Sous le sceau du secret professionnel

Par Soraya Haquani le 14/04/2011

Pour les financiers, les contraintes sont fortes en matière de confidentialité. Enfreindre les règles peut conduire au délit d'initié.

Cet article est extrait de L'AGEFI HEBDO

A *chaque fois que je vais à la machine à café, je verrouille mon ordinateur* », confie un directeur financier. « *Lorsque je parle de mes clients ou de dossiers en cours dans un lieu public, j'utilise des périphrases* », dévoile un banquier. « *Le bon endroit pour parler d'un projet d'acquisition, c'est derrière des portes closes* », soutient pour sa part un spécialiste des fusions-acquisitions. Loin d'être anodins, les usages décrits par ces professionnels visent à respecter un principe cardinal dans le secteur de la finance : le secret professionnel, qui s'applique à tous les salariés. « *L'article L.511-33 alinéa 1er du Code monétaire et financier l'impose aux membres de conseils d'administration et de surveillance mais aussi aux employés de ces établissements* », précise **Emmanuel Daoud**, avocat au cabinet Vigo*.

Sanction pénale

Le non-respect du secret professionnel est sévèrement sanctionné puisque le Code pénal le punit d'un an d'emprisonnement et 15.000 euros d'amende. Dès leur arrivée dans l'entreprise, les salariés sont donc rapidement informés du devoir de discrétion auquel ils ne doivent jamais déroger, même après la fin de leur contrat de travail (dans lequel ce devoir est mentionné). Formations dédiées, documents rappelant la déontologie, guides des bonnes pratiques (notamment sur l'utilisation des systèmes informatiques)…, divers outils sont mis en place par les directions des ressources humaines et de la conformité (ou *compliance*) pour rappeler aux salariés leurs obligations en matière de confidentialité des informations. De la gestion d'actifs à la banque de détail en passant par la banque de financement et d'investissement (BFI), tous les métiers sont concernés. « *Les salariés d'Ossiam doivent respecter les règles de confidentialité inscrites dans notre code interne de déontologie et le règlement intérieur. Ces derniers sont signés par chaque nouveau collaborateur à son arrivée*, indique **Paul-Marc Lachaud**, responsable de la conformité et du contrôle interne d'Ossiam, filiale de **Natixis Global Asset Management** spécialisée dans les ETF (*exchange-traded funds*). *Ils reprennent les règles édictées par le Code monétaire et financier, le règlement général de l'Autorité des marchés financiers et les bonnes pratiques de la profession.* »

Sensibilisation et formations

Chez **Crédit Agricole** Corporate and Investment Bank (CA CIB) où le secret professionnel est aussi inscrit dans le règlement intérieur, la sensibilisation auprès des collaborateurs commence dès qu'ils rejoignent la banque. « *Les ressources humaines distribuent des 'kits' aux nouveaux arrivants qui comprennent entre autres choses un manuel de conformité*, explique **Paule Cellard**, responsable de la conformité chez CA CIB. *La banque met par ailleurs en œuvre des formations sur la bonne utilisation de nos systèmes d'information en général et des e-mails en particulier.* » En interne, les recommandations faites aux salariés sont souvent liées à leur messagerie électronique et aux outils de communication comme les *smartphones* (de véritables mini-ordinateurs en raison de leurs multiples fonctionnalités) ou les clés USB. « *Nous recommandons par exemple aux salariés de ne jamais fournir d'informations confidentielles dans un e-mail et de privilégier le téléphone le cas échéant*, illustre **Paule Cellard**. *Le courrier électronique est en effet un puissant outil de traçabilité qui pourrait, dans des circonstances particulières, être utilisé contre la banque ou le salarié.* » Au cabinet d'avocats d'affaires **Clifford Chance**, le recours à une clé USB doit faire l'objet d'une requête spéciale : « *Nous évitons d'utiliser des clés USB, sauf circonstances exceptionnelles et, dans ce cas, nous faisons une demande spécifique auprès de notre équipe informatique* », déclare **Sandrine Colletier**, avocate et *compliance officer* du bureau de **Clifford Chance** à Paris.

