Le rôle du CIL dans l'entreprise

Compte rendu de la rencontre avec Jean-Pierre Rémy, Correspondant Informatique et Libertés de la Banque de France

Dominique BERGEROT, membre du Comité d'ADELI

La conférence du 3 février 2010 était consacrée au rôle du CIL (Correspondant Informatique et Libertés) dans l'entreprise. Elle était animée par Jean Pierre Rémy, CIL de la Banque de France, également administrateur de l'AFCDP (Association Française des Correspondants à la Protection des Données à Caractère Personnel), qui nous a fait part de son expérience, en précisant qu'il s'exprimait en son nom et que ses propos n'engageaient pas la Banque de France.
Voici un nouveau métier au croisement des systèmes d'information et du juridique.

Présentation du conférencier

Jean-Pierre Rémy a déroulé son parcours professionnel qu'il déclare « atypique » à la Banque de France, en étant 3 ans directeur de projet informatique, 9 ans responsable de la gestion informatique et de la logistique de l'institut de formation qui forme 15000 stagiaires par an, puis responsable du service de l'informatique individuelle au sens large du terme (poste de travail, bureautique, intranet, messagerie..).
À partir de 1998, il a été secrétaire général d'une organisation syndicale pendant 3 ans. Ces expériences lui sont utiles dans sa fonction. Depuis 2006, il est Correspondant Informatique et Liberté (CIL) à la Banque de France. Il enseigne également à l'ISEP (Institut Supérieur d'Électronique de Paris) qui propose un master « management et protection des données personnelles».

CNIL et Loi Informatique et Libertés (LIL)

La CNIL a été créée en 1978 par la Loi Informatique et Libertés, votée suite au scandale du projet SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus), qui visait à interconnecter les fichiers nominatifs de l'administration française, notamment par le biais du numéro INSEE.
La loi relative à l'informatique aux fichiers et aux libertés du 6 janvier 1978 constitue le fondement de la protection des données à caractère personnel dans les traitements informatiques mis en œuvre sur le territoire français.

Elle a été réformée par la loi du 6 août 2004, qui transposait la directive européenne du 24 octobre 1995 sur la protection des données à caractère personnel (DIR. 95/46/CE).
La loi de 2004 allège de façon substantielle les obligations déclaratives des détenteurs de fichiers pour les organismes qui désignent un CIL, accroît les pouvoirs de la CNIL en ce qui concerne les investigations sur place et les sanctions, et renforce les droits des personnes. La fonction de Correspondant Informatique et Liberté a été créée par la loi de 2004.

Droit des personnes et obligations de l'entreprise

La LIL donne des droits au citoyen : le droit d'être informé, le droit d'opposition, le droit d'accéder à ses données sur simple demande (accès direct et indirect) et le droit de rectification de ses données. Tout citoyen peut s'adresser à la CNIL.
L'entreprise a des obligations d'information : elle doit déclarer la mise en œuvre d'un traitement informatique de données à caractère personnel et le décrire à la CNIL ou à son CIL. Elle doit par ailleurs respecter le droit à l'oubli, en purgeant les fichiers qui contiennent les données qui ne sont plus nécessaires aux traitements. Le transfert de données personnelles hors de l'Union européenne est encadré par la loi.

Déclarations CNIL des entreprises

Il existe trois types de déclaration : la déclaration normale, la déclaration dite simplifiée et la demande d'autorisation pour les traitements sensibles.

Exemple de pénalités et de sanctions pénales prévues par la Loi Informatique et Libertés

La CNIL a un pouvoir d'investigation et un pouvoir de sanction.
La loi prévoit un droit de contrôle sur pièces et sur place dans les entreprises, pour vérifier la conformité des traitements. Les sanctions peuvent être administratives (par exemple, interruption du traitement jusqu'à mise en œuvre des modifications imposées), financières, les amendes pouvant atteindre 300 000 € et pénales si la CNIL saisit le Procureur.

CNIL et adresse IP

La CNIL considère que l'adresse IP est une donnée à caractère personnel.
Je vous renvoie à l'article de Patrick Kineider qui présente la LIL (Loi Informatique et Libertés) dans la Lettre ADELI n° 79.

Retour d'expérience du conférencier

En 2000-2001, la question de l'ouverture de l'accès internet aux postes de travail s'est posée à la Banque de France. Le danger potentiel de l'utilisation d'Internet a alors conduit à encadrer l'usage des NTIC. En phase avec l'évolution de la jurisprudence, une utilisation raisonnable à des fins non professionnelles a été tolérée.
Des scénarios concernant la LIL sont élaborés autour du poste de travail et proportionnés aux risques pour les salariés D'autre part, l'application de la LIL et du droit du travail vis-à-vis des salariés ne doit pas tout interdire, il faut encadrer le dispositif et définir les obligations de chacun (salariés, entreprise) avec des processus réalistes, définir des chartes et former le personnel.
En 2003, la Banque de France désigne, suite au « rapport sur la cybersurveillance sur les lieux de travail » de la CNIL, un « délégué à la protection des données ».
Ce délégué constitue également un pôle de compétences Informatique et Libertés, qui a existé pendant 3 ans (jusqu'à la nomination du CIL pour apporter un soutien juridique aux chefs de projet informatique), avec de nombreux échanges avec la CNIL. Le rôle de ce qui deviendra le CIL (Correspondant Informatique et Libertés) dans l'entreprise a émergé de ces réflexions avant la définition de ce nouveau métier dans la loi en 2004.

