

INTRODUCTION DE LA SESSION SUR LA PDP

Mme Isabelle Falque-Pierrotin – CNIL

Au nom de la Commission française Informatique et liberté, et de l'Association francophone des autorités de protection des données personnelles, je suis particulièrement heureuse d'ouvrir cette session dédiée à la protection des données personnelles.

Comme j'avais déjà pu en faire état lors de mon allocution d'ouverture de cette matinée, le droit à la protection des données personnelles est un droit récent. C'est aussi un droit encore assez méconnu. Ce droit est cependant devenu, face au développement de la société de l'information et de l'explosion d'Internet et des nouvelles technologies, un droit essentiel et incontournable.

Mais tout d'abord qu'entend-on par protection des données personnelles ? Ce point sera traité plus en détail dans le cadre des interventions ultérieures. Disons seulement qu'il s'agit avant tout de protéger les personnes à l'égard des traitements d'informations permettant de les identifier, directement ou indirectement.

Comme le rappelle l'article 1^{er} de la loi française de l'informatique et des libertés, « l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».

Pourquoi ce droit est-il devenu si incontournable aujourd'hui ?

Nous avons aujourd'hui à faire face à au moins deux défis (ou enjeux) majeurs :

Il s'agit du défi technologique et du défi de la mondialisation.

Les enjeux de la protection des données personnelles

Le défi technologique

Internet, téléphonie mobile, biométrie, géolocalisation, rfid...autant de technologies en développement exponentiel, autant de technologies ambivalentes.

Ambivalentes pourquoi ?

Bien évidemment, les nouvelles technologies permettent des gains de productivité fulgurants dans la gestion des organisations, en matière de communication et d'accès à l'information et aux services.

Mais elles peuvent aussi présenter des risques majeurs pour les individus et par voie de conséquence pour les entreprises, les administrations et les Gouvernements.

Les fichiers informatiques, si l'on n'y prend pas garde, peuvent être facilement détournés ou divulgués à l'insu des personnes concernées.

En novembre 2007, des CD-ROMs contenant les données bancaires de 25 millions de contribuables sont égarés par les services fiscaux britanniques. En Avril 2008, la première banque britannique a perdu un CD-ROM contenant des informations sur 370 000 de ses clients...

En août 2008, la presse allemande a révélé qu'il était possible d'acheter sur Internet des fichiers de 6 millions de données confidentielles pour 850 euros...

Ces failles de sécurité, graves, montrent que la sécurité et de façon plus générale, la protection des données ne sont malheureusement pas toujours prises au sérieux par les entreprises et les administrations, que ce soit en Europe (comme dans les exemples cités) ou ailleurs dans le monde.

Autre exemple : la biométrie : cette technologie qui fait appel aux caractéristiques physiques ou physiologiques immuables du corps humain (empreintes digitales, iris, contour de la main, ADN...) peut apporter des services considérables pour sécuriser l'identité des individus mais elle doit être accompagnée de garanties fortes pour préserver les droits et libertés de chacun.

Autre exemple : naviguer sur internet, utiliser un moteur de recherche, sont autant d'occasions de communiquer des données sur soi, sur ses habitudes de vie de consommation, ses goûts, ses loisirs, et ainsi d'être peu à peu tracé dans tous les actes de sa vie courante. Or, qui dit diffusion de ses données sur internet, signifie aussi conservation par des tiers et réutilisation possible à toutes fins (y compris d'usurpation d'identité) et notamment commerciale, des sites et de leurs multiples partenaires commerciaux, de son futur employeur peut-être

Ces exemples montrent que la traçabilité numérique est aujourd'hui omniprésente. Elle doit être encadrée au risque de représenter un danger pour les libertés individuelles, au risque de détourner les internautes dont les données sont collectées, des usages, marchands ou non marchands qu'offre l'économie numérique.

Il est par conséquent impérieux pour nos sociétés d'accompagner le développement de ces nouvelles technologies en mettant en place un cadre juridique clair, pour les administrations et les entreprises, de nature à susciter la confiance des utilisateurs.

