SYSTÈMES D'ALERTE ÉTHIQUE
Les difficultés de mise en œuvre

Laurent Viegnes

Associé

Michaël Bourdin

Associé

Neledhia

Le droit ou devoir d'alerte en entreprise concerne tous les salariés. La mise en œuvre d'un dispositif ad hoc doit cependant respecter les droits et obligations non seulement de l'alertant, mais aussi des personnels mis en cause. Cet article présente les meilleures pratiques concernant le déploiement de tels systèmes, soulignant également les réticences qu'ils ne manqueront pas de susciter.*

Une directive européenne, attendue pour cette année 2006, devrait constituer le texte de référence pour la mise en œuvre des procédures d'alerte éthiques ou professionnelles, en définissant – entre autres – le degré de protection dont bénéficieront les alertants ne disposant pas d'un autre statut que celui de salarié. Nous rappellerons les difficultés organisationnelles et techniques de conception et de déploiement des systèmes d'informations dédiés aux alertes éthiques et présenterons les meilleures pratiques qui semblent se dégager, tout en soulignant les nombreuses réticences ou aversions que ce développement majeur et inéluctable ne manquera pas de susciter.

LES CONSÉQUENCES PRATIQUES DES SYSTÈMES D'ALERTE ÉTHIQUE

Les alertes éthiques et professionnelles appliquées au milieu bancaire viennent renforcer un cadre réglementaire déjà très riche, notamment en termes de contrôle interne et de lutte contre le blanchiment. Des réglementations denses sur la mise en place de structures de contrôles internes indépendantes au sein des établissements bancaires sont à l'œuvre depuis bientôt une décennie (CRBF 97-02) et sont appliquées et enrichies lors des missions d'inspection menées par la Commission bancaire. Ces textes fixent les principes d'organisation des fonctions de contrôle au sein des établissements en déterminant comme principe de base, une indépendance totale des fonctions de contrôle des sphères opérationnelles. Cette étanchéité est délicate à mettre en œuvre lorsque les plus hautes instances de l'établissement arbitrent revenus (réels et récurrents) et risques (potentiels ou contingents).

Le législateur a complété ces systèmes de contrôle interne (par nature distants des organes de production) par la capacité accordée aux salariés et acteurs de l'entreprise à signaler des irrégularités réglementaires, légales, procédurales ou d'usage. Une première étape repose sur l'obligation de mise en place de procédures et de systèmes de lutte contre le blanchiment. Ils imposent aux salariés de signaler en interne ou, à défaut de réponse appropriée, auprès du procureur de la République, les faits ou soupçons de blanchiment dont ils auraient connaissance dans le cadre de leur activité professionnelle. Les alertes éthiques et professionnelles vont un peu plus loin en étendant le champ opérationnel sur lequel peut porter une alerte (tout élément susceptible de porter atteinte à l'établissement), en limitant cependant cette possibilité aux acteurs internes à l'établissement.

La multiplication des textes référents pose le problème de la capacité effective de traitement des alertes devant être mises en œuvre. Cette capacité

* Voir aussi l'article "Procédure d'alerte : un cadre législatif, évolutif et convergent", Revue Banque, n° 679, avril 2006.

1. PRÉCONISATIONS DE LA CNIL

Les dispositifs d'alerte

■ **Le dispositif d'alerte doit être complémentaire et limité dans son champ :** ainsi, la CNIL rappelle qu'il existe dans l'entreprise d'autres canaux (commissaires aux comptes, représentants du personnel) et que le dispositif d'alerte ne saurait se substituer à ces autres canaux, mais qu'il doit venir en complément. La CNIL considère que les dispositifs d'alerte ne sont légitimes que s'ils sont mis en place *"du fait d'une obligation légale (législative ou réglementaire)"* ou *"du fait d'un intérêt légitime du responsable du traitement et sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée"*. Elle classe ainsi dans la première catégorie les dispositions relatives au contrôle interne des établissements de crédit et des entreprises d'investissement prévu par arrêté du 31 mars 2005 modifiant le règlement du CRBF 97-02 du 21 février 1997. De plus, la CNIL précise dans sa décision d'autorisation unique les catégories de données qui peuvent être recueillies dans le cadre de l'alerte. Sur ce point, elle précise notamment que les faits recueillis sont strictement limités aux domaines concernés par le dispositif d'alerte et que les données collectées doivent être formulées de manière objective.

■ **Il ne doit pas avoir un caractère obligatoire**, la CNIL se basant notamment en l'espèce sur une lettre reçue du ministère du Travail et de l'Emploi dans laquelle celui-ci indique que *"l'obligation de dénonciation serait contraire à l'article L. 120-2 du Code du travail"*.

