21 décembre 2013
Bonnes feuilles

Du titre de transport au téléphone portable : quels objets du quotidien livrent nos données personnelles ?

À l'heure du tout numérique, la protection des données personnelles est devenue un enjeu majeur. Extrait de "Les données personnelles : quelle définition pour un régime de protection efficace ?" (1/2).

Avec Jessica Eynard

Au fil du temps, de plus en plus d'objets ont été marqués dans le but de les rendre reconnaissables. Déjà au XIXe siècle le gouvernement imposait le système d'immatriculation des véhicules172. Ce qui change avec l'évolution des nouvelles technologies c'est la nature des objets. Là où ces derniers étaient inertes, ils sont désormais communicants. Ils sont susceptibles de dialoguer à tout moment avec des récepteurs. Grâce à cette fonctionnalité, il suffit d'associer l'objet à son propriétaire pour avoir une connaissance approfondie de ce dernier. C'est ainsi que se développe l'identification par radiofréquence permise grâce à l'intégration d'une puce dans chaque objet.

Les puces RFID. Une puce dite « RFID » est composée d'une étiquette et d'une antenne qui lui permet de dialoguer avec des lecteurs par le biais des ondes radio. C'est à la fin des années 1960 que les premières applications à grande échelle de la RFID vont apparaître avec les systèmes permettant de détecter les objets volés à la sortie des magasins. Mais, à cette époque, la discussion entre la puce et le lecteur est limitée ; il ne s'agit que d'indiquer si le produit a été ou non dérobé. La puce ne contient qu'une information et ne sert qu'une seule fois. C'est avec les implants insérés sous la peau des animaux de compagnie dans les années 1990 que la possibilité de suivre un objet à la trace est devenue réalité mais c'est en 1999 que la RFID prend véritablement son envol avec l'idée de relier les objets dotés d'une puce à Internet173. Selon cette idée, une simple connexion sur la Toile devrait suffire pour savoir quels sont les lecteurs qui ont été ou qui sont en contact avec l'objet. De nombreux biens sont aujourd'hui dotés d'une puce dans un but de meilleure gestion des stocks ou de facilité et rapidité de passage. Le « passe Navigo » à Paris ou la « carte Pastel » à Toulouse qui permettent de prendre bus et métros en sont ainsi équipés ce qui permet de fluidifier le trafic mais aussi de savoir où la carte a été compostée, quel trajet a été effectué, à quelle heure et d'associer ces informations au titulaire de la carte. Le télépéage présente les mêmes spécificités en permett ant de passer sans s'arrêter aux péages et, en contrepartie, de connaître exactement l'itinéraire suivi par la voiture et le temps écoulé pour aller d'un péage à l'autre. Outre les puces RFID, d'autres objets semblent avoir la capacité de dialoguer et ainsi, de révéler des informations. Tel est le cas des téléphones portables, assistants personnels et systèmes de géo localisation présents par exemple dans les véhicules.

Les systèmes de géolocalisation. Se reportant aux données des satellites, les systèmes GPS174 permettent ainsi de localiser et de se localiser avec une grande précision. Les mobiles eux aussi sont susceptibles de devenir des objets révélateurs de position grâce aux antennes relais disséminées sur le territoire175. En fonction de l'antenne atteinte et du temps mis par l'onde pour parcourir la distance

entre le téléphone et l'antenne, il est possible de situer le mobile. Les portables peuvent encore en dire long sur le contenu de leur mémoire par le biais du système Bluetooth qui consiste à envoyer des paquets d'informations en utilisant les ondes radios. Grâce à ce protocole, il est possible de capter la liste des contacts, leur numéro de téléphone, les SMS176 reçus et envoyés ainsi que d'autres informations contenues dans un portable dont le mode est resté en « visible ». Enfin, c'est l'ordinateur qui peut servir d'intermédiaire pour en savoir davantage sur l'individu.

L'ordinateur. Lorsqu'une connexion à Internet est lancée, l'ordinateur est systématiquement identifié grâce à son adresse IP177. À chaque recherche effectuée, à chaque site visité, des informations associées à cette adresse sont envoyées et captées de sorte qu'il devient possible de savoir quelles actions ont été faites sur la Toile avec quel ordinateur.

