L'ALERTE ET LE LANCEUR D'ALERTE

195 Le dispositif d'alerte interne au service de la protection du lanceur d'alerte


Renaud Mousty,
expert conformité, Whispli
docteur en Sciences de Gestion

Sylvain Mansotte,
cofondateur et président, Whispli

In a current context where trends and regulations converge towards the importance and value of whistleblowers, the roadblocks to speaking up are standing out. Organizations across all sectors are facing the challenge of implementing an effective internal reporting tool. This article will explore how to effectively identify the right reporting channels, and to what extent can organizations leverage their whistleblowing system to reinforce whistleblowers' protection.

De nos jours, les récits de lanceurs d'alertes se multiplient et tendent à décrire un parcours du combattant où l'individu porteur du message est mis à mal. Le plus inquiétant est qu'un pourcentage infime de ces récits se termine sur une note positive. Car lancer une alerte fait peur. C'est une expérience angoissante qui se déroule dans des circonstances pénibles, sans échappatoire, et où le parcours personnel et professionnel d'un individu se risque au nom de l'intérêt général. Ce qui amène plus d'une personne à renoncer à son droit d'alerte.

C'est justement dans plusieurs de ces parcours que s'enracine l'histoire de la directive (UE) 2019/1937 du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union. D'où l'intérêt croissant pour un régulateur de cadrer l'expérience de lancement d'alertes là où l'organisation semble défaillir, du moins du point de vue extérieur : campagne #Metoo, wokisme, #Balancetonporc, etc… Toutes ces campagnes sont symptomatiques d'une volonté de transformation. La tendance est là, et les régulateurs clarifient la responsabilité qui incombent aux organisations.

La question revient donc aujourd'hui à identifier dans quelle mesure un dispositif d'alerte interne peut contribuer efficacement à la protection d'un lanceur d'alerte.

D'un point de vue organisationnel, il devient nécessaire de questionner trois aspects du lancement d'alertes :

1. Quelle organisation est nécessaire pour encadrer un dispositif d'alerte interne ?

2. Quels processus se montrent les plus efficaces pour organiser la protection d'un lanceur d'alerte ?

3. Quels sont les outils à disposition qui en simplifient l'exercice ?

Répondre à ces questions est précisément l'objet de cet article. Identifier les erreurs et les bonnes pratiques relatives à la mise en place d'un dispositif d'alerte interne permet d'augmenter significativement l'efficacité d'une démarche de mise en conformité ainsi que de réduire les risques au sein des organisations - par le biais des individus.

1. L'organisation au centre du nœud gordien

A. - Le référent

Adoptons le point de vue d'un référent. La première difficulté est d'ancrer une volonté réelle de traiter les alertes. Si cette volonté fait défaut, alors il n'y a aucun processus ni outil

pouvant garantir les conditions nécessaires et suffisantes pour organiser la défense d'un lanceur d'alerte et, par extension, la protection d'une organisation sur le long terme. Pour que les efforts déployés aient un impact significatif, le point de départ est de nommer un référent qui possède l'autorité et le courage nécessaire pour traiter chaque alerte et lui donner suite. Miser sur les valeurs éthiques et le CV d'un référent sont un facteur certes, essentiel, mais insuffisant. Cette position d'autorité doit pouvoir agir en toute indépendance.

> Les meilleures pratiques tendent à démontrer un effet corrélatif entre une augmentation dans la confiance du dispositif et du nombre d'alertes avec la nomination d'un référent qui a un parcours extérieur à l'organisation.

Si un(e) responsable a su faire faire ses premières armes à l'extérieur de l'organisation, la pression des pairs ou le truisme organisationnel auront un impact moins significatif sur ses choix.

B. - La culture

Analyser la culture de l'organisation est nécessaire pour identifier quelle stratégie est la plus efficace pour accompagner le dispositif. Celle-ci peut osciller entre le fait d'opter pour une position de force qui ancre le niveau d'autorité requis et la construction d'une coalition pour défendre les fondements du dispositif avec courage.

> L'adéquation du choix du référent ainsi qu'une analyse de la culture organisationnelle restent une condition prédictive du succès ou de l'échec de votre dispositif.

Une fois le candidat référent identifié, une organisation transparente et indépendante, effectuant une traçabilité des actions menées et communiquant régulièrement, mise en place, le dispositif d'alerte interne possède les prérequis pour gagner en efficacité. La seconde étape est d'identifier les processus adaptés à l'organisation.

