LUTTE ANTI-CORRUPTION

19 L'alerte en entreprise

Daphné Latour
consultante en éthique des affaires et conformité

CONTEXTE

Alors que les sanctions pénales et administratives prononcées pour des faits de corruption n'ont internationalement jamais été aussi importantes, tant en fréquence qu'en montants infligés, la France a promulgué le 9 décembre 2016, notamment pour s'aligner sur les standards internationaux les plus rigoureux en la matière, la loi Sapin II, qui vise à renforcer la lutte contre ce fléau.

Parmi les outils utilisés dans la répression et donc pour la régression de ce phénomène, par définition sous-terrain et dissimulé, l'alerte en est un primordial. Cependant, contrairement aux États-Unis où le mécanisme du whistleblowing est depuis longtemps encouragé et même bien rémunéré, l'alerte n'a jusqu'ici, en France, jamais été très exploitée, ni mise en avant. Notamment, car elle est assimilée, à tort, à de la délation, historiquement taboue et moralement condamnée, ainsi que certainement, en raison des conséquences très lourdes (perte d'emploi, déchéance sociale, endettement pour frais de procédures, etc.) auxquelles s'exposent ceux qui font le choix de lancer une alerte. Comme en témoigne notamment le sort médiatisé de Stéphanie Gibaud (affaire UBS), d'Antoine Deltour (affaire Luxleaks) ou encore d'Edward Snowden (NSA).

Il était donc temps que le Gouvernement français, tout en rendant obligatoire la faculté de recourir en entreprise à un dispositif d'alertes, s'attelle à renforcer la protection, jusqu'alors éparse et lacunaire, des acteurs de ce système, afin de le rendre, au moins théoriquement, possible.

COMMENTAIRES

La loi Sapin II a ainsi élargi le champ d'application des alertes et renforcé la protection des lanceurs (**1**). La question, pour les entreprises, va désormais être quel dispositif d'alertes mettre en place (**2**) et comment traiter concrètement lesdites alertes (**3**).

1. L'extension du champ d'application des alertes et la protection renforcée des lanceurs d'alertes

1.1 Les entreprises concernées

Désormais, toute personne morale de droit privé de plus de 50 salariés a l'obligation de se doter d'une procédure de recueil des alertes (faute de quoi, elle s'expose à des sanctions, si elle compte plus de 500 salariés et réalise plus de 100 millions d'euros de chiffre d'affaires annuel) qui soit accessible tant à ses collaborateurs internes qu'à ceux extérieurs et occasionnels (tels que d'anciens salariés ou des prestataires (sous-traitants, fournisseurs, etc.). Mais il y a, à cet égard, une sorte de « malfaçon » dès lors que la procédure en 3 temps décrite ci-après ne peut s'appliquer pour ces derniers puisque, n'étant pas salariés, ils ne sont pas dans un rapport hiérarchique avec le récipiendaire initial de l'alerte (déontologue interne ou autre). Ainsi, pour être assurés que leurs alertes soient néanmoins réellement et efficacement traitées, ils devraient recourir plutôt, ou en parallèle, directement au Défenseur des droits.

1.2 Les personnes concernées et les conditions à respecter

Un lanceur d'alerte devra nécessairement :
- être une personne physique ;
- être désintéressée (même si elle pourra être rémunérée en matière fiscale) ;
- être de bonne foi (les dénonciations calomnieuses sont sanctionnées d'une peine d'emprisonnement de 5 ans et d'une amende de 45 000 €) ;
- avoir connu personnellement les faits signalés ;
- dénoncer des faits constitutifs d'un crime, d'un délit, d'une violation grave à un engagement international ou, - et c'est une nouveauté -, caractérisant une menace (il n'est pas obligé d'attendre la réalisation

effective des éléments matériels caractérisant une infraction) ou un préjudice graves à l'intérêt général.

1.3 La procédure à respecter

En entreprise, le lanceur d'alerte interne devra, dans un premier temps, réaliser son signalement auprès de son supérieur hiérarchique direct ou indirect, son employeur ou un référent désigné (palier interne, de niveau 1).
Si ce dernier ne traite pas ou mal l'alerte dans un délai raisonnable (non légalement défini), il pourra remonter son alerte à une autorité judiciaire (procureur de la République, etc.) ou administrative (Agence française anti-corruption, AMF, etc.) ou aux ordres professionnels (palier externe, de niveau 2). L'alerte devra être traitée dans un délai de 3 mois.
À défaut, le lanceur sera autorisé à révéler l'objet de son signalement au public, le plus souvent via un média de presse (palier externe, de niveau 3).
Sachant que le premier palier pourra être contourné si le lanceur estime que son supérieur hiérarchique est lui-même impliqué dans les faits dénoncés ou s'il le soupçonne d'être enclin à les couvrir.