Le défi de la mondialisation

Les technologies sont universelles et, pour ce qui est de l'utilisation des nouvelles technologies, les frontières disparaissent.

De plus en plus d'entreprises européennes sous-traitent une partie de leurs activités informatiques à des entreprises basées dans des pays tiers. Ce phénomène « d'outsourcing » se développe rapidement, par exemple pour les centres d'appel et des services après-vente, dans le domaine de la gestion des ressources humaines, ou encore de la sous-traitance de la saisie informatique ; les coûts réduits des communications permettent même de délocaliser des services critiques d'une entreprise, tels que sa relation clientèle.

Ces pratiques impliquent bien évidemment la gestion de données personnelles :

Toutefois du point de vue des Etats européens, il n'est pas possible de transférer des données personnelles hors de l'Union européenne si le pays tiers n'offre pas une protection adéquate des données personnelles.

Aussi les sociétés européennes sont dans l'obligation de vérifier le niveau de protection des données du pays hôte avant de recourir à une externalisation.

Dès lors, disposer d'une loi de protection des données personnelles permet à un pays qui accueille des activités d'externalisation informatique d'offrir des garanties effectives quant à la protection des données personnelles et ainsi de rassurer les entreprises étrangères qui y investissent.

Une telle loi constitue donc un atout économique indéniable.

1. Quelle solution pour faire face à ces enjeux ?

Face à ces enjeux technologiques ou économiques, il convient de mettre en place des solutions juridiques. Ces solutions juridiques peuvent se trouver au niveau international mais aussi au niveau national.

Sur le plan international :

Des textes ont été élaborés au plan international en même temps que les premiers textes nationaux: lignes directrices de l'OCDE (1980), convention du Conseil de l'Europe (1981), principes directeurs de l'ONU (1990), directive européenne (1995), principes directeurs de l'APEC (2004), etc.

Tous ces textes s'articulent autour de principes communs en matière d'utilisation des données personnelles. Ceux-ci seront détaillés dans les interventions ultérieures de cette session.

Toutefois, nous pouvons d'ores et déjà affirmer que la collecte des données doit poursuivre une finalité légitime, que les données collectées doivent être pertinentes ; il convient d'assurer la sécurité des données collectées ou encore de consacrer le droit des individus à avoir accès aux données collectées, rectifier les données erronées, ou même s'opposer à la collecte de certaines données, etc.

Ces textes internationaux fournissent donc une base solide pour mettre en place, au plan mondial, un dispositif efficace et adéquate de protection des données personnelles.

Un tel besoin est clairement exprimé par les entreprises qui, nous l'avons dit, travaillent sur un marché mondial. Il est aussi ressenti par les individus, consommateurs de services de la société de l'information (e-commerce par exemple) auprès de sociétés qui peuvent être localisées partout dans le monde et avec lesquelles ils sont contractuellement en relation.

La Conférence internationale des Commissaires à la protection des données a souhaité participer à cette réflexion mondiale.

La 31^{ème} Conférence internationale a eu lieu à Madrid au début du mois de novembre 2009. Le 5 novembre 2009, les commissaires ont adopté une résolution visant à établir des standards internationaux sur la protection de la vie privée et des données personnelles. Ce texte offre pour la première fois un socle de principes communs à tous les Etats du monde entier et est le résultat de la conjugaison des différents systèmes juridiques nationaux et internationaux.

Certes, ce n'est qu'une première étape ; le droit international de la protection des données risque d'émerger lentement. La difficulté va maintenant être de s'entendre sur les mécanismes de mise en œuvre concrète de ces standards qui ne constituent aujourd'hui qu'un « droit mou ».

Mais, le mouvement international est lancé et il accompagne la mondialisation des économies et des usages.

A court terme, des solutions doivent être en parallèle recherchées au niveau national.

Sur le plan national :

Au plan national trois voies ont été tentées :

- **la voie de la déontologie des professionnels et de l'autorégulation** ; cette démarche se traduit par exemple par la mise en place de codes de conduite (privacy policy) définissant des bonnes pratiques de protection des données en l'absence d'obligations légales ; nous avons également vu se développer de nombreuses normes ISO dans le domaine de la protection des données. Cette approche est intéressante car elle est très proche du terrain et est respectée par les professionnels eux-mêmes mais elle reste insuffisante car bien souvent l'intérêt

économique des acteurs va primer sur la protection des données personnelles de l'individu.