2. Quels processus font preuve d'efficacité dans la protection des lanceurs d'alertes ?

A. - S'accorder au niveau des ressources de l'organisation

La première erreur à éviter est de tout miser d'emblée sur une approche processuelle graduée : contacter son manager, puis les fonctions supports en cas de doute puis enfin s'appuyer sur le dispositif d'alerte interne. Car cette approche fonctionne uniquement lorsqu'une organisation a les ressources suffisantes pour effectuer une campagne de sensibilisation relative à l'éthique et la conformité, et ce, à tous les niveaux de l'organisation. Dans le cas contraire, l'organisation s'expose à deux risques : le manque de confidentialité et l'ingérence.

Adoptons le point de vue d'une alerte effectuée par un salarié de bonne foi auprès de son responsable direct. Sans campagne de sensibilisation cyclique, il existe une probabilité élevée que la visibilité des politiques d'alertes au sein de l'organisation soit faible. La réaction du responsable recevant l'alerte est donc de se renseigner.

Voici comment se déroule le cheminement d'une alerte observée en situation réelle : le responsable pose la question à l'un de ses confrères. Celui-ci l'invitera à demander à sa femme, responsable des ressources humaines de la zone. Cette dernière se souvient que l'assistante du président directeur général était chargée il y a dix ans du processus d'alertes. Elle lui transmettra donc par courriel. L'assistante du président sait que le directeur du développement durable a pris le relai concernant l'éthique. De son point de vue, il doit donc être en charge et lui transfère à nouveau le courriel en question. Une décision d'arbitrage organisationnelle a transféré le dispositif d'alerte dans le giron du directeur juridique qui, une fois de plus, est mis en copie. Ce dernier a nommé récemment un responsable conformité à qui l'on transfère la requête pour action. Celui-ci demandera à son assistante de créer une alerte au sein du dispositif technologique récemment acquis pour assigner un enquêteur local… qui n'est autre que la responsable des ressources humaines de la zone ! Au final, 14 jours séparent la demande initiale d'un salarié de l'assignation d'un référent local, 7 personnes prendront connaissance des modalités de l'alerte avant même que la confidentialité de la démarche puisse s'organiser.

> Il est donc nécessaire d'opter pour des processus en phase avec l'organisation et les ressources dédiées.

B. - Distinguer investigation et prise de décision

Un second élément à prendre en considération est de faire une distinction sans équivoque dans un processus entre investigation et prise de décision. La première consiste à garantir que l'alerte et son investigation soient gérées en conformité avec les règles de l'art. La seconde consiste à prendre les décisions appropriées qui s'imposent. Cette distinction est primordiale, sans quoi la zone grise entre les deux poussera un responsable à faire ce pour quoi il est payé, à savoir traiter des problèmes. Dans ces circonstances, il est fort probable que l'alerte soit gérée localement dans la sueur, les larmes et le sang. Une bonne pratique en la matière est de clarifier la responsabilité de l'encadrement intermédiaire et son rôle dans les processus de traitement d'une alerte qui consiste à déclarer toute alerte via l'outil privilégié par l'organisation dans les 24 heures. Edifier les rôles et préciser, dans une procédure, la méthodologie de traitement d'une alerte permettent deux bénéfices : d'une part, encadrer le risque lié à la confidentialité de la démarche ; d'autre part, rassurer sur le rôle d'un référent (organiser les modalités d'investigation, assurer le caractère conforme de la démarche dans le temps et mettre ses compétences au service de la ligne hiérarchique appropriée pour que cette dernière puisse prendre ses responsabilités).

Sans cette distinction entre l'investigation et la prise de décision, le risque est fort de générer une levée de bouclier au sein des équipes lors de la campagne de sensibilisation et, par extension, de la défiance vis-à-vis du dispositif d'alerte interne.

Une fois l'organisation et les processus de traitement d'une alerte avalisés, la dernière question concerne les outils à mettre à disposition.

3. Quels outils peuvent encadrer une gestion sans faille de l'expérience de lancement d'alerte ?

Trois usages d'un dispositif d'alerte interne sont connus : l'internalisation, la prestation de services ou la technologie. Les trois modèles présentent du bon ou du mauvais en fonction de l'organisation et des objectifs poursuivis.

A. - L'internalisation

L'internalisation consiste à se reposer sur une technologie sommaire (par exemple, un courriel, le numéro de téléphone du référent, publié dans la politique de l'organisation, ou encore l'utilisation d'un coffre-fort numérique pour sécuriser les échanges). Simple, rapide à mettre en œuvre et permettant d'optimiser les coûts de gestion, l'internalisation est efficace pour assurer la protection d'un lanceur d'alerte, et elle repose avant tout sur une organisation spécifiquement formée pour gérer la confidentialité.

Autrement dit, l'internalisation s'adresse à des experts métiers possédant les ressources adéquates.

