Les nouvelles technologies et la maîtrise des données personnelles – comment l'Allemagne et la France abordent-elles l'impact de l'évolution technologique sur la protection des données ?

SONJA KORSPETER ET ALAIN HERMANN*

La microélectronique et les techniques d'information et de communication continuent de se développer en permanence. Ainsi la vision d'une « informatisation » et connexion globale du monde et de ses objets du quotidien devient de plus en plus proche, un développement qui est décrit comme l'informatique omniprésente (réf. F.Mattern, ETH Zürich). Les étiquettes utilisant le principe RFID, les téléphones portables multimédia et les puces des cartes de crédit et cartes d'identité en sont les premiers signes. Bientôt des millions de capteurs miniatures sans fil reliés en réseau pourraient être installés dans notre environnement ou de manière invisible dans les objets.

Grâce aux nouvelles technologies de localisation, des objets très banals acquièrent une valeur complètement nouvelle. Ils peuvent ainsi déterminer l'endroit où ils se trouvent, quels autres objets ou personnes se trouvent dans les environs et ce qui s'est produit dans le passé. A long terme se dessine un « Internet des objets » qui devrait avoir des effets durables sur de nombreuses transactions économiques et de vastes domaines de la vie privée et sociale. La Commission européenne l'a aussi reconnu et a publié en 2009 le document « Internet des objets – plan d'action pour l'Europe ».

* Sonja Korspeter est conseillère politique de l'European Milk Board, Alain Hermann est ingénieur pour la compagnie Procter & Gamble. Le texte n'engage que ses auteurs.

Le traitement omniprésent des données exige une infrastructure conséquente pour acquérir et analyser en permanence les données personnelles, ce qui permet accessoirement une surveillance potentiellement parfaite. Parmi les personnes pouvant être intéressées par ces données on trouve par exemple des fournisseurs de services et de produits, des employeurs, assureurs, services de renseignement ou organes étatiques de surveillance mais aussi le voisin curieux ou un amant jaloux. Pour que ces innovations technologiques rendent le monde meilleur, selon A. Roßnagel de l'université de Kassel, il faut arriver à séparer les potentiels de réalisation des rêves, des potentiels d'accomplissement des cauchemars. L'Etat a pour devoir d'encourager la liberté, l'épanouissement et la démocratie mais aussi de protéger des contraintes techniques. Le cadre législatif européen et les lois allemandes et françaises ainsi que leur application remplissent pour le moment ce devoir dans le domaine de la protection des données, mais il est tout de même de plus en plus clair qu'ils ne seront plus suffisants dans le futur.

Prise de conscience de l'importance de la protection des données

Le graphique ci-dessous montre l'évolution qualitative de la conscience de l'importance de la protection des données dans la population en France et en Allemagne, où des tendances semblables peuvent être observées : le sujet « protection des données » a gagné en importance à la fin des années 70 et au début des années 80, bien que les moyens technologiques de surveillance aient été très limités par rapport aux possibilités actuelles. C'est à cette période qu'ont été mises en place les autorités de protection des données. Dans les années 90 le sujet a perdu en importance dans le débat public. Après les attaques terroristes de 2001 et les modifications législatives qui en ont découlée, la conscience de la nécessité de la protection des données a crû de nouveau, mais pas suffisamment rapidement pour adapter les lois et les comportements aux fulgurants développements technologiques (Street View, réseaux sociaux, Smartphones, systèmes de localisation…)

Il s'agit maintenant de continuer à développer au plus vite la conscience et l'éducation de la population sur l'importance de la protection des données, pour que les individus et les organisations puissent s'adapter aux opportunités et aux risques des possibilités technologiques actuelles et futures.

