Vie privée et données personnelles

Melanie Dulong de Rosnay

Melanie Dulong de Rosnay, Vie privée et données personnelles, in Divina Frau-Meigs et Alain Kiyindou (dir.), *Glossaire critique sur la diversité culturelle à l'ère du numérique*, Commission Nationale Française de l'UNESCO, La Documentation Française, Janvier 2015, p. 292-296.

Vie privée / données personnelles

Développement des législations européennes

Les premières législations sur la protection de la vie privée ont accompagné le développement du fichage dans des bases de données informatisées dans les années 1970 en Allemagne, en Suède et en France. C'est après l'affaire Safari en 1974 qui vise à l'interconnexion des fichiers de l'administration que la CNIL, la Commission nationale de l'informatique et des libertés, est mise en place pour veiller à ce que l'informatique ne porte pas atteinte aux libertés individuelles ni à la vie privée. Le principe de la loi éponyme de 1978 est la déclaration a priori des traitements de données à caractère personnel, définies à son article 2 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. 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".
La loi pose des obligations pour la conservation de ces données : les principes de finalité, de proprotionnalité, d'exactitude, d'accès, de rectification et de sécurisation des données. La directive européenne 95/46/CE sur la protection des données personnelles reprend le principe de consentement expresse, ou *opt-in*, qui s'oppose à la pratique du *opt-out* où le citoyen doit explicitement interdire l'usage de ses données personnelles.

Les risques du traitement de grandes masses de données et des traces involontaires

Le développement des capacités de traitement des grandes masses de données (*big data*) et les révélations en 2013 par Edward Snowden sur l'existance de programmes de surveillance d'agences de renseignements en dehors de tout contrôle juridique donnent une ampleur sans précédent à la question de la protection de la vie privée sur internet. La collecte d'information par les fournisseurs de service s'accompagne de la constitution de traces numériques involontaires par les internautes lors de l'utilisation de tout système d'information connecté à l'internet, permettant le profilage comportemental et le ciblage à partir des recherches et des visites.
Le traitement de données personnelles peut avoir de simples visées marketing, mais peut aussi mettre en danger plus gravement la vie privée et la sécurité des personnes qui peuvent être réidentifiées par simple croisement de données même anonymisées. Associées avec des données de géolocalisation, les techniques d'analyse de données (*data mining*) permettent de proposer des services personnalisés, d'influencer les comportements, mais aussi de réduire l'espace de liberté. Elles peuvent conduire à des décisions d'exclusion, par exemple l'appréhension d'individus potentiellement soupçonnés de pratiques déviantes dans les dossiers scolaires ou dans les profils des passagers aériens ou dans l'appréciation du risque de crédit. Les technologies de surveillance permettent de suivre les activités des employés et des membres de la famille sans qu'ils en soient informés. L'absence de maîtrise technique et juridique sur le devenir ses propres informations, renforcées par la réidentification et la collecte involontaire, menace le libre arbitre et la liberté d'expression.

Les stratégies de réappropriation de ses propres données

L'analyse des données personnelles présente certains avantages pratiques, comme la mise à disposition de services personnalisés. Le phénomène de quantification de soi consiste à la captation de ses propres données, par exemple liées à sa santé avec une application sur son téléphone intelligent, afin d'en extraire des corrélations dans un but médical personnel et pour aider la recherche. Cette pratique se situe dans la lignée du partage volontaire des données publiques ou scientifiques lié au mouvement pour l'accès ouvert (*open data*). Certains actent la fin de la vie privée avec la divulgation volontaire d'informations sur les réseaux sociaux, dans lesquels les données personnelles de l'utilisateur constituent le produit qui est vendu à des entreprises, en échange desquelles l'utilisation du service est gratuite. La réalité des pratiques sociales est plus complexe et les adolescents développent des stratégies associant la révélation de l'intime avec des codes masquant la signification réelle des messages aux personnes extérieures.
D'autres proposent de mettre en place des mécanismes juridiques de réappropriation de ses propres données sur la base des droits de propriété ou des droits de personnalité, du droit à l'oubli ou du droit à la désindexation des moteurs de recherche. L'accès à ses propres données collectées par des gouvernements et des entreprises privées est une question économique, juridique, éthique, politique et technique : tout le monde n'a pas la capacité d'analyser ces données, de les visualiser pour mieux les comprendre ou en extraire des connaissances. La vie privée peut être perçue comme contextualisée, impliquant de concevoir les conditions de collecte et de partage de données afin de refléter le choix informé d'une personne en lien avec l'utilisation à laquelle elle consent. Et le consentement éclairé d'une personne à partager ses données personnelles ne peut pas vraiment être obtenu en lui imposant d'accepter un contrat d'une dizaine de pages au moment de la souscription à un service. Le projet de 2012 de réglement européen sur la protection des données prévoit que les informations données aux personnes devraient être transparentes et compréhensibles, la portabilité des données est également prévue.
Enfin, on voit se développer l'usage de la cryptographie et de services d'anonymisation pour chiffrer ses communications et limiter ses traces numériques. Ces applications se développent à la destination non seulement des informaticiens, mais aussi du grand public et des communautés à risque : les journalistes et les avocats qui doivent protéger leurs sources, les lanceurs d'alerte, les dissidents et les militants des droits humains menacés par des régimes politiques répressifs qui surveillent les communications et les données personnelles.
Les mécanismes législatifs et réglementaires de protection de la vie privée pouvant sembler inefficaces face aux capacités techniques de surveillance des entreprises et des gouvernements, l'autorégulation et le développement d'outils de gestion des données personnelles incluant le cryptage et la *privacy by design* paraissent la meilleure voie à même de garantir le respect de la vie privée et des libertés individuelles.

