

Vie privée ou innovation : faut-il choisir ?

Les entreprises veulent innover. Pour cela, elles cherchent à mieux connaître leurs clients et développer avec eux une proximité. Mais cette proximité augmentée génère des risques si les utilisations de données collectées et manipulées ne sont pas canalisées.

Une véritable poudrière

Vie privée ou innovation, faut-il choisir ? Cette question nous a interpellés à l'occasion du tour d'horizon que nous avons réalisé sur le sujet du traitement des données personnelles.

Les applications et les services qui se créent autour d'avancées technologiques récentes telles que la RFID, la biométrie ou encore les objets communicants font appel de façon grandissante aux données à caractère personnel et font planer ainsi de nouveaux risques sur notre vie privée.

Si à l'avenir rien n'est fait pour mieux protéger les données personnelles, on peut craindre des réactions qui ne se limiteront plus aux mouvements de protestation des activistes, mais qui pourront éventuellement aboutir à une contestation généralisée.

"ProspectTIC 2010", exercice collectif de prospective technologique initié par la FING (Fondation Internet Nouvelle Génération) le soulignait bien dans sa synthèse finale : *"les nouvelles technologies contiennent un potentiel de transformation sans précédent, mais en même temps elles font émerger des méta-risques, voire même des questions proprement métaphysiques qui, s'ils ne sont pas explicités et discutés dès aujourd'hui, pourraient générer de violents chocs en retour"*.

Au-delà du risque sur la vie privée, il y aurait un autre risque, celui de remettre en question le progrès et l'innovation. Un effet particulièrement pervers qu'il vaudrait mieux éviter.

La tentation de l'immobilisme

Ce problème de la gestion des données personnelles tend à devenir une question particulièrement épineuse pour les entreprises. Comment innover, proposer de nouveaux services s'appuyant sur des données personnelles sans pour autant s'attirer les foudres de leurs clients et de leurs partenaires ?

Au centre de cette problématique, le DSI risque fort de se retrouver tiraillé entre deux attitudes opposées : prendre le parti de l'innovation avec tous les risques que cela comporte ou se réfugier dans l'immobilisme s'il ne peut pas prouver que les données sont correctement utilisées.

Car, en cas de litige, les DSI seront sans nul doute au coeur de la polémique, voire mis en accusation dans des procès judiciaires ou médiatiques.

De nouvelles obligations pour le DSI

En dépit de cette situation inconfortable, les DSI peuvent jouer un rôle actif dans l'anticipation des problèmes et réduire ainsi un tel risque. Ils sont de plus en position de suggérer une politique en matière de protection des données sensibles et être le fer de lance de sa mise en oeuvre.

De nouveaux devoirs les attendent : devenir des "champions" du respect de la vie privée, élaborer une déontologie et s'y tenir même face à leur direction, savoir jouer des solutions techniques à leur

Le Journal du Net **du 18 juin 2007**

disposition en rompant avec les habitudes du passé où l'on sécurisait le contenant et pas le contenu, garantir l'anonymat des données tout au long du cycle de vie des données personnelles au sein du système d'information...

Il reste que la protection des données personnelles ne concerne pas les seuls DSI, c'est aussi une question sociétale. Il va donc falloir agir sur d'autres leviers, que ce soit au niveau des Etats, des instances législatives ou de la société elle-même. Le grand public, bien qu'il en semble pour l'instant peu conscient, a de toute évidence un rôle important à jouer.

Hold-up sur les données personnelles

Qu'il s'agisse de faire du commerce, de réaliser des études statistiques ou encore de renforcer la sécurité nationale, les données personnelles sont devenues de véritables marchandises qui attirent la convoitise des entreprises et des administrations.

Aujourd'hui, la collecte se fait à grande échelle et le phénomène prend de l'ampleur, si bien que certains parlent même de pillage des données personnelles.

De son côté, le grand public - parfois sans trop se poser de questions ou même sans s'en rendre compte - communique ou laisse dans son sillage en surfant sur Internet une multitude d'informations qui n'ont rien d'anodin : informations de type administratif, informations biométriques utilisées par exemple pour le contrôle d'accès ou les cartes d'identité électroniques, données comportementales, sans oublier les données de géolocalisation, ou encore les données relatives à la santé lorsqu'elles ne se limitent pas aux seules données comptables et administratives.

Menace sur notre vie privée

Il va sans dire que si l'on est capable de recouper toutes ces données, il devient possible de pénétrer très loin dans l'intimité des individus. En l'absence de pratiques de collecte et de traitement rigoureux, le risque est réel et conséquent.

Et force est de constater que les failles techniques, organisationnelles ou réglementaires, les comportements inconscients, les négligences, l'éparpillement des données, les pratiques contestables de management des données, la mauvaise interprétation des textes législatifs, la primauté de la raison d'état... offrent de multiples occasions de dérives.

Le caractère sensible de ces données, l'utilisation et l'interprétation que l'on peut en faire via des recoupements ou des traitements croisés, constituent pour chacun d'entre nous autant de sources d'inquiétude, auxquelles s'ajoutent de nombreuses questions restant sans réponse : où sont stockées mes données personnelles ? Qui y a accès ? Comment sont-elles sauvegardées et archivées ? Sont-elles détruites une fois devenues obsolètes ?...

Quand la société se réveillera...

Le traitement massif des données personnelles porte aujourd'hui essentiellement sur les données à caractère administratif ; le traitement des données biométriques reste pour l'heure encore assez confidentiel. Mais les choses évoluent vite et la biométrie arrive à grand pas dans la vie de tous les jours.

Alors que les utilisateurs communiquent assez facilement des données de type administratif, ils se montrent beaucoup plus réticents lorsqu'il s'agit de données biométriques.

A la suite de premières expérimentations de déploiement de la biométrie ou de puces RFID dans des contextes grand public, on a pu voir apparaître des signes de rejet et même de rébellion chez les utilisateurs. Certains allant

Le Journal du Net
du 18 juin 2007

même jusqu'à se livrer à des actions commandos "à la José Bové", à l'exemple des élèves du lycée de Gif-sur-Yvette en 2005.

Si jusqu'à présent le développement des TIC n'a donné lieu qu'à un nombre relativement faible de controverses et de conflits, il faut rester vigilant et se méfier des problèmes dormants, véritables volcans qui peuvent se réveiller à tout instant.

Le retournement de situation autour des machines à voter est symptomatique de cet état de fait. Après des mois et des années de désintérêt pour le sujet, certains semblent réussir depuis l'élection présidentielle à réveiller l'intérêt, d'une partie au moins, du grand public.

Chantal Frasez