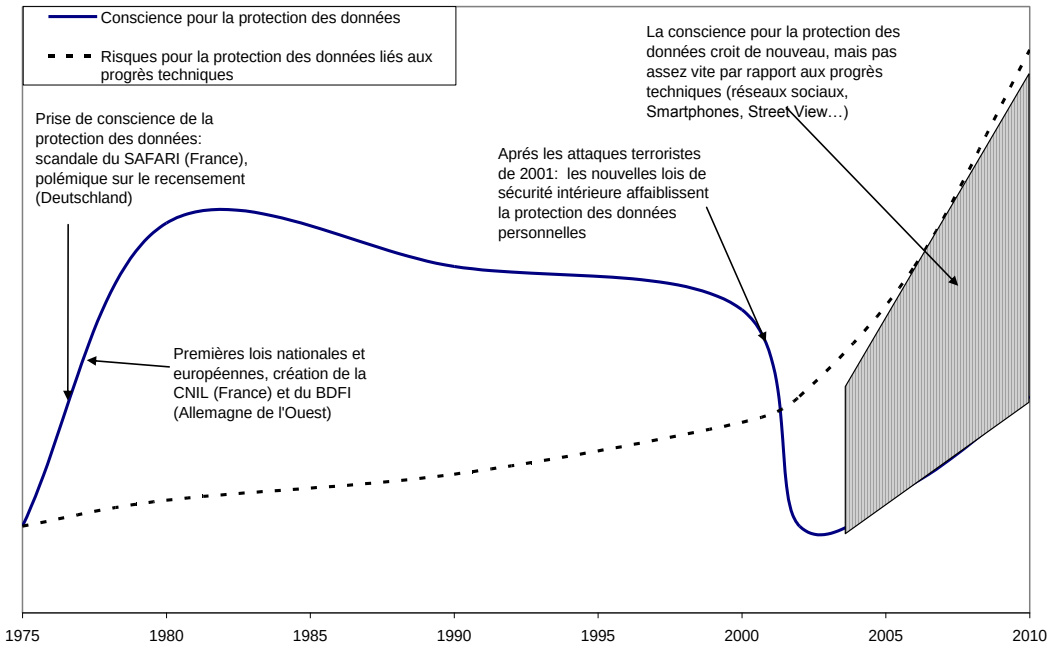

Fig 1: Évolution de la prise de conscience de la protection des données en France et en Allemagne de l'Ouest (1975-2010) (représentation des auteurs)

La dernière étude de l'Institut Allensbacher sur la protection des données montre que la conscience de la sensibilité des données personnelles augmente certes, mais aussi que de grandes lacunes subsistent sur ce qu'il advient des données personnelles et où se situent les limites légales de leur utilisation par des tiers. Une nouvelle tendance apparaît toutefois dans les deux pays à l'abandon « en toute conscience » de l'intimité, comme le formule Rainer Kuhlen : « A l'ère du commerce électronique, de Facebook et autres services personnalisés, l'intimité est considérée de moins en moins comme une condition absolue à une vie autodéterminée, mais plutôt comme un bien négociable et auquel on peut renoncer partiellement. De plus en plus de personnes sont prêtes à renoncer volontairement à leur droit à l'intimité s'ils en tirent un avantage matériel suffisant (par exemple des réductions pour les titulaires de cartes de fidélité, des rabais offerts par les assureurs automobiles qui peuvent en contrepartie analyser la manière de conduire de l'assuré) ». En particulier les jeunes fournissent d'eux-mêmes de nombreuses informations sur les réseaux sociaux comme Facebook ou les forums Internet.

Les nouveaux défis de la protection des données

Une protection efficace des données est indispensable pour empêcher la mise en place d'une société « transparente » sans aucune sphère intime pour les individus. Dans une telle société les individus échangeraient non seulement beaucoup moins d'informations, mais ils auraient tendance à se retirer de la vie sociale et politique, de peur que leurs données personnelles soient

détournées et que l'on puisse ainsi connaître en détail leur personnalité. Le commerce est également menacé, si les entreprises doivent craindre que leurs données confidentielles se retrouvent dans de mauvaises mains. Déjà aujourd'hui le manque de protection des données engendre des pertes économiques importantes : une étude globale du fabricant d'anti-virus Symantec en 2010 a montré que les PME ont dû subir en moyenne une perte de 188 000 dollars par an. Les objectifs poursuivis par le traitement croissant et omniprésent des données sont partiellement contraires à ceux associés aux principes de droit de la protection des données. Un des défis principaux pour l'adaptation de la législation consiste justement à considérer le fait que, dans la plupart des cas, la collecte de données est souhaitée par les utilisateurs. Ainsi par exemple, l'enregistrement des données et la création d'un profil personnel sont clairement souhaités par les millions d'utilisateurs de Facebook. Les principes actuels de la protection des données – transparence, spécificité et depuis quelques années également nécessité et parcimonie – ne sont donc plus suffisants.

Nous voyons trois domaines d'action qui devraient être examinés pour qu'Internet et les technologies associées continuent de promouvoir dans le futur la liberté d'expression et l'activité économique.

L'adaptation de la législation sur la protection des données

Les législations nationales actuelles sont issues des normes européennes. Au niveau des Etats membres, peu de différences institutionnelles sont à remarquer. Tous les grands pays ont une autorité de protection des données comme la CNIL (Commission Nationale de l'Informatique et des Libertés) en France ou le BFDI (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit) en Allemagne. Toutefois, comme le fait remarquer Alex Türk, le président de la CNIL, la collaboration au niveau international doit s'approfondir pour un meilleur échange des expériences et expertises technologiques et judiciaires des différents pays. C'est le seul moyen pour les autorités de s'adapter aux défis technologiques qui se renouvellent en permanence[1].