■ **Le dispositif d'alerte doit viser une catégorie de personnes précisément définie par le dispositif.**

■ **Il doit privilégier la "confidentialité" par rapport à l'anonymat pour celui qui procède à un signalement ou une alerte.** Le recours à l'anonymat n'est toutefois pas exclu par la CNIL mais celle-ci fixe alors des conditions restrictives.

■ **Le dispositif d'alerte doit faire l'objet d'une information claire et complète dans l'entreprise.** La CNIL précise dans sa décision d'autorisation unique le contenu de cette communication et indique notamment sur ce point, qu'il doit être clairement indiqué que l'utilisation abusive du dispositif peut exposer son auteur à des sanctions disciplinaires ainsi qu'à des poursuites judiciaires et qu'à l'inverse, l'utilisation de bonne foi du dispositif, même si les faits se révèlent, par la suite, inexacts ou ne donnent lieu à aucune suite, ne peut exposer son auteur à des sanctions.

■ **Il doit reposer sur une organisation présentant en elle-même des garanties :** recueil des alertes selon des moyens dédiés, recueils de données pertinentes, adéquates et non excessives, dispositif géré par un nombre limité de spécialistes dans un cadre confidentiel contractuellement défini, accès aux données sécurisé, une conservation limitée des données à caractère personnel (2 mois pour les alertes fondées sauf en cas d'engagement d'une procédure disciplinaire ou judiciaire, obligation de détruire sans délai les données recueillies en cas d'alerte infondée), l'information de la personne mise en cause par l'alerte dès l'enregistrement des données de façon à garantir son droit d'accès et de rectification.

« La multiplication des textes référents pose le problème de la capacité effective de traitement des alertes devant être mises en œuvre. »

repose avant tout sur des procédures (pour lesquelles la CNIL donne un certain nombre d'indications, voir *encadré 1*) à formaliser et un système de traitement adapté qui reste à concevoir.

LE SYSTÈME D'INFORMATION À L'ŒUVRE

■ **Le périmètre d'un système d'information d'alerte professionnelle** Ce système permet à un organisme privé (ici un établissement bancaire national ou international) d'inciter ses employés à signaler tout problème susceptible d'affecter son activité, sa responsabilité ou sa réputation. Le périmètre couvert doit donc inclure l'ensemble des succursales et filiales, l'outil doit être accessible à leurs employés. Les clients disposent de contacts et canaux commerciaux qui leur sont dédiés et ne doivent donc pas pouvoir accéder au système de saisie d'alerte. Les stagiaires et prestataires (toute personne employée, quel que soit son statut d'emploi) doivent avoir accès au système d'alerte (cf. la décision d'autorisation unique de la CNIL du 8 décembre 2005). Il appartient cependant à l'établissement de déterminer si les entités non consolidées sont incluses dans le

périmètre d'activité de ce système, notamment dans le cadre de joint-ventures ou d'entités recourant à des personnels détachés. De même, le système d'alerte doit être accessible (en saisie d'alerte) par tout employé dûment concerné, qu'il soit en déplacement ou hors des locaux professionnels. Dans ce cas la collecte des alertes peut s'opérer aux travers de canaux téléphoniques (une ligne d'alerte professionnelle), d'une adresse e-mail (pour délivrer un numéro d'alerte et une adresse sécurisée de dépôt de l'alerte elle-même) ou d'un extranet sécurisé.

Les composants d'un système d'information d'alerte professionnelle

Un tel système comporte plusieurs modules distincts (*encadré 2*) :

– un module d'information général sur la procédure d'alerte et les droits et responsabilités des alertants : accessible par l'intranet de l'entreprise pour tout employé disposant d'un poste de travail informatique et par l'extranet pour les autres (employés sur des postes partagés par exemple), il présente les textes réglementaires en vigueur, décrit la politique de l'entreprise et permet de télécharger la procédure d'alerte professionnelle ;

– le ou les modules (internes et externes) de signalement des alertes (ligne téléphonique enregistrée, protocole d'entretien confidentiel, courrier ou fax, pages intranet ou extranet, application dédiée de collecte des alertes...). L'alertant au travers de ce module disposer d'un identifiant unique pour son alerte, d'une preuve de dépôt de son alerte en retour (date, contenu de l'alerte, identification de l'interlocuteur ou du système de saisie), d'une déclaration de vérification et de prise en compte des informations transmises ainsi que le rappel écrit de la procédure en vigueur, notamment en termes de chronologie de traitement et de reprise de contact, en conformité avec l'article 32 de la loi Informatique et Libertés : identité du responsable, finalité du système et des traitements, destinataires des données et informations remises, droits des personnes, transfert des données et information hors de l'Union européen le cas échéant...) ;

– un module d'administration des alertes qui va permettre à l'instance de gestion (comité d'audit, section spécifique de l'inspection générale, département de la conformité et de la déontologie...) de statuer sur l'alerte (prise en compte ou rejet, investigation, décisions opérationnelles) et d'assurer la traçabilité des informations collectées dans le respect de la confidentialité et de la protection des donneurs d'alerte.