Les traitements après la loi de 2004

Le répertoire des fichiers déclarés par une entreprise est appelé un Registre. A la Banque de France, ce registre est constitué d'une fiche descriptive pour chaque traitement, diffusée sur le site internet.
Les Délégués du Personnel disposent d'un droit d'alerte, lorsqu'ils constatent une atteinte au droit des personnes ou aux libertés individuelles.

Le Correspondant Informatique et Libertés

Rôle et responsabilités

Selon la loi Informatique et Libertés, le CIL est chargé « d'assurer, d'une manière indépendante, le respect des obligations prévues » dans la LIL. Le responsable des traitements (c'est le Directeur Général le plus souvent qui peut déléguer cette responsabilité) doit se conformer à la loi, tant en termes d'accomplissement des formalités préalables nécessaires à un traitement (déclaration CNIL) que de respect des droits des personnes.

Le Correspondant Informatique et Libertés dans les entreprises

Le CIL est une fonction de l'entreprise qui n'est pas obligatoire selon la loi de 2004. S'il existe, il doit être déclaré à la CNIL.
Désigner un correspondant permet à l'entreprise de bénéficier d'un allègement des formalités déclaratives mais surtout de s'assurer que l'informatique de l'organisation se développera sans danger pour les droits des usagers, des clients et des salariés. C'est aussi, pour les responsables de fichiers, le moyen de se garantir de nombreux risques résultant d'une mauvaise application du droit en vigueur.

Le CIL est à la fois celui qui communique dans l'entreprise et l'interlocuteur de la CNIL. La nomination d'un CIL dans une entreprise a pour autre avantage de réduire le délai de réponse de la CNIL.
Une proposition de loi de 2009 vise à rendre obligatoire la fonction du CIL dans les entreprises de plus de 50 personnes.
En 2009, un peu plus de 5 000 entreprises avaient désigné un Correspondant Informatique et Libertés.

Le CIL, salarié dans l'entreprise
Le CIL, comme tout salarié, peut être licencié et l'entreprise doit alors en faire la déclaration à la CNIL. En contrepartie, le CIL est révocable par la CNIL.
Le CIL peut dénoncer à la CNIL les non conformités vis-à-vis de la loi. Son pouvoir et sa responsabilité peuvent être étendus aux filiales de l'entreprise. Ceci explique que le CIL puisse être considéré comme un « danger » pour l'entreprise et le responsable de l'entreprise (PDG ou directeur général).

Le CIL, fonction indépendante dans l'entreprise
Le décret du 20 octobre 2005 précise le statut du CIL et son indépendance dans l'entreprise. Ce dernier, s'il est salarié, a un lien de subordination. A la Banque de France, le CIL est rattaché au gouverneur afin d'éviter les conflits d'intérêts qui pourraient se présenter dans une direction opérationnelle. Pour garantir l'indépendance du CIL, la gestion des traitements informatiques et le CIL doivent avoir deux responsables distincts dans l'entreprise. On peut remarquer que cette problématique d'indépendance a été rencontrée dans les années 80 pour le statut du responsable qualité de l'entreprise, mais sans l'aspect obligation légale[1]. Il n'existe pas à ce jour de certification du métier de CIL et, selon le conférencier, la création d'une profession réglementée serait une bonne chose.

Le CIL d'une entreprise peut-il être un avocat ? Peut-il être un sous-traitant ?
Le CIL peut, s'il le juge nécessaire informer la CNIL en cas de non-conformité à la loi. Un avocat répond aux critères d'indépendance mais ne peut, en principe, pas dénoncer son client. Le règlement intérieur national du Barreau a donc été modifié pour permettre aux avocats d'être CIL externe : en cas de manquements qu'il ne parvient pas à faire régulariser par l'entreprise, l'avocat doit se démettre de sa mission.

La fonction de CIL peut être sous-traitée par les entreprises qui doivent, dans ce cas, prévoir les clauses contractuelles vis-à-vis du sous-traitant.

Qualités du CIL dans l'entreprise
Le CIL de l'entreprise a un rôle de conseil plus que de dénonciateur et doit avoir un œil « neuf », il est un frein aux dérives sur les données personnelles (des clients ou des salariés) de l'entreprise. Il doit bien connaître la culture de l'entreprise, pour bien intégrer les fondements et les enjeux des projets de traitements.
Il doit également diffuser une culture « informatique et libertés » dans l'entreprise et donc communiquer.

