publicité lumineuse, d'économies d'énergie et de prévention des nuisances lumineuses au sens du chapitre III du présent titre, à des prescriptions fixées par décret en Conseil d'Etat en fonction des procédés, des dispositifs utilisés, des caractéristiques des supports et de l'importance des agglomérations concernées. Ce décret précise également les conditions d'utilisation comme supports publicitaires du mobilier urbain installé sur le domaine public. Peuvent être autorisés par arrêté municipal, au cas par cas, les emplacements de bâches comportant de la publicité et, après avis de la commission départementale compétente en matière de nature, de paysages et de sites, l'installation de dispositifs publicitaires de dimensions exceptionnelles liés à des manifestations temporaires. Les conditions d'application du présent alinéa sont déterminées par le décret mentionné au premier alinéa. L'installation des dispositifs de publicité lumineuse autres que ceux qui supportent des affiches éclairées par projection ou par transparence est soumise à l'autorisation du maire. Tout système de mesure automatique de l'audience d'un dispositif publicitaire ou d'analyse de la typologie ou du comportement des personnes passant à proximité d'un dispositif publicitaire est soumis à autorisation de la Commission nationale de l'informatique et des libertés".

4 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

5 Loi n° 2016-1321 du 7 octobre 2016 pour une république numérique

6 MM. Gaëtan Gorce et François Pillet, "La protection des données personnelles dans l'open data : une exigence et une opportunité", mission d'information de la commission des lois du Sénat, 16 avril 2014

7 Avis n° 05/2014 du 10 avril 2014 sur les Techniques d'anonymisation du Groupe de travail "article 29" sur la protection des données

8 Décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

9 CE 10ème/9ème SSR, 23 mars 2015, n° 357556