– un module de contact avec les donneurs d'alerte permettant de les informer confidentiellement du statut de leur alerte et de son traitement.

– un module de contact avec les personnes mises en cause de façon à garantir leur droit d'accès et de rectification dès l'enregistrement de l'alerte.

Un workflow complexe

Le nombre d'acteurs potentiellement impliqués dans le processus et l'indispensable équilibre entre les droits et obligations des différentes parties complexifient la gestion des flux d'information inhérents aux alertes professionnelles.

Une alerte est émise par un acteur interne à l'entreprise à destination d'une instance de gestion pluridisciplinaire. Cette instance de gestion doit intégrer les représentants des différentes sphères fonctionnelles, opérationnelles et exécutives de l'entreprise afin de détailler les composantes de l'alerte et d'en mesurer les multiples incidences (légales et réglementaires, financières, opérationnelles, réputationnelles, sociales). Sont également impliqués les acteurs visés par l'alerte ainsi que, le cas échéant, l'ensemble des intervenants mandatés par la société (inspection, spécialistes métiers, prestataires...) pour s'enquérir de la validité de l'alerte et éventuellement déterminer les mesures correctrices.

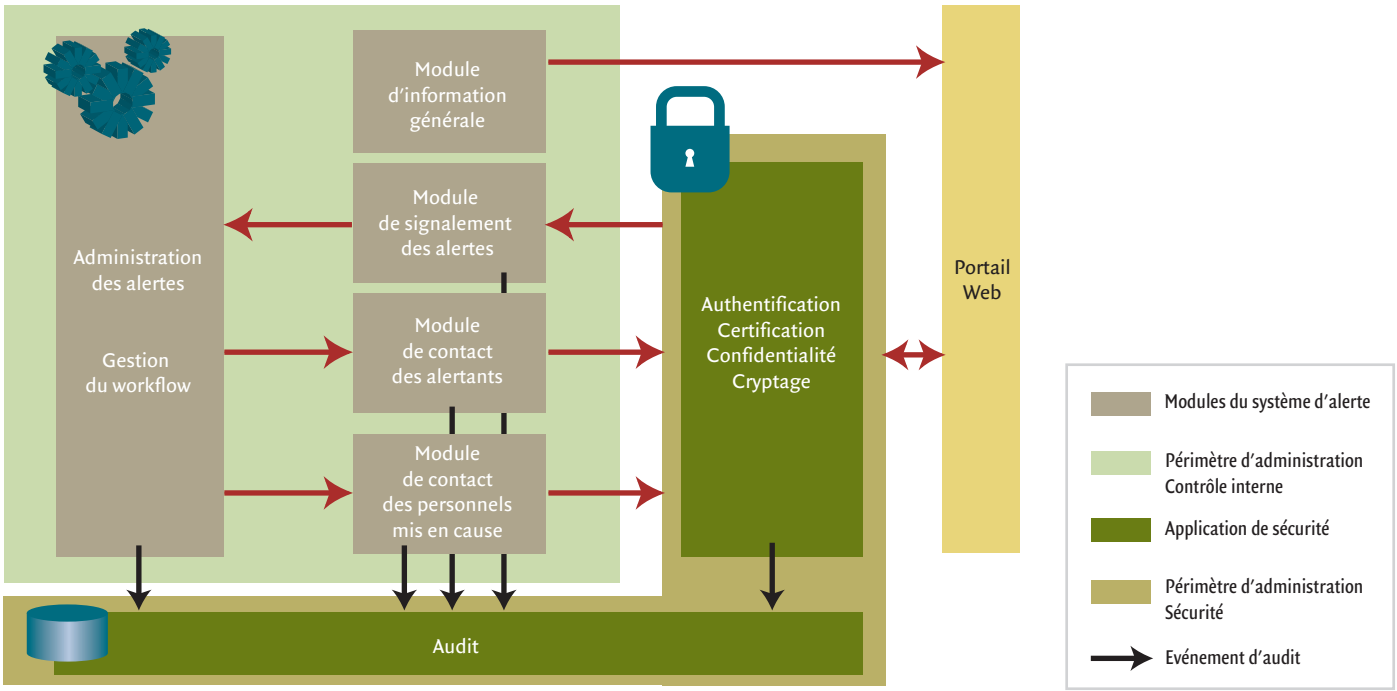
« Le nombre d'acteurs potentiellement impliqués dans le processus et l'indispensable équilibre entre les droits et obligations des différentes parties complexifient la gestion des flux d'information inhérents aux alertes professionnelles. »