LIL, CIL et l'État français

A l'heure actuelle, il n'y a pas de Correspondant Informatique et Libertés dans la Fonction Publique d'État (ministères). Par contre, des CIL sont déployés dans les Fonctions publiques territoriale et hospitalière. Il existe une association professionnelle dédiée.

Le responsable des traitements

Le responsable des traitements doit déclarer les finalités du traitement, les éventuelles interconnexions, l'origine des données traitées, la durée de conservation des données, les entités qui y ont accès, le ou les services chargés de mettre en œuvre le traitement, les dispositions prises pour la sécurité des données, le recours éventuel à un sous traitant, les transferts de données vers un pays tiers.
Il est responsable de la mise à jour des informations déclarées, de la sécurité des traitements, de la durée de conservation des données, de la finalité des traitements et des flux transfrontaliers.

Démarche de projet système d'information dans l'entreprise – délai de conservation des données
Le CIL intervient dès les phases amont des projets systèmes d'information pour éviter les erreurs futures en cours de projet.
L'équipe projet amont est constituée avec le CIL, le chef de projet et ses partenaires (DRH, juristes, RSSI,..) pour faire un état des lieux et faire des propositions.

[1] *Il s'agit toujours d'une exigence de la norme ISO 9001*

La durée de conservation des données est un sujet difficile qui nécessite souvent un arbitrage pour les projets.
Le CIL a une démarche de contrôle, en coordination avec le « Risk Manager », pour répondre aux questions suivantes : quelles sont les données sensibles pour l'entreprise ? Quel est leur délai de conservation ?
Parmi les recommandations émises par le CIL, figure le cryptage des données sensibles.

Loi Informatique et Libertés à l'étranger

CNIL européennes

Une directive européenne du 24 octobre 1995 harmonise, au sein des États membres, la protection assurée à toute personne quel que soit le lieu où sont opérés les traitements de ses données à caractère personnel. A ce jour, les 27 États membres ainsi que les pays de l'Espace Économique Européen (Islande, Liechtenstein, Norvège), disposent d'une loi « informatique et libertés » et d'une autorité de contrôle indépendante.
Ces autorités indépendantes conseillent la Commission européenne sur ses initiatives législatives et pour harmoniser leurs pratiques ou recommandations destinées aux concepteurs et aux utilisateurs des technologies de l'information. Ces « CNIL » européennes réunies au sein du « groupe de l'article 29 », par référence à l'article de la directive qui l'institue, se prononcent par des avis qui sont rendus publics. Alex Türk, Président de la CNIL en France, a été élu Président du G29 en février 2008.

Et hors Europe ?

Les « Binding Corporate Rules » - BCR (ou règles internes d'entreprise)
Ces règles sont relatives aux transferts de données à caractère personnel à l'étranger vers des pays non membres de l'Union Européenne (UE). Par principe, les transferts en dehors de l'UE sont interdits sauf si le pays ou l'entreprise destinataire assurent un niveau de protection adéquat aux données transférées.
Les entreprises européennes doivent donc définir des règles internes de transfert de données personnelles hors Europe (par exemple vers leurs filiales), en particulier vers des pays n'assurant pas de protection suffisante.

Les Autorités de Protection des Données hors Europe
Par exemple en Argentine et au Canada, les dossiers des entreprises sur la déclaration des données personnelles sont transmis à l'état. Pour les entreprises françaises, le transfert des données sensibles est un sujet important. En Inde, si la gestion du personnel est sous-traitée, le prestataire doit fournir à l'entreprise cliente la preuve qu'il est conforme à la loi sur la protection des données.

Conclusion

Jean-Pierre Rémy nous a présenté le nouveau métier de Correspondant Informatique et Libertés. À ce jour, non obligatoire dans les entreprises, cette fonction va sans doute le devenir (une proposition parlementaire a été faite dans ce sens et pourrait déboucher rapidement).
Le conférencier a précisé, en réponse aux questions posées, que la démarche du CIL est plus une démarche de contrôle pour laquelle il travaille avec le « Risk Manager », plutôt qu'avec le responsable qualité pour examiner le cycle des données de l'entreprise.

La protection des données personnelles, qui est une obligation légale, se trouve ainsi, de plus en plus, intégrée formellement à la gouvernance des systèmes d'information et à celle des entreprises.▲

dominique.bergerot@adeli.org

Références

Site de la CNIL : www.cnil.fr
Site de l'AFCDP : www.afcdp.net
L'AFCDP est une association créée en 2004 qui a pour objet de promouvoir et développer une réflexion quant au statut et aux missions des correspondants à la protection des données personnelles. Elle regroupe des correspondants informatique et libertés d'entreprise, des avocats, des universitaires.