1.4 Une protection renforcée

S'il satisfait aux conditions énumérées ci-dessus, le lanceur pourra désormais bénéficier des mesures de protection suivantes :
- interdiction de se voir infliger des sanctions disciplinaires et/ou mesures discriminatoires (notamment relatives à sa rémunération ou une promotion) et/ou un licenciement fondés sur son signalement (à défaut, il pourra être réintégré avec des indemnités) ;
- pénalisation des représailles : sanctions pénales pour violation de la confidentialité devant entourer l'alerte (2 ans d'emprisonnement et 30 000 € d'amende), ou pour entrave à la transmission d'un signalement (1 an d'emprisonnement et 15 000 € d'amende) ; et,
- sanction civile de 30 000 € d'amende pour procédure abusive en diffamation contre un lanceur.

Mais concrètement, quel dispositif les entreprises doivent-elles mettre en place et comment doivent-elles traiter les alertes ainsi recueillies ?

2. La plateforme d'alertes

Quand une entreprise est confrontée à la mise en place d'un système d'alertes, plusieurs questions se posent et plusieurs choix s'offrent à elle. Dans les grands groupes, les instances doivent, en amont, décider si elles optent pour un traitement des alertes centralisé au niveau du groupe, ou décentralisé en local.

À noter
Précisons que les problématiques relatives aux données personnelles et à la CNIL (obligation de déclaration préalable, consultation des instances représentatives du personnel, information individuelle des salariés, etc.) ne seront pas traitées dans cet article.

2.1 Un dispositif de signalement ouvert à tous

En principe, le dispositif doit être ouvert et accessible aux salariés de l'entreprise, mais également à toute personne externe (notamment sous-traitants, fournisseurs, etc.), ayant eu connaissance, dans le cadre de son activité professionnelle, de faits pouvant faire l'objet d'une alerte. Ainsi, l'adresse email (ou le site) dédiée, éventuellement complétée d'une ligne téléphonique, constituant la plateforme, devrait être une adresse internet et pas uniquement de type intranet. Le problème étant qu'elle doit être suffisamment facilement accessible et connue de l'extérieur, ce qui suppose que l'entreprise communique efficacement sur son existence, ce qui n'est, évidemment, pas nécessairement son souhait réel.

2.2 Un système externalisé ou administré en interne

Le deuxième choix important qu'il lui appartient de faire est de décider si elle souhaite administrer totalement en interne sa plateforme, ou sous-traiter totalement ou partiellement la collecte et le traitement de ses alertes à un prestataire extérieur. Ce choix étant guidé par les ressources et compétences dont elle disposera éventuellement en interne, mais également par le souci de la confidentialité devant entourer le traitement des alertes. Aspect à double tranchant. D'aucuns considèreront qu'il est risqué que des incidents internes soient connus et éventuellement traités par des interlocuteurs externes en raison des fuites possibles d'informations, une solution étant alors de recourir à un professionnel tenu par un secret absolu tel que l'avocat.

À noter
Précisons, à cet égard, que les seules informations ne pouvant faire l'objet d'une alerte, donc totalement couvertes par le secret, sont celles relevant du secret défense national, du secret médical et du secret liant un avocat à son client.

Tandis que d'autres considèreront que la confidentialité en interne entre collègues est extrêmement difficile à respecter, a fortiori si l'alerte est traitée par des personnes n'ayant pas de savoir-faire en la matière.

2.3 Un lanceur anonyme ou identifié

L'entreprise peut opter pour un dispositif où le lanceur a la faculté de rester anonyme (comme dans le système anglo-saxon), ou alors est obligé de s'identifier dès le début de sa démarche de signalement.
En France, la loi impose au lanceur d'alerte de s'identifier. Toutefois, une alerte anonyme pourra, à titre exceptionnel, être traitée, dès lors, notamment, que les faits allégués sont d'une certaine gravité et la preuve de leur véracité suffisamment établie.

