Présentation de M. Bruno RASLE, AFCDP

M. RASLE a fait une présentation sur l'éventuelle future « obligation de déclaration des atteintes aux données personnelles », liée notamment au texte proposé par les sénateurs Détraigne et Escoffier et voté au Sénat.

La réunion a commencé par un rappel du « statut » des Correspondants Informatique et Libertés (CIL) et, d'une façon plus générale, des conséquences de la loi Informatique et Libertés.

La fonction de CIL est apparue suite à un décret d'octobre 2005. Le CIL est une personne désignée par le responsable d'un traitement (au sens de la loi Informatique et Libertés), afin qu'il soit le garant de la conformité de l'entité à la loi Informatique et Libertés. On peut donc le voir comme une forme d'intermédiaire entre la CNIL et le responsable d'un traitement. Le CIL n'est pas un opérationnel : son rôle est d'informer, de diligenter des contrôles, mais pas de les réaliser. Par contre, il a des responsabilités significatives en cas de non-conformité, selon un mécanisme d'escalade relativement classique : information du responsable du traitement puis, si les non-conformités ne sont pas corrigées, information de la CNIL.

Le CIL n'est soumis qu'à l'autorité hiérarchique du responsable du traitement. Le bilan annuel qu'il doit rédiger n'a donc à être avalisé par personne. Il est remis directement par le CIL au responsable du traitement.

M. RASLE souligne qu'une action efficace d'un CIL ne peut s'envisager sans avoir réalisé au préalable un inventaire des traitements mis en place par l'entité.

L'un des composants du texte des sénateurs Détraigne-Escoffier concerne la mise en place obligatoire d'un CIL pour toute entité dans laquelle plus de 100 personnes peuvent accéder à des données personnelles. Ce seuil paraît quelque peu bizarre et flou, notamment dans la qualification de « pouvoir accéder à des données personnelles ».

Il existe plusieurs parallèles entre un RSSI et un CIL, tout particulièrement dans les difficultés qu'ils peuvent rencontrer :

- ils sont malheureusement peu sollicités en amont des projets, alors que le « privacy by design » devrait être un axe majeur de réflexion,
- ils devraient être proactifs plutôt que réactifs, mais ne sont souvent sollicités qu'après des incidents,
- ils constatent un manque parfois flagrant de sensibilisation, surtout lorsque l'on s'élève dans la hiérarchie, les VIPs ayant tendance à ignorer tout ce qui pourrait être vu comme une contrainte,
- ils rencontrent des difficultés significatives à faire appliquer les décisions concernant la sécurité et la bonne gestion des données personnelles,
- s'ils ont un droit de regard et de contrôle, ils ne sont pas des autorités d'investigation,

- le retour sur investissement, en matière de sécurité informatique ou de conformité, est difficile à définir,
- leurs actions sont souvent sous-valorisées voire dévalorisées.

Il faut souligner que, aux termes de l'article 34 de la loi Informatique et Libertés, le responsable des traitements est le garant des données personnelles ainsi traitées. Il doit prendre toutes les précautions nécessaires pour en assurer la sécurité « au regard des données et des risques », ce qui confirme la nécessité de l'inventaire des risques et de leur analyse.

Un commentaire de la CNIL souligne d'ailleurs que « ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts, un niveau de sécurité approprié au regard des risques ». A cet égard, la déclaration faite à la CNIL, ainsi que les annexes qui peuvent y être attachés, doivent contenir les moyens de sécurité mis en place. A l'inverse, l'accusé de réception de la CNIL n'est rien de plus qu'un accusé de réception et ne vaut pas acceptation des moyens de protection ou des traitements ainsi déclarés.

La réunion s'est poursuivie sur le projet de loi du 6 novembre 2009, voté au Sénat le 23 mars 2010, et concernant, dans son article 7, « l'obligation de notification des violations des données personnelles ».

Cet article 7 renforce l'article 34 de la loi Informatique et Libertés, et fait donc apparaître l'obligation de notification des violations des données personnelles. Dans une telle situation (violation constatée ou supposée), le responsable du traitement doit informer son CIL, lequel informe la CNIL. En l'absence de CIL, le responsable du traitement doit informer directement la CNIL. En parallèle, il doit aussi informer les propriétaires des données personnelles « touchées », c'est-à-dire les utilisateurs, clients, adhérents, etc. dont les données personnelles sont concernées par la violation.

L'article 7 n'introduit aucun degré de gravité ou de risque associé à la violation. Cela signifie que les incidents doivent être signalés dans toutes les situations, en-dehors de toute qualification sur les conséquences éventuelles (réelles ou supposées) de l'incident pour les propriétaires de données.

M. RASLE a ensuite fait une comparaison des différents textes qui ont pu être votés et appliqués dans d'autres pays. Les textes ont parfois une application globale (tous secteurs d'activité) ou au contraire très ciblée (un secteur d'activité particulier).

Il n'existe pas d'études formelles sur les impacts des différents textes nord-américains, mais les entreprises concernées reconnaissent que cela les a amenées :

- à faire de réels efforts de sécurisation de leur système d'informations,
- à désigner des CPO (Chief Privacy Officer),
- à gérer correctement et de manière active la purge des données de leur système d'informations.

Indirectement, elles reconnaissent que, disposant ainsi de moins d'informations « sensibles », elles sont aussi moins sujettes aux risques liés à l'intelligence économique.

A cet égard (conservation des données), M. RASLE souligne que la CNIL impose la définition des délais de conservation des données personnelles ainsi que leur purge lorsque ces délais sont dépassés. Il existe de fait différents niveaux et notions de « stockage ou archivage ». Les recommandations de la CNIL font état de trois niveaux différents :

1. l'archive courante, liée à l'exploitation : il s'agit des données « à chaud », qui peuvent être utilisées dans des processus directement liés à la production de l'entité ordonnatrice des traitements,
2. l'archive intermédiaire, qui correspond à la gestion des données liés aux processus annexes de l'entité (contentieux, facturation, comptabilité, etc.). Les données sont nécessaires, mais peut-être pas dans leur ensemble et pas pour les mêmes personnes.
3. Enfin, l'archive définitive, associée au respect de contraintes règlementaires de conservation de certaines informations sur une durée longue. Il s'agit là d'un véritable archivage, les données n'ayant pas vocation à être utilisées « immédiatement » mais devant pouvoir « être identifiées, extraites et restituées ».

En Allemagne, une loi similaire au projet Détraigne-Escoffier a été votée le 1er septembre 2009. Elle contient quelques éléments très significatifs pour les entreprises :

- si le non-respect de la loi a entrainé un avantage pour l'entreprise (distortion de la concurrence), il n'existe alors plus aucun plafond dans le montant des sanctions
- les entités ordonnatrices de traitements qui seraient défaillantes dans la protection de ces dernières ont l'obligation d'aider les propriétaires des informations à gérer les conséquences des violations de ces données
- les entités ordonnatrices de traitements ont l'obligation d'expliquer les mesures qu'elles ont prises afin que les incidents ne puissent plus se reproduire.

Que peut faire une entreprise française ? Même si la loi n'est pas encore passée devant le Parlement, il est évident que les réflexions sur une véritable gestion des données personnelles sont dans l'air du temps. Il faut donc se préparer de façon appropriée aux futures contraintes, qui ne manqueront pas d'apparaître.