Bases de données

COMMENT LES UTILISER ?

L'entreprise ne peut pas utiliser comme bon lui semble les données personnelles trouvées sur le Net ou ses bases de données clients. Malgré l'évolution des technologies, la protection des données à caractère personnel s'impose.

Par Claudia Weber, avocat fondatrice, et Eloïse Urbain, avocat, ITLAW Avocats

Peut-on envoyer des offres de services aux prospects dont on trouve les coordonnées sur les réseaux sociaux ou dans des annuaires ?

Non, pour utiliser des données collectées *via* des supports tels que les réseaux sociaux ou des annuaires, il faut avoir, au préalable, obtenu l'accord de la personne concernée et aussi l'avoir informée de son droit d'opposition. Cet accord peut être obtenu si, lors de l'inscription de ses coordonnées sur le site du réseau social ou dans l'annuaire, la personne concernée a été informée que les données collectées pourraient faire l'objet d'un transfert à des tiers à des fins commerciales et qu'elle a expressément donné son accord pour une telle utilisation.

Peut-on vendre sa base de données clients ?

Non. Les cessions de fichier sont autorisées à condition que les personnes concernées aient été prévenues de cette éventualité et aient accepté le principe. Il convient donc aussi ici, au préalable, d'informer les personnes concernées de ces transferts de données à des tiers, de préciser les finalités de ces transferts (à des fins de statistiques, commerciales...) et surtout d'obtenir leur consentement. Il est alors primordial de toujours permettre à la personne concernée de pouvoir s'opposer à ce que ses données soient transférées à des tiers.

Peut-on héberger sa base de données clients auprès de n'importe quel prestataire dans le monde ou en *Cloud Computing* ?

Oui, si on respecte certaines conditions. La loi Informatique et Libertés de 1978 (modifiée par la loi de 2004 transposant la directive du 24 octobre 1995) a, en effet, précisé les conditions de transfert de données à caractère personnel vers des pays n'assurant pas un niveau de protection adéquat au sens de la directive, c'est-à-dire à peu près l'ensemble des pays hors UE, y compris Monaco ! L'hébergement des données dans un pays dit « tiers », par une société à laquelle la loi française s'applique, doit donc être encadré par des clauses contractuelles types, ou selon les principes du *Safe Harbor* (pour un hébergement situé aux USA), ou sur la base de BCR (*Binding Corporate Rules*), ou selon une des exceptions de l'article 69 de la loi Informatique et Libertés (sauvegarde de l'intérêt public, consentement de la personne... cela demeurant des exceptions). Pour un hébergement sur des serveurs dans un pays tiers déterminé ou *via* le système du *Cloud Computing*, les transferts de données devront ainsi respecter ces modalités d'encadrement et être soumis à l'autorisation de la CNIL pour être conformes à la réglementation Informatique et Libertés française et européenne. Si le *Cloud Computing* pose tant de soucis quant à la protection des données personnelles, c'est parce qu'il implique que le responsable de traitement perd en partie la maîtrise de la localisation de ses données.

Notre conseil

À l'égard des personnes dont les données sont traitées : les informer, obtenir leur consentement, surtout si les informations proviennent de tiers, et leur accorder les droits d'accès, de rectification et d'opposition.

À l'égard des sous-traitants (gérant, administrant ou hébergeant les données) : intégrer aux contrats les mesures de transfert, de sécurité, de confidentialité, d'intégrité et les responsabilités de chacun au regard de la loi Informatique et Libertés.

À l'égard des salariés : les sensibiliser sur l'utilisation des outils informatiques et la protection des données personnelles *via* une Charte informatique ou une Politique de confidentialité.