Au premier abord, les informations dont il est question dans chacun des cas susvisés concernent un objet et non une personne physique ce qui conduit à exclure l'application de la loi informatique et libertés. Toutefois, au-delà de l'objet, n'est-ce pas l'individu que l'on cherche à atteindre ? Quel est l'intérêt pour un tiers de savoir où se trouve un objet si ce n'est pour localiser la personne qui le détient et suivre ses déplacements ? De même, pourquoi vouloir associer un ordinateur aux informations découlant de la navigation sur Internet si ce n'est pour surveiller l'internaute ou pour établir un profil de consommation ? Aussi, si les informations se rapportent directement à un objet, elles concernent indirecte ment une personne physique178. Cette idée est confirmée à la lecture de la directive 2002/58/CE179 du 12 juillet 2002 qui complète la directive 95/46/CE du 24 octobre 1995. Ce texte vise à introduire les dispositions protectrices des données personnelles dans le secteur des communications électroniques. Il prévoit l'application d'un régime protecteur pour les données de trafic et de localisation. Or, la donnée de localisation est par exemple définie comme « toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public »180. Il s'agit donc bien ici de protéger des données qui se rapportent à un objet parce qu'indirectement, elles concernent un individu.

En ce sens, doit être désapprouvé l'arrêt de la Cour d'appel de Paris181 aux termes duquel cette juridiction décide, en parlant de l'adresse IP, que « cette série de chiffres […] ne constitue en rien une donnée indirectement nominative relative à la personne dans la mesure où elle ne se rapporte qu'à une machine, et non à l'individu qui utilise l'ordinateur ». L'information, se rapportant indirectement à une personne, devrait pouvoir bénéficier des dispositions de la loi protectrice. Telle est la position prise par le Groupe de l'article 29182, par la Cour de justice des Communautés européennes183 et par la CNIL au regard de l'adresse IP184. Toutefois, se rapporter à une personne ne suffit pas pour entrer dans la catégorie des données à caractère personnel : encore faut-il que la personne soit identifiée ou identifiable. Cette difficulté a été soulevée avec acuité par la Cour d'appel de Paris qui a considéré que « l'adresse IP ne permet pas d'identifier le ou les personnes, qui ont utilisé cet ordinateur puisque seule l'autorité légitime pour poursuivre l'enquête (police ou gendarmerie) peut obtenir du fournisseur l'accès d'identité de l'utilisateur »185. Dans le même sens, le Conseil constitutionnel a décidé que les données recueillies par les sociétés de gestion et de perception des droits d'auteur et des droits voisins dont l'adresse IP n'acquéraient « un caractère nominatif que dans le cadre d'une procédure judiciaire et par rapprochement avec des informations dont la durée de conservation est limitée à un an »186. D'après ces juridictions, le fait que l'accès à l'identité de l'internaute ne soit possible qu'au terme d'une procédure stricte suffit à considérer ce dernier comme non identifiable. Elles en concluent donc que l'adresse IP n'est pas une donnée personnelle. Cette position paraît encore une fois critiquable au regard des termes mêmes des législations informatique et libertés qui exigent de prendre en compte tous les moyens susceptibles d'être raisonnablement mis en oeuvre pour savoir si une personne est ou non identifiable. Or, le simple fait d'avoir à ouvrir une procédure pour avoir connaissance de l'identité de l'internaute ne semble pas exiger des efforts déraisonnables de la part de celui qui prétend subir un dommage du fait du comportement de l'internaute. En outre, le raisonnement de la Cour laisse à penser que l'identification n'a lieu qu'à partir du moment où l'identité de l'internaute est connue or, sans toujours connaître le nom de l'individu, il est possible de l'identifier par sa seule façon de naviguer sur la Toile et par les sites qu'il visite. En revanche, aurait pu être soulevée par la Cour d'appel la possibilité pour une même machine d'être utilisée par plusieurs utilisateurs ou la possibilité pour une même adresse IP d'être attribuée à plusieurs ordinateurs connectés au même réseau local. Dans ces cadres, plusieurs internautes se cachent derrière une seule adresse IP si bien qu'il est légitime de se demander s'il est possible de les différencier et de savoir qui était devant l'ordinateur lors de telle connexion. Si la réponse à cette question est positive, le caractère identifiable de l'internaute sera acquis et l'adresse IP sera qualifiée de donnée personnelle sans aucun doute. Le plus simple face à cette interrogation est de procéder par situations, en analysant chaque cas de configuration. Le cas le plus répandu est celui de l'ordinateur familial, une machine servant à tous les membres d'une famille. Dans ce contexte, l'adresse IP de l'ordinateur pourra être associée à chacun des parents ou aux enfants. Or, il semble aisé de reconnaître quel membre de la famille est connecté grâce à la façon de naviguer et aux sites visités. Un jeune enfant, un adolescent, une adolescente, un homme, une femme, une personne âgée n' appréhendent pas la Toile de la même manière, ne cherchent pas les mêmes informations et ne réagissent pas de façon identique face à une page Web. À partir de ces différences, il est possible de définir quelle personne au sein du cercle familial est en train d'utiliser l'ordinateur. Mais, si cela est faisable pour un groupe restreint, il semble en tout état de cause que ce sera beaucoup plus difficile face à une multitude d'utilisateurs. En effet, comment identifier une personne derrière une machine implantée dans un cybercafé ou dans une bibliothèque si aucun code d'accès personnel ne permet d'accéder à l'ordinateur ? À cet égard, la condition d'identification ou de possibilité d'identification de l'individu semble impossible à remplir. Aussi, loin de conforter les positions prises par la CNIL, par la Cour de justice des Communautés européennes et par le Groupe de l'article 29, il faut admettre que l'adresse IP a une nature juridique variable si bien que sa qualification doit être le fruit d'une appréciation au cas par cas par les juges du fond. Soit il est possible d'identifier l'internaute au regard de sa navigation et dans ce cas l'adresse IP est une donnée personnelle, soit cela est totalement impossible du fait notamment du nombre élevé d'utilisateurs de la machine et d'absence de code pouvant personnaliser la connexion à l'origine et dans ce cas, l'adresse IP est une information quelconque non protégée par la loi informatique et libertés.