ALERTES ÉTHIQUES

Quelques exemples

En 2002 un journal américain publia un dessin satirique où l'on voyait un recruteur interviewer un candidat à un emploi. Or ce dernier lui remettait un CV largement déchiqueté par un passage au broyeur et le premier commentait sans réelle surprise *"Je vois que vous avez dernièrement travaillé chez Arthur Andersen..."*. Ce dessin rappelle l'énorme scandale que constitua l'affaire Enron. Les répercussions aux États-Unis furent multiples : promulgation de la loi Sarbannes-Oxley, prise de conscience aiguë que certains risques juridiques et réputationnels peuvent être mortels pour les plus grands groupes mais surtout pour leurs salariés, mise en lumière de la procédure de *whistleblowing*. Le magazine Time nomma cette année-là comme *People of the Year* les cadres Cynthia Cooper de Worldcom et Sherron Watkins d'Enron qui révélèrent certains aspects de ces deux affaires ainsi que l'enquêtrice Coleen Rowley du FBI pour son alerte sur les lenteurs et inerties de son agence avant les attentats du 11 septembre 2001. En matière d'alertes éthiques, il y a désormais un avant et un après 2002 : les articles associent désormais les noms de Cooper et Watkins à celui, plus ancien, de Jeffrey Wigand (cadre du cigaretier B&W qui révéla à CBS les pratiques de manipulation de la nicotine et de ses effets menées par sa firme) et à celui, plus récent, de Paul van Buitenen (dont l'alerte sur la corruption de membres de la Commission européenne amena la démission de la Commission Santer).

2. UN EXEMPLE D'ORGANISATION



Le problème le plus aigu réside dans la gestion des différents statuts de la vie de l'alerte et des possibilités que ces statuts ouvrent aux différents acteurs en termes d'information et de respect de leurs droits. Comment concilier le juste respect de la confidentialité des alertants avec la possibilité pour les "mis en cause" d'exercer un droit d'accès et de rectification dès l'enregistrement de l'alerte ? Comment instaurer une procédure contradictoire dans le respect de cette confidentialité ? Enfin, et alors que chacune des parties en présence (alertant, mis en cause, instance de gestion des alertes, inspection...) ne dispose pas des mêmes droits ni des mêmes moyens d'investigation sur des éléments matériels probants (tant à charge qu'à décharge), l'existence d'une alerte signifiée trop rapidement aux "mis en cause" ne peut-elle conduire à la disparition prématurée de pistes d'audit et d'éléments probants ?

RÔLE CENTRAL DU GESTIONNAIRE DES ALERTES

La définition et la formalisation d'un *workflow* de gestion d'alerte sont cruciales pour garantir la double préservation des droits des acteurs impliqués et la confidentialité assurant la persistance des éléments probants. Les textes stipulent, en effet, que ces preuves doivent être collectées lors de l'examen relatif aux griefs énoncés et que leur absence dans l'alerte elle-même n'est pas opposable à l'alertant (ce dernier ne disposant que rarement de la faculté de collecter ces éléments et presque jamais du pouvoir d'investigation qui s'avérerait nécessaire).

Le rôle central occupé par le gestionnaire des alertes (personne ou instance) est également complexe. Si les alertants constatent une dérive (absence de prise en compte des informations remises, chronologie de traitement inadéquate, rejet mécanique des alertes, absence d'information sur les suites données, violation de la confidentialité des alertes et de l'identité des alertants), le mécanisme d'alertes professionnelles perd toute crédibilité interne et donc toute utilité propre.

Les travaux de conception de tels *workflows* et de positionnement des instances de suivi devraient dans un avenir proche remanier quelque peu la stratification des organes de contrôle interne mis en place lors de la parution de textes comme le CRBF 97-02. En faisant apparaître des besoins plus transversaux et la nécessité de véritables investigations contradictoires ils forcent les établissements bancaires à repenser le rôle, l'organisation et jusqu'aux procédures de leurs contrôles internes.■