

## L'annulation d'un dispositif d'alerte professionnelle pour non conformité

### La loi du 6 janvier 1978 non respectée

► En **octobre 2007**, le tribunal de grande instance de Nanterre a **annulé** un dispositif d'alerte professionnelle implémenté au sein d'un grand groupe en 2004 en faisant partiellement droit aux contestations de la fédération CGT de la métallurgie (1)

► Le tribunal a jugé que le dispositif d'alerte instauré n'était **pas conforme** aux dispositions des articles 6, 7, 32, 34 et 36 de la loi du 6 janvier 1978 et qu'il devait en conséquence être annulé.

► Il s'agissait de **permettre à toute personne** ayant connaissance d'un manquement sérieux aux principes décrits par le Code de bonne conduite du groupe en matière comptable, financière ou de lutte contre la corruption **de signaler** ce manquement aux personnes compétentes du groupe lorsqu'était mis en jeu « *l'intérêt vital du groupe ou l'intégrité physique ou moral d'une personne* ».

### Des données recueillies illégalement

► Le tribunal a considéré qu'en l'espèce, la **notion de manquement grave** lorsqu'est « *mis en jeu l'intérêt vital du groupe (...) ou l'intégrité physique ou moral d'une personne* » apparaissait **trop vaste**.

► Les juges ont également considéré que le code de bonne conduite du groupe ne prévoyait ni une **formation spéciale**, ni une **obligation renforcée de confidentialité** des personnes chargées de recueillir et de traiter des alertes professionnelles pour **préserver la sécurité** des données recueillies.

► En outre, selon les articles 6 et 32 de la loi Informatique et libertés, la personne qui fait l'objet d'une alerte doit être **informée** par le responsable du dispositif dès l'enregistrement de données la concernant afin de lui **permettre de s'opposer** au traitement de ces données, ce qui n'était pas prévu par le présent dispositif d'alerte.

► En conséquence, les **données recueillies** dans le cadre du dispositif d'alerte l'ont été **illégalement** et ont donc du être détruites.

### L'essentiel

Il résulte de l'article 7 de la loi Informatique et libertés que les dispositifs d'alerte ne peuvent être considérés comme légitimes que du fait de l'existence d'une obligation législative ou réglementaire imposant la mise en place de tels dispositifs ou du fait de l'intérêt légitime du responsable du traitement dès lors que celui-ci est établi et sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

(1) TGI Nanterre, 19/10/2007 RG n°06/06460, disponible sur notre site : <http://www.alain-bensoussan.com/pages/915/>

**Chloé Torres**  
[chloe-torres@alain-bensoussan.com](mailto:chloe-torres@alain-bensoussan.com)

# Impact sectoriel

## Inquiétude des entreprises françaises sur le transfert de données personnelles aux Etats-Unis

### La Cnil se penche sur la problématique de transferts de données

#### L'essentiel

▶ La Cnil se penche sur la problématique de transferts de données à caractère personnel **vers les Etats-Unis** depuis des sociétés françaises. Elle a été saisie par plusieurs sociétés françaises ou étrangères établies en France en raison des demandes nombreuses de communication de données à caractère personnel vers les Etats-Unis (1).

▶ Les **entreprises américaines** demandent à leurs **filiales** situées en France et en Europe de leur communiquer des données à caractère personnel portant sur leurs **salariés**, dans le cadre de procédures américaines.

▶ Cette demande de données répond généralement aux **règles de procédures américaines** qui exigent la collecte et la conservation de données avant tout procès ou dans le cadre des **enquêtes** menées par les autorités administratives américaines telles que la Security and Exchange Commission (**SEC**).

▶ Or, ces demandes de communication de données soulèvent des problèmes d'application des **règles françaises** en matière d'**entraide judiciaire internationale**. Elles contreviennent également aux dispositions de la **loi Informatique et libertés** en matière de transferts de données hors de l'Union européenne laquelle exige de garantir un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet.

▶ Face à l'augmentation du nombre de sociétés concernées qui contactent aujourd'hui la Cnil, celle-ci a tenu à attirer l'attention du gouvernement sur ce point.

▶ Ainsi, une **réflexion interministérielle** pourrait être engagée. Cette question fait également l'objet d'une analyse au sein du **groupe dit « de l'article 29 »** qui regroupe les différentes autorités nationales de protection des données à caractère personnel au sein de chaque Etat membre de l'Union européenne.

▶ Les travaux du G29 sont réalisés en concertation avec les institutions européennes et en particulier la Commission, afin d'engager des **négociations** entre l'**Europe** et les **Etats-Unis** sur cette problématique.

Quatre cas de figure se présentent en ce qui concerne les demandes de communication d'informations dans le cadre de procédures américaines :

1. « Litigation hold », « litigation freeze » ;
2. « Pre-trial discovery » ;
3. Injonctions d'autorités publiques américaines ;
4. Délit de « destruction d'information ».

Ces notions sont introduites notamment par la loi dite Sarbanes-Oxley de 2002, modifiant le US Code Titre 18, Chapitre 73 : Obstruction of Justice.

(1) En bref le 15/01/2008, sur le site de la Cnil, [www.cnil.fr](http://www.cnil.fr)

# Les FAQ juristendances

## Les transferts de données à caractère personnel vers des pays non membres de l'Union européenne sont-ils soumis à des formalités particulières ?

