PAR CLAIRE LEVALLOIS-BARTH

maître de conférences en droit à Télécom ParisTech, coordinatrice de la chaire Valeurs et politiques des informations personnelles

L'**utilisation** raisonnée des données **personnelles**

Les *big data* soulèvent des questions d'autonomie, de libre choix et de confiance. Ces enjeux philosophiques rejoignent la question du respect des libertés et des droits fondamentaux du citoyen. Est notamment concerné le droit à la protection des données personnelles.

Une enseigne américaine s'est retrouvée au cœur d'un scandale, un père ayant découvert la grossesse de sa fille mineure parce qu'elle recevait des publicités de produits pour nourrisson ciblant les femmes qui attendent un enfant.

Les machines comme les individus produisent en temps réel un volume croissant de données variées, structurées ou non. D'infinies possibilités de création d'applications et de richesse semblent s'offrir à nous, sachant qu'aujourd'hui le traitement des données de masse joue un rôle majeur pour améliorer les offres de services, la sécurité des produits, l'analyse des risques, ou pour prévenir les maladies, les fraudes ou la criminalité.

Les* big data *accroissent les possibilités de recoupement des données

Une société de surveillance et d'anticipation

Parmi les données traitées se trouvent des données personnelles, à savoir des données qui concernent des personnes physiques. Réalisée à la fois par les entreprises et les États, la capture en masse de ce type de traces numériques concourt à la construction d'une société de la surveillance. En témoigne la récente controverse sur la transmission de données d'utilisateurs d'Internet par des multinationales comme Google, Apple, Microsoft ou Facebook aux services de renseignements américains. C'est également une société de l'anticipation, voire de la prédiction, qui se dessine.

Une vigilance accrue

L'analyse du caractère « personnel » d'une donnée doit prendre en compte tous les moyens permettant d'identifier une personne, y compris les moyens qui ne sont pas directement accessibles à l'entreprise procédant au traitement des données de masse. La vigilance s'impose car *big data* et *open data* accroissent considérablement les possibilités de recoupement des données et donc d'identification d'une personne. Une fois repérées les données personnelles, leur traitement – leur collecte, utilisation, transmission et interconnexion – doit se conformer à l'ensemble des obligations fixées par la loi Informatique et Libertés. L'opération peut se révéler complexe. Ce faisant, la loi Informatique et Libertés contribue également à protéger la liberté de déplacement, la liberté de penser, le droit à la non-discrimination, le droit au respect de la vie privée.

REPÈRES

La création et l'usage des données personnelles sont réglementés en France par la loi Informatique et Libertés de 1978 qui, dans sa version modifiée, transpose la directive européenne Protection des données personnelles de 1995. Les données personnelles consistent en « 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 ». Cette définition, interprétée de façon large par la Commission nationale de l'informatique et des libertés (CNIL) et ses homologues européennes, couvre à la fois des informations directement nominatives (nom et prénom, adresse postale ou électronique) et des informations indirectement nominatives telles que le numéro de téléphone d'un individu.

Confidentialité et sécurité

La loi Informatique et Libertés fixe d'autres obligations telles que l'obligation de confidentialité et de sécurité des traitements de données personnelles.

Finalité et droit à l'oubli

Les données personnelles doivent être collectées et traitées pour des « finalités » (c'est-à-dire des usages) « déterminées, explicites et légitimes » ; elles ne doivent pas être traitées ultérieurement de manière incompatible avec ces finalités. Ce principe, qui irrigue tout le champ de la protection, est un préalable au principe de qualité des données.

D'une part, seules les données nécessaires et pertinentes pour atteindre les finalités doivent être collectées. D'autre part, la durée de conservation des données ne doit pas excéder la durée nécessaire aux finalités pour lesquelles elles sont collectées. Passé ce délai, les données doivent être détruites. Apparaît ainsi un droit à l'oubli.

Dans un monde de *big data* fondé sur une méthode inductive et non plus déductive, un monde où l'analyste cherche à établir des corrélations entre plusieurs informations sans hypothèses prédéfinies, comment respecter ces obligations ? Une solution, qui est loin de répondre à l'ensemble des problèmes posés, consiste à utiliser la marge de manœuvre offerte par la loi Informatique et Libertés, celle-ci précisant qu'un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données.

L'obligation d'information

L'obligation d'information implique, quant à elle, d'avertir la personne de la collecte des données personnelles et de leur utilisation. Cette étape de transparence est primordiale car elle conditionne l'exercice du droit d'accès aux données personnelles et du droit d'opposition. En accordant à la personne un certain contrôle sur ses propres données personnelles et sur son image informationnelle, elle constitue un élément important de confiance.

Le droit d'information est allégé lorsque les données collectées sont très vite rendues anonymes ou lorsque les données ne sont pas recueillies directement auprès de la personne. Il est même exclu lorsque l'information de la personne « se révèle impossible ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche ». La CNIL admet l'application de cette exception tout en l'assortissant de garanties portant sur la délivrance d'une information générale, « sur un site Internet dédié par exemple ».

Une réflexion au cas par cas

La loi Informatique et Libertés ainsi que la doctrine de la CNIL fournissent un cadre légal mais n'apportent pas une solution « clé en main ». Pour utiliser les données personnelles de façon raisonnée, une réflexion globale au cas par cas se révèle nécessaire pour parvenir à un « juste » équilibre entre la protection du citoyen et l'intérêt légitime poursuivi par l'entreprise procédant à l'analyse des *big data*. Cette analyse devra prendre en compte les paramètres éthiques et sociétaux, notamment la façon dont les utilisateurs perçoivent la protection de leur vie privée selon le contexte dans lequel s'opère l'utilisation des données personnelles : le traitement de données médicales de masse sera perçu différemment s'il a pour objectif de prévenir une épidémie ou d'afficher de la publicité en ligne pour des produits coupe-faim.

La capacité à innover dans l'intérêt de l'ensemble des parties prenantes – entreprise, citoyen, État, société dans son ensemble – suppose alors d'intégrer le plus en amont possible la dimension « protection des données personnelles ». Il s'agit de mettre en place une démarche globale de *privacy by design* impliquant une personne spécialement formée, par exemple un correspondant Informatique et Libertés (CIL), et l'ensemble des opérationnels (service marketing et juridique, direction des systèmes d'information, etc.).

Il peut également être pertinent de consulter la CNIL. Cette démarche ne doit pas être considérée comme une contrainte mais comme l'occasion d'instaurer un véritable dialogue. Cette évolution vers moins de procédure administrative au profit d'une démarche d'*accountability* (responsabilité) est clairement perceptible dans la proposition de règlement Protection des données personnelles de 2012.

Ce processus continu permet à l'entreprise de s'assurer qu'elle utilise à bon escient les données personnelles *via* des outils variés : adoption de règles internes, analyses d'impact, formation des personnels, audits, etc. Le recours à ces outils contribue alors à faire de la protection des données personnelles un label de qualité dans le cadre d'un usage raisonné des données contribuant à la construction d'un véritable climat de confiance. ■

Intégrer le plus en amont possible la dimension Vie privée et données personnelles