Une main tendue pour la sécurité des systèmes d'information

Comme l'illustrent les récents scandales relatifs à la perte de données à caractère personnel par de grandes entreprises comme Sony, Apple ou encore Facebook, la protection des systèmes d'information peut revêtir une importance capitale en terme d'image. Mais c'est aussi et surtout sur le plan juridique que l'obligation de sécurisation prend toute son importance.

En effet, l'obligation de sécurisation est une obligation légale imposée par la loi dite Informatique et libertés[1] dès lors que le système d'information contient des données à caractère personnel.

Ces données sont définies comme étant « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne»[2].

L'article 34 de ladite loi met à la charge du responsable du traitement une obligation de sécurisation consistant à « prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »

Parfois même, cette obligation est réaffirmée dans les engagements contractuels des entreprises.

Enfin, la nécessité de protéger son système d'information découle du bon sens notamment au regard de la jurisprudence rendue en la matière. En effet, faisant application de l'adage « nul ne peut se prévaloir de sa propre turpitude », la Cour d'appel de Paris a notamment considéré que l'exploitant d'un site internet qui n'aurait pas suffisamment sécurisé l'accès à certaines données ne pouvait se prétendre victime d'une atteinte à un système de traitement automatisé de données et de ce fait obtenir réparation des dommages causés par l'intrusion[3].

Dès lors, il appartient aux entreprises de prendre les mesures appropriées pour se conformer à ces exigences.

Actuellement, la politique de sécurité des entreprises passe majoritairement par l'attribution d'un login auquel est associé un mot de passe.

Or, force est de constater que la fiabilité de ce système de sécurité est assez faible compte tenu notamment de la possibilité de transmission volontaire, voir involontaire, des ces codes à un tiers. Par ailleurs, il suffit parfois de quelques minutes et de peu de matériel pour « craquer » ces mots de passe, et ce malgré l'utilisation de nombreux caractères alphanumériques et spéciaux conformément aux recommandations de la Cnil[4].

---

[1] Loi n°78-17 du 6 janvier 1978 relative à l'Informatique, aux fichiers et aux libertés.
[2] Article 2 de la loi Informatique et libertés.
[3] CA Paris, 12ème ch., Sect. A, 30-10-2002, n°02/04867, Kitetoa c. Tati
[4] Voir notamment : fiche pratique de la Cnil, 10 conseils pour sécuriser votre système d'information, 12-10-2009.

D'autres solutions, pourtant simples et surtout plus efficaces, sont néanmoins envisageables et notamment grâce à la mise en place de procédés de reconnaissance biométriques.

La biométrie est définie comme l'ensemble des techniques informatiques permettant d'identifier un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales.

Certes, l'utilisation de la biométrie peut présenter certains inconvénients puisqu'elle induit certaines démarches auprès de la Commission nationale informatique et liberté (Cnil), et compte tenu du coût financier de l'installation.

En effet, en raison du caractère sensible des données biométriques, la loi informatique et libertés instaure un contrôle particulier de la Cnil sur ce type de traitement fondé essentiellement sur l'impératif de proportionnalité. De fait, c'est le régime de l'autorisation préalable qui est, par principe, applicable. La Cnil a cependant mis en place un régime simplifié pour certains dispositifs biométriques[5].

De plus, l'installation du dispositif représente un coût qui est, de fait, bien supérieur à une politique de sécurité fondée sur l'utilisation d'un simple mot de passe.

Cependant, un changement paraît inévitable au regard de l'évolution du droit qui tend vers une responsabilité accrue du responsable de la sécurité.

Le projet d'ordonnance relative aux communications électroniques qui fait actuellement l'objet d'une consultation publique lancée par le gouvernement, illustre parfaitement cette tendance.

L'article 38 du projet prévoit en effet d'ajouter un article 32 bis dans la loi Informatique et libertés rédigé comme suit :

« Art. 32 bis.- I.- Le présent article s'applique au traitement des données à caractère personnel mis en oeuvre dans le cadre de la fourniture au public de services de communications électroniques sur les réseaux de communications électroniques ouverts au public, y compris ceux prenant en charge les dispositifs de collecte de données et d'identification.
II. Pour l'application du présent article, on entend par violation de données à caractère personnel :
- toute violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération ou la divulgation de données à caractère personnel transmises, stockées ou traitées d'une autre manière en relation avec la fourniture au public de services de communications électroniques accessibles ;
- l'accès non autorisé à de telles données.
III - En cas de violation de données à caractère personnel, le fournisseur services de communications électroniques accessibles au public avertit, sans délai, la Commission nationale de l'informatique et des libertés.
Lorsque cette violation peut porter atteinte aux données à caractère ou la vie privée d'un abonné ou d'un particulier, le fournisseur avertit également, sans délai, l'intéressé.
La notification d'une violation des données à caractère personnel à l'abonné ou au

[5] Par exemple : Autorisation unique n° AU-19 – Délibération n°2009-316 du 7 mai 2009 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail.

particulier concerné n'est toutefois pas nécessaire si la Commission nationale de l'informatique et des libertés a validé les mesures de protection technologiques mises en oeuvre par le fournisseur pour remédier à la violation des données à caractère personnel et constaté que ces mesures ont été appliquées aux données concernées par ladite violation.
A défaut, la Commission nationale de l'informatique et des libertés peut, après avoir examiné la gravité de la violation, mettre en demeure le fournisseur d'informer également les intéressés. Si la mise en demeure n'est pas suivie d'effet dans le délai fixé par la Commission, celle-ci peut prononcer une sanction à l'encontre du fournisseur. »

Compte tenu des risques encourus par les entreprises si ce projet d'ordonnance venait à être adopté en l'état, la mise en œuvre de dispositifs biométriques doit être considérée comme étant la solution la plus à même d'assurer une sécurité optimum.

Il existe de nombreux dispositifs de sécurité faisant appel à la biométrie qui peuvent être classés en deux catégories :

- les dispositifs biométriques avec trace ;
- les dispositifs biométriques sans trace.

C'est cette dernière catégorie, dont font partie les dispositifs de reconnaissance du réseau veineux de la main, qui doit être privilégié puisqu'elle ne présente aucun risque de violation de l'intégrité de la personnelle de l'utilisateur.

Leur fonctionnement est assez simple. Il suffit d'enregistrer un gabarit, puis, pour chaque utilisation un capteur infrarouge analysera le réseau veineux et s'assurera que la personne dont la main est analysée est bien autorisée à pénétrer dans les locaux, le système ou encore à accéder au poste de travail.

Ce type de dispositif présente de nombreux avantages en terme de sécurité puisque le réseau veineux, propre à chaque individu, ne se modifie pas dans le temps et qu'il est impossible de l'imiter puisque celui-ci ne laisse aucune trace et est invisible à l'œil nu.