172. Une ordonnance de la Préfecture de Police de Paris du 14 août 1893 édictait : « Tout véhicule à moteur doit apposer une plaque métallique sur laquelle est inscrite de manière lisible le nom et l'adresse du propriétaire ainsi qu'un numéro d'autorisation. Cette plaque devra être fixée sur le côté gauche du véhicule et ne devra pas être cachée ». 173. Pour un historique complet, voir l'ouvrage de M. ALBERGANTI, « Sous l'oeil des puces. La RFID et la démocratie », Actes Sud, 2007, p. 55 et s.174. Abréviation de l'anglais

Global Positioning System. 175. À ce sujet, voir l'avis du G29, « Opinion 13/2011 on Geolocalisation services on smart mobile devices », WP 185, 16 mai 2011, op. cit. 176. Abréviation de l'anglais Short Message Service. 177. Abréviation de l'anglais Internet Protocol. 178. Pour les puces RFID, voir le document de travail du G29 sur les questions de protection des données liées à la technologie RFID (radio-identification), WP 105, 19 janvier 2005, op. cit.179. Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), JOCE L 201 du 31 juillet 2002, p. 37. 180. Art. 2 c), ibid. 181. CA de Paris, 13e chambre, Section A, S. c/ Ministère public et autres, 15 mai 2007, Juris-Data n° 2007-336454. Voir aussi l'arrêt Anthony G. c/ SCPP du 27 avril 2007 rendu par la même Cour, Section B, consultable à l'adresse http://www.legalis.net/jurisprudencedecision. php3?id_article=1954, l'arrêt Cyrille S. c/ Sacem, Sdrm du 1er février 2010 de la 12e chambre de la CA de Paris, Pôle 5, n° 09/02337, n° Lexbase A9354ETM ainsi que l'arrêt de la chambre criminelle de la Cour de cassation du 13 janvier 2009, n° 08-84088, Bull. crim. 2009, n° 13. 182. Avis 4/2007, op. cit., p. 18. 183. CJCE, arrêt Promusicae contre Telefónica, C-275/06, 29 janvier 2008. Dans un récent arrêt, la Cour confirme cette position. Selon elle, les adresses IP sont « des données protégées à caractère personnel car elles permettent l'identification précise (des) utilisateurs », arrêt Scarlet Extended SA contre Société belge des auteurs, compositeurs et auditeurs SCRL (SABAM), C-70/10, 24 novembre 2011, considérant 51. 184. Telle est aussi la conclusion du rapport d'information des sénateurs Y. DETRAIGNE et A.-M. ESCOFFIER au terme duquel ces auteurs recommandent d'affirmer sans ambiguïté que l'adresse IP constitue une donnée à caractère personnel, Rapport n° 441 fait par le groupe de travail relatif au respect de la vie privée à l'heure des mémoires numériques, 27 mai 2009, p. 98. Les conclusions de ce rapport ont été reprises dans une proposition de loi n° 93 visant à mieux garantir la vie privée à l'heure du numérique, enregistrée à la Présidence du Sénat le 6 novembre 2009 et adoptée par le Sénat le 23 mars 2010 sous le numéro 81. 185. CA de Paris, Anthony G. / SCPP, op. cit. 186. Considérant 13 de la décision n° 2004-499 DC du 29 juillet 2004 sur la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO du 7 août 2004, p. 14087.

Extrait de "**Les données personnelles : quelle définition pour un régime de protection efficace ?**", Jessica Eynard (**Michalon Editions**), 2013. Pour acheter ce livre, **cliquez ici.**