- **La voie des législations spécifiques et sectorielles**, approche adoptée par exemple par les Etats-Unis d'Amérique, souvent en réaction à des scandales : the Fair credit reporting ACT- 1970 , the video privacy protection Act- 1988, the children's protection Act-1998..... Cette démarche peine cependant à régler de façon cohérente l'ensemble des questions relatives à la protection des données personnelles.
- **Celle de la régulation par la loi**, approche globale reposant sur une législation de portée générale fixant les principes de protection des données personnelles complétés d'un mécanisme de contrôle et de sanctions qui est l'approche européenne et notamment française. (à cet égard, Madame Vulliet-Tavernier exposera plus en détail les caractéristiques de la loi française sur la protection des données ainsi que les modalités concrètes de fonctionnement de la CNIL).

C'est bien sûr cette dernière voie, qui peut se combiner avec les deux autres, qui semble la plus de nature à construire un cadre complet de confiance et de compétitivité pour les individus comme pour les entreprises. L'autorégulation y est comprise comme un mécanisme de mise en œuvre des principes généraux de la loi et est contrôlée par un organisme indépendant.

L'approche européenne repose sur quatre axes essentiels :

- La reconnaissance du droit à la protection des données personnelles comme droit fondamental,
- La mise en place de normes en droit positif, précisant les règles à respecter notamment en matière de finalité des traitements, de conservation des données, de sécurité, d'information des personnes....
- L'institutionnalisation d'une autorité de contrôle indépendante, disposant de pouvoirs de contrôle et de sanction effectifs
- L'adoption de garanties juridiques appropriées s'agissant des flux transfrontières de données. Les flux transfrontières de données ne peuvent en effet se faire que

vers des pays offrant une protection des données personnelles « adéquate ». Cette adéquation peut être

Par exemple au niveau d'un Etat (reconnaissance de la protection adéquate par la Commission européenne ; Canada, Suisse, Argentine notamment ; en cours pour Israël), au niveau d'une entreprise (BCR ou règles d'entreprises contraignantes, adhésion d'une entreprise au Safe Harbor aux Etats-Unis), ou encore au niveau de l'exécution d'un contrat (clauses contractuelles de la Commission).

2. Quel est le bilan ?

Au total, à ce jour, plus de cinquante Etats dans le monde se sont dotés de législations relatives à la protection des données personnelles, la plupart au Nord, mais de plus en plus au Sud.

Tel est le cas des Etats européens, du Canada, Maroc, de la Tunisie, du Sénégal, du Bénin, du Burkina Faso en Afrique, de Maurice dans l'Océan Indien mais aussi, en Asie de la Thaïlande, qui élabore actuellement une loi en ce sens.

La création de l'association francophone des autorités de protection des données personnelles en 2007 a permis de renforcer la mobilisation politique internationale sur ces questions. La CNIL et l'AFAPDP ont ainsi entrepris de nombreux déplacements à l'étranger pour échanger avec les décideurs nationaux sur la question de la protection des données personnelles. La CNIL a également pu faire bénéficier de son expertise et de son expérience en élaborant un canevas législatif sur la protection des données personnelles.

Par ailleurs, la CNIL et l'AFAPDP viennent en soutien aux autorités de protection des données nouvellement installées, souvent sous la forme de stages d'échanges entre autorités. Ces stages sont l'occasion d'échanger des expériences et des bonnes pratiques dans le domaine de la protection des données.

En conclusion

J'aimerais donc insister en conclusion sur la nécessité dans un monde sans frontières d'adopter une approche globale et protectrice des données personnelles. Cette approche est indispensable, non seulement dans l'intérêt de l'individu, mais

aussi dans l'intérêt économique de l'Etat concerné qui favorise ainsi la compétitivité de ses entreprises.

L'association francophone des autorités de protection des données personnelles et la CNIL se tiennent ainsi à votre entière disposition sur l'ensemble de ces questions.