La négation de la diversité des approches

La diversité des positionnements éthiques et des stratégies de valorisation et de protection des données personnelles reflètent des différences importantes entre des régions du monde, des approches culturels et des idées politiques, des modèles économiques, des systèmes juridiques et des capacités techniques individuelles et collectives, reproduisant les divisions et rapports de pouvoir observés classiquement par les analyses critiques du libéralisme.
La vision occidentale de la vie privée oppose les normes anglo-saxonnes plutôt utilitaristes aux valeurs européennes continentales plus déontologiques, chacun des deux modèles de contrôle informationnel se retrouvant exporté dans les technologies et systèmes juridiques. Aux Etats-Unis, la réglementation des données personnelles est fragmentée entre des législations sectorielles, favorisant la collecte par les entreprises commerciales, qui vont typiquement détenir par défaut les données générées par les utilisateurs qui pourront bénéficier d'une possibilité de retrait. Au contraire, l'approche européenne privilégie le consentement explicite des individus qui bénéficient

de droits auxquels ils ne peuvent pas renoncer, imposant des coûts aux entreprises et administrations qui ne peuvent pas utiliser les données pour un autre propos que celui pour lequel elles ont été collectées et le consentement a été obtenu.
Le droit au respect de la vie privée fait l'objet de l'attention de la Déclaration universelle des droits de l'homme et du Pacte international relatif aux droits civils et politiques, et la protection des données personnelles fait l'objet de nombreuses normes régionales, les normes européennes étant les plus détaillées.
La transposition du concept individualiste de vie privée et les conceptions alternatives ont été moins étudiées dans les cultures dont les législations et les applications ne reflètent pas nécessairement les valeurs protégeant l'entreprise privée et la personne individuelle, les entités de base des systèmes occidentaux de contrôle des données personnelles. En Chine, les informations sur la famille ou la communauté seront encore peut-être plus sensibles que les données personnelles des individus. Au Japon, la personne pourra être protégée comme faisant partie d'un groupe. L'Inde s'est dotée en 2011 d'une législation sur la protection des données personnelles collectées par le secteur privé uniquement. L'Argentine a été reconnue par la Commission Européenne comme le premier pays d'Amérique Latine à donner un niveau de protection adéquat aux données personnelles.
La majorité des grandes plateformes et services en ligne étant basée aux Etats-Unis, leurs conditions d'utilisation ne sont pas favorables aux utilisateurs. Leur modèle de stockage, centralisé et en nuage, rend les données personnelles vulnérables. Les consommateurs européens pourront bénéficier de la protection que le droit communautaire accorde aux données personnelles à la condition qu'un contexte techno-juridique favorable parvienne à émerger. Cela implique que la recherche et les entreprises européennes développent des services en ligne concurrents des plateformes américaines et aux architectures décentralisés. Il sera également nécessaire que l'Europe parvienne à imposer des valeurs de confidentialité et de respect de la vie privée dans le règlement européen sur la protection des données et les accords bilatéraux comme le Partenariat transatlantique de commerce et d'investissement (TTIP).

Bibliographie

Dan Burk, Privacy and Property in the Global Datasphere, in Soraj Hongladarom, Charles Ess (eds), *Information Technology Ethics: Cultural Perspectives*, 2007, Hershey: Idea Group Reference, pp 94-107.

Jessica Eynard, L'éthique à l'épreuve des nouvelles particularités et fonctions des informations personnelles, *Éthique publique*, vol. 14, n° 2, 2012.

Toby Mendel, Andrew Puddephatt, Ben Wagner, Dixie Hawtin et Natalia Torres, *Étude mondiale sur le respect de la vie privée sur l'Internet et la liberté d'expression*, Éditions UNESCO, 2013, 158 pp.

Masahiko Mizutani, James Dorsey, James H. Moor, The internet and Japanese conception of privacy, *Ethics and Information Technology*, 2004, Volume 6, Issue 2, pp 121-128.

Helena Nissenbaum, A Contextual Approach to Privacy Online, *Daedalus, the Journal of the American Academy of Arts & Sciences*, 140 (4), Fall 2011: 32-48.

Liens avec d'autres termes du glossaire

algorithme
identité numérique
privacy