La protection des données personnelles, un enjeu organisationnel et technique*

Guillaume Piolle†

2013

1 De la réglementation inconfortable à l'impératif opérationnel

Depuis l'avènement de la loi "Informatique et Libertés"en 1978, l'image de la protection des données personnelles auprès du public et de l'industrie a beaucoup évolué. Originellement motivée par un besoin de contrôle des capacités de traitement et de recoupement de fichiers de l'État, son application à l'ensemble des acteurs a pu en faire la bête noire de certaines entreprises. En effet, la loi 78-17 est une collection de règles très contraignantes sur la collecte, le traitement, la conservation, la transmission... de toute information se rapportant à une personne physique, ce qui peut impacter une part significative de l'activité économique. Si l'explosion des usages sur Internet a rendu encore plus prégnantes ces contraintes, elle a également accentué la prise de conscience des risques liés à la vie privée et de la nécessité des précautions liées à la manipulation de données à caractère personnel, afin d'éviter des "brèches de vie privée"qui peuvent s'avérer désastreuses pour les personnes concernées, pour l'image des organisations impliquées et pour la sécurité de leur patrimoine informationnel. Aujourd'hui, le renvoi dos à dos des exigences de la protection des données personnelles, de la sécurité des systèmes d'information et des impératifs métier de l'entreprise semble relégué à un combat d'arrière-garde. La protection de la vie privée (non limitée au simple respect de la loi de 1978) est devenue l'un des principaux axes de travail des RSSI, en intrication avec les autres exigences de confidentialité et d'intégrité.

En janvier 2012, la Commission européenne a fait une proposition de règlement pour remplacer la directive européenne sur la protection des données personnelles. Le Parlement, les agences nationales de protection des données (la CNIL en France), les agences européennes concernées ainsi que divers groupes d'intérêt travaillent depuis à converger sur une nouvelle version du texte. Entreprises et administrations réfléchissent déjà aux moyens de mettre en œuvre les probables futures dispositions, en particulier l'obligation de notification des brèches de vie privée (à la CNIL et aux personnes concernées), actuellement limitée aux seuls opérateurs de télécommunications, le *Privacy Impact Assessment* qui devra précéder toute demande d'autorisation, ainsi que les exigences du *Privacy by Design*, qui veut que la protection de la vie privée soit prise en compte dès la phase de spécification d'un système. Au cœur des controverses, on trouve également la mention – sinon la définition – d'un "droit à l'oubli"spécifique, qui modifierait le droit à la suppression des données, suscitant sans aucun doute des attentes significatives de la part des usagers.

2 La nécessité d'une approche transdisciplinaire

L'activité de recherche informatique dans le domaine de la protection de la vie privée et des données personnelles est liée aux travaux en sécurité informatique des trente dernières années. Depuis quelques années cependant, la protection de la vie privée devient un champ disciplinaire à part, avec ses problématiques propres, qui deviennent plus évidentes avec la distribution massive, sur Internet, des données et des applications. L'une des particularités du domaine, devenue de plus difficile à ignorer, est l'inefficacité des approches purement informatiques (ou purement juridiques) de la question. La vie privée est une problématique essentiellement humaine comprenant une grande part de subjectivité. Les risques associés ont

*Ce document est une version auteur d'un article initialement publié dans *Flux* [Pio13].

†guillaume.piolle@supelec.fr – SUPELEC, équipe CIDRE, CS47601, Avenue de la Boulaie, 35576 Cesson-Sévigné Cedex, France.

des causes de nature à la fois organisationnelle et technologique et, comme on l'a vu, les activités liées aux données à caractère personnel sont encadrées par le droit national et communautaire. C'est pour ces raisons que la recherche associée est souvent menée de manière transdisciplinaire, associant des spécialistes de divers domaines, essentiellement informatique et droit, mais aussi philosophie, sociologie ou psychologie. Aux questions spécifiques à chaque discipline s'ajoute alors le défi d'une réelle rétroaction entre les différentes approches et les différents résultats. L'informatique juridique, champ disciplinaire s'intéressant notamment à la modélisation informatique de concepts issus du droit et à l'application de méthodes de décision et d'intelligence artificielle à ces concepts, est un exemple particulier de collaboration transdisciplinaire particulièrement adaptée aux problèmes de la protection des données personnelles.

3 Les travaux de recherche de l'équipe CIDRE

Lorsque l'équipe de recherche SSIR de Supélec, sur le campus de Rennes, est devenue CIDRE, deux nouveaux axes de recherches ont été ajoutés à l'activité existante en détection d'intrusion : la gestion de la confiance et la protection de la vie privée. En ouvrant ce dernier domaine, l'équipe met à profit les résultats d'une communauté de recherche en essor, pour y intégrer son expertise en sécurité informatique et en systèmes distribués.

Une piste de recherche naturelle pour l'équipe est de valoriser son travail sur les politiques de sécurité pour développer la **protection de la vie privée guidée par les politiques**. L'utilisation d'outils issus de l'intelligence artificielle symbolique et de l'informatique juridique permet d'envisager la modélisation et le raisonnement automatique sur un contexte réglementaire donné en matière de protection des données personnelles. L'objectif, séduisant, est de permettre un *Privacy by Design* efficace autorisant la conception de systèmes auto-adaptatifs, modifiant leur comportement de manière autonome pour protéger au mieux des données sensibles en regard d'un ensemble de règles de diverses natures. Cependant, les difficultés sont nombreuses et variées : complexité sémantique des règles à modéliser, hétérogénéité des contextes juridiques, gestion fine des contraintes temporelles et des conflits normatifs, et bien sûr légitimité de la machine à prendre une décision ayant un effet juridique.

Un autre axe de recherche, plus centré sur les applications, concerne **la vie privée dans les réseaux sociaux distribués**. Les réseaux sociaux classiques, construits sur un modèle client-serveur centralisé, cristallisent (à tort ou à raison) une grande part de l'inquiétude du public quant à sa vie privée. Dans ce schéma, un prestataire unique a accès à l'ensemble des informations de profil, d'usage et de communication des utilisateurs, qui bien souvent constitue une source de revenus significative, via l'exploitation ou la revente de profils comportementaux. C'est en ce sens que l'on dit parfois que les données personnelles sont devenues le "carburant"d'Internet. De nombreux projets ont vu le jour, visant à concevoir des architectures de réseaux sociaux distribuées, ne permettant pas à un acteur unique un contrôle trop grand sur les données. L'équipe CIDRE s'intéresse aux problématiques spécifiques à ces propositions : compromis entre confidentialité et disponibilité des données, application distante de politiques, prise en compte de la notion de finalité, mise en œuvre du droit à l'oubli…

La troisième orientation de recherche poursuivie, en lien avec la précédente, s'intéresse aux applications géo-localisées. Que de telles fonctionnalités soient intégrées ou pas à des réseaux sociaux, elles présentent un risque de profilage et de traçage particulier et prêtent le flanc à de nombreux types d'attaques sur les données. Les travaux au sein de l'équipe consistent notamment à analyser ces attaques possibles, caractériser les informations supplémentaires qu'elles permettent d'inférer sur les personnes et mettre au point des techniques pour rendre impraticables ces attaques.

References

[Pio13] Guillaume Piolle. La protection des données personnelles, un enjeu organisationnel et technique. *Flux*, (274) : pp. VIII–IX, mars-avril 2013.