

LUTTE CONTRE LES MALVERSATIONS LES SALARIÉS ONT AUSSI LE DROIT D'ÊTRE PROTÉGÉS !



Jean-Pierre
Verrons

Associé
DzR Conseil

La protection des informations personnelles n'est pas réservée aux seuls clients des banques.

La loi impose également la protection des données des salariés des entreprises bancaires et financières. Deux cas illustrent cette obligation : le droit d'alerte professionnelle et l'enregistrement des conversations téléphoniques.

Le règlement général de l'AMF – en ce qui concerne les sociétés de gestion de portefeuilles –, mais aussi la réglementation bancaire pour les banques et les entreprises d'investissement prévoient la faculté, pour tout dirigeant ou collaborateur, de faire part de ses interrogations sur d'éventuels dysfonctionnements, au responsable de la conformité de l'entité ou de la ligne de métier à laquelle il appartient.

Cette procédure s'apparente au "whistle blowing" mis en œuvre par la loi Sarbanes-Oxley pour les entreprises américaines et leurs filiales à l'étranger.

La Cnil a répertorié cette disposition sous le nom de "droit d'alerte professionnelle", défini comme "un système mis en place par un organisme public ou privé pour inciter ses employés à signaler des problèmes pouvant sérieusement affecter son activité ou engager gravement sa responsabilité".

Pour éviter que le droit d'alerte ne s'apparente à une incitation à la délation sur les lieux de travail, la Cnil a encadré ce dispositif pour qu'il soit pleinement compatible avec la loi informatique et liberté (décision d'autorisation unique du 8 décembre 2005).

Son champ d'application doit être limité à des faits présentant des risques sérieux pour l'entreprise dans les domaines comptable, d'audit financier et de lutte contre la corruption. Il s'agira de cas de dysfonctionnements comptables, de faux en écriture, de fraude fiscale, de financement du terrorisme ou de blanchiment... D'autres faits, d'une particulière gravité car étant susceptibles de mettre en jeu l'intérêt vital de l'entreprise ou l'intégrité physique ou morale de ses employés, peuvent être recueillis et enregistrés par le responsable en charge de la gestion des alertes, comme des cas de harcèlement moral, de délits d'initiés de conflits d'intérêt...

Une information complète sur ces dispositifs doit être diffusée à tout le personnel.

GARANTIR LA CONFIDENTIALITÉ DES ALERTES

La Cnil ne souhaite pas encourager l'anonymat des alertes, mais celles-ci doivent demeurer confidentielles, qu'elles soient identifiées ou non. Le salarié donneur d'alerte doit recevoir l'assurance que son identité ne sera pas communiquée à la personne mise en cause.

Les données se rapportant à l'alerte peuvent donner lieu à une enquête dont la durée ne peut excéder 2 mois. À l'issue de cette enquête, si une action disciplinaire ou judiciaire est entreprise, les données sont conservées tant que dure la procédure puis, archivées suivant les règles en vigueur dans l'établissement. En l'absence de procédure, elles sont détruites ou archivées.

L'organisme qui met en place ce dispositif doit le porter à la connaissance de son personnel et doit adresser à la Cnil un simple engagement de conformité à la décision du 8 décembre 2005.

L'ENREGISTREMENT DES CONVERSATIONS TÉLÉPHONIQUES PROFESSIONNELLES

Un autre exemple de mesure de contrôle réglementaire devant être encadrée par la loi informatique et liberté nous est fourni par l'enregistrement des conversations téléphoniques professionnelles de certains salariés des entreprises d'investissement.

Le Règlement général de l'AMF prévoit que les prestataires de services d'investissement enregistrent, dans des conditions conformes à la loi, les conversations des négociateurs financiers et, plus généralement, de tout collaborateur en relation commerciale avec un client, donneur d'ordres. Cette obligation est étendue aux sociétés de gestion de portefeuilles pour les ordres qu'elles passent dans le cadre de leur gestion. Il appartient au responsable de la conformité de désigner les personnes dont les postes téléphoniques sont enregistrés.

Cette procédure a pour but de faciliter la vérification de la régularité des transactions (l'AMF peut demander au prestataire d'écouter les enregistrements en cas de soupçon de délits d'initié, par exemple) ainsi que leur conformité aux instructions des donneurs d'ordres, en cas de litige.

La procédure doit prévoir les conditions dans lesquelles les conversations peuvent être écoutées, toujours en présence du responsable de la conformité, ou avec son accord, ainsi que l'accès aux enregistrements en cause par les personnes enregistrées.

La durée de conservation de ces enregistrements par

les établissements assujettis est comprise entre 6 mois et 5 ans.

En plus de ces obligations réglementaires, la Cnil a prévu des garanties au profit des salariés dont les conversations peuvent être écoutées sur leur lieu de travail. Ainsi les salariés doivent être informés, ainsi que les instances représentatives du personnel, préalablement à l'installation du dispositif d'enregistrement. Les salariés doivent disposer d'un moyen leur permettant de tenir des conversations téléphoniques d'ordre privé en dehors du champ du dispositif d'enregistrement, enfin l'enregistrement et l'écoute des conversations téléphoniques doivent faire l'objet d'une déclaration normale auprès de la Cnil. Cette déclaration n'est pas nécessaire si l'établissement dispose en son sein d'un correspondant informatique et libertés.

PROTÉGER L'INTÉGRITÉ DES MARCHÉS ET LES DONNÉES PERSONNELLES

La réglementation et les pratiques professionnelles du monde bancaire et financier, qui tendent à promouvoir la protection des transactions et l'intégrité des marchés, sont donc encadrées par la protection nécessaire des données personnelles. C'est au responsable de la conformité de s'assurer que les objectifs assignés aux organisations mises en place répondent bien à toutes les obligations légales et garantissent les droits des salariés. Il doit aussi vérifier que les dispositifs en cause ont bien été déclarés auprès de la Cnil. ■

«Le salarié donneur d'alerte doit recevoir l'assurance que son identité ne sera pas communiquée à la personne mise en cause.»

POUR EN SAVOIR PLUS

A LIRE

■ La Charte des droits fondamentaux de l'Union européenne, qui affirme que «Toute personne a droit à la protection des données à caractère personnel la concernant»

■ La protection des données personnelles

Cyril Pierre-Beausse, Gérard Lommel (Préfacier)

A TÉLÉCHARGER

■ Protection des données personnelles au sein de l'Union européenne
http://ec.europa.eu/justice_home/key_issues/data_protection/data_protection_0108_fr.pdf

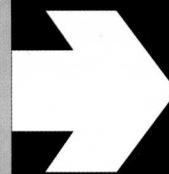
■ Les problématiques sur les réseaux sociaux

Opinion 5/2009 on online social networking, adopted on 12 June 2009
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf

SITES À CONSULTER

■ An open letter to Google's CEO, Eric Schmidt. (rédigée juin 2009)
<http://www.cloudprivacy.net/letter/>

■ Before the Federal Trade Commission Google, Inc. and Cloud Computing Services
<http://epic.org/privacy/cloudcomputing/google/ftco31709.pdf>



Voir aussi le prochain dossier de Banque & Stratégie n° 274 à paraître en octobre.