À noter
L'anonymat n'est, cependant, pas recommandé car il complique le traitement de l'alerte ainsi que la bonne mise en œuvre de l'éventuelle politique interne anti-représailles.

2.4 Destinataires de l'alerte

Le système doit déterminer qui est destinataire des alertes. Il peut s'agir du directeur éthique et conformité, seul, ou accompagné, selon l'activité, la taille et l'organisation de la société, du directeur juridique,

éventuellement du directeur de l'audit et/ou des risques et du directeur de la sécurité, réunis dans un comité. L'idéal restant cependant qu'il y ait, pour des raisons de confidentialité, le moins possible de personnes destinataires des alertes.

2.5 Modèle simplifié de formulaire d'alertes

Le formulaire d'alerte est un élément essentiel du dispositif dès lors qu'il permet de rapidement filtrer les alertes et, ainsi, d'évacuer les alertes parasites qui sont « hors du champ », car elles relèvent davantage de plaintes d'ordre privé, ou sont réellement fondées mais ne pourront donner lieu à une suite faute d'être suffisamment étayées de preuves utiles et recevables. Il permet également de les trier par catégories, facilitant la tâche du destinataire qui les réoriente alors, le cas échéant, vers les personnes et départements compétents.

Nom, prénom, fonction, entité, coordonnées du donneur d'alerte	
Champ concerné (à cocher)	➜ Fraude financière/fiscale ➜ Délit d'initiés ➜ Corruption/paiements de faci ➜ litation ➜ Cadeaux et invitations ➜ Harcèlement moral/sexuel ➜ Discrimination ➜ Sécurité ➜ Santé/hygiène ➜ Droits de l'Homme ➜ Conflits d'intérêts ➜ Pratiques anticoncurrentielles ➜ Environnement
Description précise, objective et circonstanciée des faits (idéalement complétée de pièces)	Manquement/violation constaté(e) Précision de la ou des loi(s) et/ou politique(s) interne(s) violée(s)
Nom, prénom, fonction du mis en cause	

Une fois l'alerte enregistrée, elle devra naturellement être traitée.

3. Le traitement des alertes

3.1 La procédure de traitement des alertes

L'entreprise doit construire une procédure de traitement des alertes qui établira le cadre et les modalités (répartition des tâches, gouvernance, etc.) des étapes suivantes :

- réalisation d'une première caractérisation et analyse des faits ;
- s'il y a matière, déclenchement d'une enquête avec désignation d'un enquêteur interne ou externe, seul ou assisté d'un chargé de conformité, réalisée sous le contrôle de la direction éthique ou, le cas échéant, du comité en charge ;
- analyse des résultats du rapport d'enquête ;
- établissement d'un plan de mesures correctives ;
- évaluation, à court et moyen terme, des résultats des actions et clôture de l'alerte.

3.2 La procédure d'enquête

L'entreprise devra donc également rédiger une procédure relative à la réalisation de ces enquêtes particulièrement sensibles. Cette procédure devra notamment prévoir :

- le mode de recueil, d'analyse et d'archivage des preuves (emails, comptes rendus de réunions, documents, enregistrements, etc.) dans le respect des principes de légalité pour leur bonne opposabilité et des droits de la défense ;
- l'établissement d'un cahier des charges de mission de l'enquêteur : ses objectifs (rapports intermédiaires, rapport final incluant des recommandations), ses obligations, sa méthodologie, les modalités pratiques (calendrier, ressources, etc.) ; et,
- les modalités relatives aux entretiens des personnes interrogées : le mode de convocation, la liste des personnes habilitées à être présentes, la signature d'un engagement de confidentialité, les questions matérielles (pas d'enregistrement audio ni vidéo, faculté pour l'interrogé de revoir le PV d'audition, si possible pas de confrontation, etc.).

La mission de l'enquêteur étant extrêmement sensible, ce dernier doit revêtir les qualités suivantes : indépendance, autonomie et objectivité ; déontologie, discrétion et sens accru de la confidentialité ; éthique, transparence et intégrité ; rigueur, conscience, compétence, prudence, ainsi qu'humanité et délicatesse.

Il est donc idéalement recommandé de mandater, pour une telle mission, un avocat extérieur à l'entreprise.

Cependant, cette dernière pourra juger opportun de se doter d'une telle compétence en interne.