Références

► **Oui.** La loi Informatique et libertés a introduit des règles précises pour encadrer les transferts de données vers des pays n'appartenant pas à l'Union européenne et n'ayant pas un niveau suffisant de protection de la vie privée, des libertés et des droits fondamentaux (1).

Ainsi, les personnes bénéficiant d'une protection au regard du traitement de leurs données en France sont assurées de continuer à en bénéficier lorsque leurs données quittent le territoire français pour faire l'objet d'un traitement hors de l'Union européenne.

Les dispositions de la loi n'encadrent que les transferts de données à caractère personnel qui quittent le territoire français à destination de pays n'appartenant pas à l'Union européenne. Elles n'encadrent pas les transferts issus de pays tiers à destination du territoire français. Mais, ces dispositions s'appliquent si les données importées en France quittent de nouveau le territoire français à destination d'un pays n'appartenant pas à l'Union européenne..

(1) Art. 68 de la loi 78-17 du 06.01.1978 modifiée.

## Qu'est-ce que le contrat de transfert de données à caractère personnel ?

► Il s'agit de clauses contractuelles permettant à un responsable de traitement de transférer des données à caractère personnel vers un destinataire établi dans un pays n'accordant pas une protection adéquate (2).

(2) Art. 69 de la loi 78-17 du 06.01.1978 modifiée.

## Lorsqu'une entreprise responsable d'un traitement est établie dans un Etat de l'Union européenne et que le traitement est réalisé par une filiale située en France, la loi française s'applique-t-elle ?

► **Oui.** La loi française s'applique aux traitements dont le responsable est établi dans un Etat de l'Union européenne et que le traitement est réalisée par une filiale établie sur le territoire français (3).

(3) Art. 5 de la loi 78-17 du 06.01.1978 modifiée.

## Quand un traitement est réalisé dans un autre état membre de l'UE, et concerne des données collectées en France, la loi française s'applique-t-elle ?

► **Non.** Quand un traitement est réalisée dans un autre Etat de l'Union européenne et concerne des données à caractère personnel collectées en France, la seule loi applicable est la loi du pays à partir duquel les données sont collectées sauf si un des moyens utile au traitement (le serveur, par exemple) des données se trouve sur le territoire français.

Le responsable du traitement doit désigner en France un représentant auprès de la Cnil qui se substitue à lui dans l'accompagnement de ses obligations.

# Actualité

## Protection des données : l'Europe doit reprendre l'initiative !

► Les questions internationales imprègnent de plus en plus les dossiers que traite la Cnil : les groupes « externalisation des entreprises françaises hors Union européenne » et « Discovery », ont ainsi vocation à proposer des solutions aux entreprises.

► La Cnil inscrit dès lors ses actions en concertation étroite avec ses homologues européens, tant au niveau du groupe des « CNILs européennes » dit G29, que de « l'initiative de Londres ». L'occasion est ainsi donnée à l'Europe d'améliorer l'effectivité de la protection des données dans le monde (1).

### Sources

(1) Tribune du 20/02/2008, sur le site de la Cnil, [www.cnil.fr](http://www.cnil.fr)

## Fichier FICOBA : une nouvelle procédure de droit d'accès

► Le fichier FICOBA recense les ouvertures, modifications et clôtures de comptes bancaires. Malgré le droit d'accès direct, l'administration fiscale ne donnait pas suite aux demandes invoquant le respect du secret professionnel. Contre ce blocage, le fichier FICOBA est désormais soumis à un droit d'accès mixte : direct, auprès de l'administration fiscale, s'agissant des données d'identification ; indirect, par l'intermédiaire de la CNIL, s'agissant des informations relatives aux comptes bancaires (2).

(2) En bref 19/02/2008, sur le site de la Cnil, [www.cnil.fr](http://www.cnil.fr) par un arrêté du 13 décembre 2007 sur [www.legifrance.fr](http://www.legifrance.fr)

## La Cnil autorise un dispositif biométrique

► La Cnil a pour la première fois autorisé la mise en œuvre de dispositifs reposant sur la reconnaissance du réseau veineux du doigt et de la voix, après qu'elle se soit assurée par des expertises techniques, que cela ne présentaient pas de risques particuliers au regard de la protection des données (3).

(3) Communiqué du 28/12/2007, sur le site de la Cnil, [www.cnil.fr](http://www.cnil.fr)

## La Cnil simplifie la déclaration

► La CNIL a mis en ligne sur son site un module interactif qui permet de vérifier si un fichier doit être déclaré, et sous quelle forme (déclaration simplifiée, normale) (4).

(4) Module disponible sur, [www.cnil.fr](http://www.cnil.fr)

## Edition 2008 du guide Cnil pour les Collectivités locales

► La Cnil accompagne les élus locaux qui recourent de façon croissante à l'informatique (fichiers d'état civil, fiscalité, listes électorales, télé-services, vidéosurveillance, etc.) en leur donnant les clés pour bien utiliser ces outils (5).

(5) Guide disponible sur le site de la Cnil, [www.cnil.fr](http://www.cnil.fr)

Directeur de la publication : Bensoussan Alain Rédigée et animée par Isabelle Pottier Diffusée uniquement par voie électronique ISSN (en cours) Abonnement à : <a href="mailto:avocats@alain-bensoussan.com">avocats@alain-bensoussan.com</a>
---