

## Informatique et libertés

La Commission informatique et libertés (CNIL) a finalisé le processus d'intégration des systèmes "d'alerte professionnelle" dans les filiales françaises de sociétés américaines.

# La dénonciation anonyme de comportements "anti-éthiques" est désormais adaptée à la France

PAR SONIA HADJALI, AVOCATE, CABINET ALAIN BENSOUSSAN



La loi «Sarbanes Oxley» a fait couler beaucoup d'encre en France, quant à la manière dont on allait pouvoir introduire, dans les filiales françaises de sociétés américaines, le système de dénonciation anonyme de comportements « anti-éthiques », suite aux scandales financiers aux Etats-Unis. La France, au travers de la Commission nationale de l'informatique et des libertés, s'est énergiquement opposée à deux éléments figurant dans cette loi, en indiquant que le dispositif d'alerte ne peut avoir une vocation générale et concerner tous domaines et qu'il ne doit pas encourager les dénonciations anonymes, qui ouvriraient la porte aux débordements. La réflexion s'est orientée autour de la nécessité de restreindre le périmètre du domaine de l'alerte et de la volonté d'éloigner le spectre du « dérapage » vers la délation et la dénonciation calomnieuse. Ce qui est louable, car il s'agissait là d'éléments sensibles du dispositif américain. Dans cette voie, la Cnil a, tout d'abord, en mai 2005, affirmé sa position, en refusant d'autoriser l'introduction de deux projets d'alerte professionnelle non-restreints, indiquant qu'ils pouvaient conduire à « un système organisé de délation professionnelle ».

Elle a établi un document d'orientation définissant les conditions de conformité « d'une alerte idéale » à la française : le dispositif d'alerte professionnel « à la française » ne peut avoir qu'un caractère complémentaire, être facultatif et avoir un champ restreint. En septembre 2005, le juge, qui s'est également penché sur la question, n'a pas interdit ces dispositifs d'alerte, mais en a limité strictement les modalités. Fin 2005, la Cnil a finalisé le processus d'intégration de l'alerte professionnelle dans les entreprises françaises. Elle a adopté une délibération qui porte autorisation unique de traitement automatisé de données, à caractère personnel, mis en œuvre dans le cadre d'un dispositif d'alerte professionnelle et qui en facilite l'intégration, si l'on se conforme intégralement à la délibération. Le système d'alerte version française doit répondre à une obligation législative ou réglementaire de droit français visant déjà à établir une procédure de contrôle interne dans les domaines financier, comptable, bancaire et de lutte contre la corruption. La loi américaine Sarbanes Oxley entre dans le champ de cette délibération pour les domaines comptables et d'audit. On doit pouvoir identifier l'émetteur de l'alerte, son identité devant toutefois rester confidentielle ; les données recueillies sont restreintes au domaine concerné par le dispositif d'alerte ; les destinataires des données doivent être chargés de la gestion des alertes professionnelles ; il est possible de transférer les données hors de l'Union européenne sous conditions ; les données recueillies ne doivent pas être conservées plus de deux mois après la clôture des opérations de vérification, si l'alerte n'est pas suivie d'une procédure disciplinaire ou judiciaire. Des mesures de sécurité spécifiques doivent être mises en œuvre, la circulation des informations devant être limitée. L'entreprise doit informer préalablement les salariés sur l'utilisation et les objectifs du dispositif d'alerte, ensuite le salarié faisant l'objet d'une alerte professionnelle doit être informé après que l'entreprise a recueilli les éléments de preuve. Enfin, tout salarié identifié dans le dispositif d'alerte dispose des droits d'accès aux données le concernant, et aussi de rectification ou de suppression, si elles sont inexactes, incomplètes, équivoques ou périmées, sans qu'il soit possible d'obtenir l'identité de l'émetteur de l'alerte. En pratique, les entreprises vont adresser à la Cnil un engagement de conformité à la décision et recevoir un récépissé de leur déclaration par courrier. Les choses sont donc facilitées, mais encadrées. Attention, si le dispositif d'alerte sort du descriptif, l'entreprise devra adresser à la Cnil un dossier complet de déclaration classique, qui fera l'objet d'un examen par la Cnil. ●

### CARACTÈRE COMPLÉMENTAIRE

> D'autres voies existent : la voie hiérarchique, les représentants du personnel, les rapports des commissaires aux comptes.

### JUGEMENT DU TGI

> Tribunal de grande instance de Libourne, 15 septembre 2005, comité d'établissement BSN glasspack et syndicat BSN glasspack.

### 3<sup>e</sup> DÉLIBÉRATION CNIL

> Délibération n° 2005-305 du 8 décembre 2005 (AU n°004).

### EXEMPLE DU DOMAINE BANCAIRE

> La loi impose un certain nombre de contrôles internes.

### DEUX PREMIÈRES DÉLIBÉRATIONS CNIL

> Deux délibérations de la Cnil n° 2005-110 et 2005-111 du 26 mai 2005 sur des dispositifs envisagés par la Compagnie européenne d'accumulateurs et la société McDonald's France.

### DOCUMENT D'ORIENTATION

> Adopté le 10 novembre 2005.

### L'ENJEU

> Ne pas encourager la délation professionnelle et la dénonciation calomnieuse – Limiter les alertes à certains domaines.

### LA MISE EN ŒUVRE

> Déclarer obligatoirement le dispositif d'alerte professionnelle avant sa mise en œuvre – Respecter strictement le périmètre de délibération de la Cnil.

disciplinaire ou judiciaire. Des mesures de sécurité spécifiques doivent être mises en œuvre, la circulation des informations devant être limitée. L'entreprise doit informer préalablement les salariés sur l'utilisation et les objectifs du dispositif d'alerte, ensuite le salarié faisant l'objet d'une alerte professionnelle doit être informé après que l'entreprise a recueilli les éléments de preuve. Enfin, tout salarié identifié dans le dispositif d'alerte dispose des droits d'accès aux données le concernant, et aussi de rectification ou de suppression, si elles sont inexactes, incomplètes, équivoques ou périmées, sans qu'il soit possible d'obtenir l'identité de l'émetteur de l'alerte.

En pratique, les entreprises vont adresser à la Cnil un engagement de conformité à la décision et recevoir un récépissé de leur déclaration par courrier. Les choses sont donc facilitées, mais encadrées. Attention, si le dispositif d'alerte sort du descriptif, l'entreprise devra adresser à la Cnil un dossier complet de déclaration classique, qui fera l'objet d'un examen par la Cnil. ●

### PROCÉDURE "PUREMENT DÉCLARATIVE"

> La Cnil n'opère pas de contrôle avant de délivrer le récépissé.