Le choix de l'internalisation peut paraître un bon pari au départ. Toutefois, une mise en garde est nécessaire si l'organisation en place n'est pas suffisamment formée ou mature pour encadrer la gestion des alertes. Un autre risque est celui de la méfiance que suscite par défaut un processus internalisé, surtout si la culture d'entreprise n'est pas préparée au lancement d'alertes. Pour un référent, se confrontant pour la première fois au déploiement d'un dispositif, le pari le moins risqué est d'opter pour une prestation de service externalisée.

B. - L'externalisation

L'externalisation de la gestion d'un dispositif garantit l'apport de compétences requises pour une gestion diligente des alertes.

L'expert tiers guide l'organisation du début à la fin et établit des recommandations permettant une prise de décision adéquate et circonstanciée. En fonction du niveau de services contracté, un transfert de compétences est possible et permet à un référent néophyte de progressivement monter en compétences jusqu'à atteindre le point d'autonomie requis pour internaliser le dispositif. À l'inverse, si cette prestation possède un coût humain moins important elle a un impact financier non négligeable. La question du budget est donc au centre d'un niveau de service externalisé et de qualité. Plusieurs profils sont envisageables : avocats, experts forensiques ou encore, plus récemment, consultant en conformité ayant une expérience précédente en matière de gestion d'alertes internalisée. Chaque profil est en mesure de proposer une prestation de services en phase avec vos objectifs.

C. - La technologie

Enfin, la dernière option est technologique et garantit une protection du lanceur d'alerte par design et par défaut.

Il existe deux types de prestataires technologiques. Les prestataires historiques, traditionnellement ancrés dans le modèle de la hotline, s'adressent principalement à des organisations ayant la capacité d'absorber une gestion en mode projet complexe. Le budget pour atteindre une performance adéquate reste cependant significatif et les coûts de gestion, notamment liés à la hotline, peuvent surprendre. À l'opposé, la nouvelle génération de dispositif d'alerte professionnelle, plus simple, mieux sécurisée, prenant à la fois en compte l'expérience du lanceur d'alerte et celui des référents, apporte une agilité sans pareille qui s'adapte progressivement aux objectifs d'une organisation. Reposant principalement sur l'innovation, l'orientation de ces nouvelles technologies concède une place de choix aux technologies web. Il devient donc nécessaire d'évaluer les canaux qui font sens au sein de l'organisation. Bien que de plus en plus plébiscitée, la technologie demeure le reflet de l'organisation et des processus mis en place. Il est primordial de tester la capacité du prestataire à accompagner l'organisation avant, pendant et après la mise en œuvre, sans quoi l'investissement effectué peut être contre-productif et générer de l'hypocrisie organisationnelle.

4. Déterminer son modèle de gestion d'alerte interne : les nouveaux enjeux

A. - Un dispositif interne attrayant

Du fait des nouvelles réglementations d'origine européenne ou nationale (directive européenne, loi Waserman), la hiérarchie des signalements est complètement déconstruite, laissant ainsi le libre choix du canal de signalement aux lanceurs d'alerte. D'où l'enjeu principal des organisations : rendre ses canaux internes les plus attrayants possible, faute de seconde chance. Un dispositif qui n'est pas en adéquation avec le profil d'une organisation ne sera pas utilisé et empêchera, de ce fait, la détection de risques occultes, obligera à faire face à un signalement externe ou public et causera une perte de contrôle de l'information et de la résolution d'incident - sans mentionner l'image générale de l'organisation. Parmi les aspects à prendre

en considération, le niveau d'appétence technologique (à tous les niveaux hiérarchiques), la culture globale (culture familiale, internationale, etc.), l'industrie dans laquelle l'organisation évolue, son niveau de régulation ainsi que le niveau de ressources sont des points clés à analyser pour identifier le modèle de gouvernance vers lequel tendre.

B. - Raconter le succès et les échecs d'une démarche de conformité

En définitive, l'enjeu est de proposer une organisation, des processus et un outil facile à activer, le tout accompagné d'un effort de communication et de démocratisation de la prise de parole adapté au profil d'une organisation. C'est à ce prix que se valorise une démarche de mise en conformité aujourd'hui. Le retour sur investissement dépasse cependant le strict encadrement de la protection des lanceurs d'alerte. En effet, si un dispositif d'alerte interne est pensé comme un véritable outil de gestion, celui-ci devient une mesure concrète des succès et des échecs d'une organisation et, par extension, de son instance dirigeante. Couplée à une digitalisation maîtrisée, l'histoire que raconte un dispositif d'alerte interne récompense la fonction conformité. C'est une finalité certes effrayante pour un dirigeant mais un grand pas en avant pour l'intérêt général et ceux qui ont eu le courage de faire valoir leur droit d'expression.