C'est surtout à l'extérieur que des risques peuvent peser sur la protection d'informations confidentielles et sensibles. Souvent amenés à se déplacer dans le cadre de leurs missions et leurs rendez-vous professionnels, les financiers se situent dans des environnements (taxis, trains, avions, aéroports…) où ils doivent en permanence prendre garde à ne rien laisser filtrer de leurs conversations téléphoniques ou de visu avec leurs interlocuteurs. « *Lorsque l'on se trouve en dehors de son bureau, il faut toujours se poser la question : si je parle de tel dossier ou de tel client, y a-t-il un risque dans mon environnement immédiat ?* », prévient **Sandrine Colletier**.

Les salariés doivent parfois suivre des consignes assez précises, comme en témoigne **Marie-Antoinette Tanguy**, directrice des ressources humaines du **Crédit Mutuel Arkéa** : « *Dans les lieux publics, nous sommes invités à ne jamais citer ni le nom de notre entreprise, ni les noms de nos collaborateurs.* » Dans le secteur de l'audit où les contraintes de confidentialités sont aussi très fortes, le quotidien des professionnels est régi par une série de règles. « *Notre profession est très réglementée*, rappelle **Jean-Luc Barlet**, associé chez **Mazars** et *chief compliance officer*. *Notre obligation de secret professionnel est directement organisée par le législateur (la loi de Sécurité financière est d'ailleurs venue la renforcer) et elle est de niveau absolu. Elle s'applique même à la fin des missions à nos associés et nos collaborateurs. Seule l'autorité judiciaire peut la lever.* » Associé au sein du département *consulting & risk services* de **Deloitte** où il exerce depuis treize ans, **Rédouane Bellefqih** affirme ainsi que « *la confidentialité fait partie intégrante de la culture d'entreprise* ». « *Nos équipes veillent à ne pas transporter des documents papier sensibles lorsqu'elles sont en déplacement, mais également à ne pas évoquer de sujets confidentiels dans des endroits publics* », poursuit ce consultant qui a l'habitude de travailler avec des ordinateurs à disques cryptés et des connexions à distance sécurisées.

Les « initiés »

Pour certains cadres de la finance qui ont accès à une information dite « privilégiée » (sur une entreprise cotée par exemple), le risque lié à la violation du secret professionnel est le délit d'initié. Une fois identifiés, les salariés exposés à ce risque sont soumis à un régime particulier. « *Un encadrement procédural précis édicté par le département de la conformité s'applique*, confirme **Paule Cellard**. *Ils n'ont accès qu'aux informations utiles sur la base du 'need to know' ; leur noms peuvent être inscrits sur des listes d'initiés, le cas échéant. Les opérations dans lesquelles ils sont impliqués peuvent également être inscrites sur la liste globale de surveillance qui fait l'objet d'un suivi rapproché. Tout manquement aux règles de confidentialité pourrait donner lieu à des sanctions.* » Chez **Mazars** aussi, « *c'est une problématique gérée de façon très stricte*, souligne **Jean-Luc Barlet**. *Lorsqu'il s'agit par exemple d'une opération de fusion-acquisition, nous inscrivons les collaborateurs ayant accès à une information privilégiée sur les listes d'initiés, conservées cinq ans, comme le demande l'Autorité des marchés financiers.* » Destiné à protéger l'entreprise, le secret professionnel peut parfois se retourner contre elle. Ainsi, un salarié suspecté de diffuser des informations confidentielles par e-mail pourra l'invoquer afin d'empêcher son employeur d'accéder à sa messagerie électronique. Mais dans un contexte où le contrôle interne s'est nettement renforcé dans le secteur de la finance, les établissements n'hésitent plus, en cas d'indices probants, à employer les grands moyens, selon Philippe Bouchez El Ghozi, avocat associé chez **Paul Hastings** : « *Parmi mes clients du secteur financier, je constate que de plus en plus d'entreprises me demandent de saisir un juge pour des 'mesures de constat' avec la présence d'un huissier. Cette procédure, qui peut être mise en œuvre dans des délais très rapides (en quelques heures), permet, lorsque l'on a des suspicions sur un salarié par exemple, d'accéder notamment à tous ses e-mails.* » « *J'interviens pour de telles mesures en moyenne une fois par mois* », précise cet avocat. Si les dispositifs internes, technologiques et réglementaires sont multiples, le « risque zéro » n'existe pas pour assurer la confidentialité des informations…