PAR JEAN-MARC GOETZ

consultant senior chez Parker & Williborg

L'entreprise **doit** protéger les données **personnelles**

L'actualité présente de plus en plus de cas de sociétés confrontées à des pertes de données, ou à des transferts d'informations personnelles mal contrôlés ; des réseaux sociaux invitent leurs abonnés à fournir des données qu'ils ne maîtriseront plus. Face à cette situation, quelle est la bonne attitude ? Des dispositifs de suivi et de marquage des données apportent une première réponse.

Nous sommes à tout moment amenés à fournir des données personnelles, parfois confidentielles, que ce soit volontairement ou non. Or, l'actualité présente de plus en plus de cas de sociétés confrontées à des pertes de données, ou encore à des transferts d'informations personnelles mal contrôlés ; par ailleurs, des réseaux sociaux invitent leurs abonnés à fournir des données sans nécessairement leur donner les moyens de les retirer ou, au minimum, de les suivre. Face à cette situation, quelle est la bonne réponse individuelle et collective ? Faut-il adopter la position du « laisser faire » pour la plus grande satisfaction d'un *Big Brother* ? Faut-il être suspicieux à la limite de la paranoïa et ne rien fournir ? Dans cette chaîne de responsabilités, qui doit faire quoi, quelles sont les responsabilités respectives de l'individu et de l'entreprise ?

L'Union européenne applique une politique de protection des données des plus rigoureuses

REPÈRES

La réglementation protégeant les données personnelles se met en place et se renforce dans de nombreux pays. Les autorités de contrôle et notamment la CNIL (Commission nationale Informatique et Libertés) en France se montrent de plus en plus actives et les particuliers font davantage valoir leurs droits. Dans ce paysage, l'entreprise joue un rôle essentiel.

Un arsenal complexe

La Directive européenne 95/46/CE constitue le cadre juridique de la protection des données personnelles et limite fortement l'accès à ces données en dehors du périmètre de l'Union européenne, en interdisant les transferts de ces données hors de l'Union. Les évolutions pressenties de ce texte visent à encadrer plus strictement le traitement de données personnelles : obligation de désignation d'un correspondant Informatique et Libertés, alourdissement des sanctions, etc.

Une situation contrastée

Le paysage international est pour le moins contrasté. L'Union européenne applique une politique de protection des données considérée comme une des plus rigoureuses, or les entreprises, notamment les multinationales, vivent constamment des situations incompatibles avec ces obligations réglementaires : comment accéder, à partir des États-Unis, à un annuaire électronique de personnes d'un groupe d'origine allemande dans le respect de ces obligations ? Aussi existe-t-il un système dérogatoire admis par les autorités de contrôle si un arsenal juridique *ad hoc* est instauré au sein de l'entreprise : les *Binding Corporate Rules* pour l'Union européenne, le *Safe Harbor* pour les États-Unis. La réglementation internationale évolue également avec des initiatives qui rapprochent différentes zones géographiques de la position européenne.

Cloud computing et dématérialisation

Si les données sont soumises à la réglementation en vigueur sur le lieu et le pays d'hébergement, le *cloud computing* vient brouiller les cartes en donnant peu ou pas d'indications sur la localisation de l'hébergement des données et, qui plus est, sur la nature de l'hébergement : s'agit-il d'un hébergement permanent ou provisoire ? Sommes-nous dans une situation où il n'existe qu'une seule source de production

Règles internationales

Les *Binding Corporate Rules* (BCR) constituent un code de conduite définissant la politique d'une entreprise en matière de transferts de données. Elles offrent une protection adéquate aux données transférées depuis l'Union européenne vers des pays tiers à l'Union européenne au sein d'une même entreprise ou d'un même groupe. Le *Safe Harbor* est un ensemble de principes de protection des données personnelles, négociés entre les autorités américaines et la Commission européenne en 2001. Les entreprises établies aux États-Unis adhèrent à ces principes auprès du Département du Commerce américain. Cette adhésion les autorise à recevoir des données en provenance de l'Union européenne.

de la donnée, avec un seul hébergement ? Quel est le statut des données de sauvegarde ? Mais le *cloud* non maîtrisé n'est pas une fatalité : les entreprises peuvent continuer à internaliser leurs ressources d'hébergement de données sensibles, quitte à mettre en place un environnement de *cloud computing* privé.

L'entreprise, acteur clé

Nous sommes encore loin d'un accord mondial pour la gestion et la circulation des données personnelles ; d'autre part, l'individu ne peut pas éternellement faire de la résistance quant à la fourniture de ses données. L'entreprise a donc un rôle majeur à jouer car ses activités impliquent le traitement de données personnelles de collaborateurs, de clients, de fournisseurs et autres tiers. Son rôle se révèle déterminant pour différentes raisons. Elle collecte et gère des données personnelles, elle peut être à même de transférer ces données au-delà des frontières ; elle doit donc présenter toutes les garanties de conformité à la réglementation du pays. Elle doit aussi maîtriser la chaîne de traitement des données personnelles : s'assurer de la finalité des données, garantir l'usage prévu sans détournement, gérer la sécurité des données personnelles avec les règles de confidentialité appropriées, ainsi que leur durée de conservation. Enfin, elle doit assurer la meilleure transparence en informant les personnes, en leur proposant des droits d'accès, de modification, voire d'opposition sur les informations personnelles communiquées.

Opacité

Si l'entreprise garde la maîtrise de ses données, en revanche l'individu a de moins en moins le choix : une situation de recherche d'emploi l'invite à fournir sans réserve des données privées ; les e-services et téléprocédures viennent l'encourager à formuler ses demandes bien fournies en données personnelles *via* Internet parfois sans indication sur la localisation ni le sort de ces informations.

Impact large

Un programme de protection des données personnelles a un impact sur un large ensemble de processus de l'entreprise : les ressources humaines, le juridique, mais aussi les achats, la sûreté, les systèmes d'informations, etc. Son application peut prendre diverses formes. D'abord, assurer des formations, des actions de sensibilisation auprès des collaborateurs amenés à traiter régulièrement des données personnelles. Ensuite, définir des clauses et des mentions types concernant la protection des données personnelles à intégrer dans les contrats. Enfin, définir un cadre méthodologique pour la conception des processus et applications d'entreprise, avec l'application de règles pour le respect de la vie privée dès la phase de conception des processus et applications d'entreprise.

Is Big Brother still watching you [1] ?

Certes, ce type de programme, mis en place par de plus en plus d'entreprises, permet de donner une réponse aux enjeux réglementaires de la protection des données personnelles, mais il constitue aussi une opportunité intéressante pour l'analyse du système d'information existant et de ses données. Il offre également un cadre méthodologique de gestion de la traçabilité, en permettant de répondre au mieux aux questions posées sur le stockage et l'historique des données personnelles. Il permet enfin une politique de communication interne et externe axée sur la transparence et la confiance.

Ainsi, avec ce type de programme, l'entreprise assure pleinement son rôle dans cette chaîne de responsabilités, dans un contexte où les autorités de contrôle montent en puissance et où les réglementations se durcissent.

Si *Big Brother* nous regarde, peut-être commencera-t-il cependant à craindre ces dispositifs de suivi et de marquage des données qui apportent une meilleure traçabilité. ■

L'individu ne peut pas éternellement refuser de fournir ses données

1. « *Big Brother* vous regarde-t-il toujours ? »