En premier lieu les lois de protection des données personnelles doivent s'adapter aux évolutions technologiques. Par exemple la création de profils personnels doit être réglementée de telle sorte qu'elle ne soit pas complètement interdite mais soit rendue transparente et influençable. Les utilisateurs devraient savoir autant que possible qui utilise leurs propres données et dans quel but et pouvoir s'opposer directement sur Internet à l'utilisation de leurs données. Le niveau de base de la protection des données doit aussi être précisé dans la législation. Les fournisseurs de produits et

[1] Alex Türk, "28th Conference of Data Protection and Privacy Commissioners", London, Grande-Bretagne 2/3 novembre 2006

services doivent assurer que les paramètres de base garantissent un haut niveau de protection des données personnelles, qui est ensuite seulement modifiable, en toute conscience, par l'utilisateur.

La protection de leurs propres données par les individus

Toutefois, au delà du cadre législatif, les mesures préventives doivent être fortement étendues. Ainsi, de même que le terrorisme ne peut pas uniquement être combattu par les organes de police mais nécessite également une population vigilante, la protection de données ne peut pas être uniquement assurée par les autorités. La méthode la plus efficace est que chacun protège ses propres données. Si les citoyens fournissent leurs données consciemment et avec prudence, le risque qu'elles soient détournées à de mauvaises fins est fortement réduit. Le gouvernement fédéral allemand veut montrer, avec la création prévue de la fondation de « financement de la formation au maniement des données », qu'il a reconnu l'importance du fait que chaque citoyen protège ses données. L'aptitude à manier ses propres données devrait également être incluse dans les programmes scolaires. La « Bundeszentrale für Politische Bildung » ainsi que les organismes de protection des données pourraient aussi participer à cet effort en fournissant du matériel de formation adapté aux publics visés.

La CNIL fournit sur son site web une grande quantité d'informations sur les droits et devoirs des citoyens et des entreprises et donne également des conseils sur la manière de protéger les données personnelles et confidentielles. Un site web dédié aux jeunes de 10 à 16 ans (www.jeunes.cnil.fr) leur explique comment les données qu'ils fournissent maintenant sont enregistrées et pourraient être utilisées contre eux pendant leur future vie d'adulte. Il y a donc déjà plusieurs initiatives de qualité qui portent leur effet : un sondage de 2007 indique que 50% des personnes interrogées connaissent la CNIL. Le degré de notoriété a ainsi progressé au cours des années précédentes (34% seulement en 2004) mais il doit encore augmenter : seulement 26% des Français ont l'impression d'être suffisamment informés sur leurs droits. Les autorités de protection des données doivent être encore plus présentes dans les médias, pour que le grand public soit mieux informé des risques associés aux nouvelles technologies et puisse ainsi manier en toute conscience ses propres données et celles des autres.

Les citoyens peuvent aussi exercer en tant que consommateurs de la pression sur les fournisseurs de produits et services, afin que ceux-ci respectent des standards acceptables de protection des données. Au cours des dernières années les labels de qualité « Bio » et « commerce équitable » ont fortement gagné en importance et sont la preuve que les consommateurs sont prêts à récompenser les entreprises dont les produits sont fabriqués en respectant certains standards de qualité.

Autorégulation des entreprises traitant des données personnelles

Selon nous un troisième champ d'action pourrait conduire à un changement fondamental : les entreprises devraient voir dans le futur la protection des données comme une opportunité et non comme une contrainte, de telle sorte que cette protection soit considérée dès les premières étapes de développement des produits. Un tel procédé serait pour les fabricants beaucoup plus simple et économique que de devoir modifier les produits après leur mise sur le marché, car certains critères n'auraient pas été respectés. L'objectif doit être d'inclure la protection des données dès la conception des produits, afin de se démarquer de manière positive de la concurrence.

Le projet EuroPriSe (European Privacy Seal – Label de qualité européen de protection des données) donne la possibilité aux entreprises informatiques de faire tester leurs produits, de manière volontaire, par des experts indépendants en protection des données. Ainsi les entreprises certifiées bénéficient d'un avantage concurrentiel. Les médias et les autorités de protection des données peuvent contribuer à faire connaître ce type de projets dans la population, afin que les consommateurs puissent soutenir, par leurs décisions d'achat, des produits conformes aux standards de protection des données.

En conclusion nous souhaitons insister sur le fait que la collaboration au niveau européen et international est essentielle au succès de la protection des données personnelles dans un monde où le traitement des données est omniprésent. Wikileaks, Google Street view, capteurs miniatures : ces quelques exemples montrent que, même si les législations nationales peuvent s'appliquer, les données ne s'arrêtent pas aux frontières, ce qui nécessite l'implémentation de normes rigoureuses, reconnues au niveau international. L'Allemagne et la France, avec leurs autorités de protection des données bien établies et leurs populations impliquées devraient également dans ce domaine jouer un rôle déterminant et montrer l'exemple avec une législation sans équivoque, un programme d'information et de prévention et le soutien de la responsabilité des entreprises.