

Boite à outils
Anticorruption

Outil relatif au
Whistleblowing

Élaboré par : Hatem MANSALI

Introduction

Le dispositif d'alerte (terme français correspondant à l'anglais « whistleblowing ») est un outil important parmi les mécanismes de lutte contre la corruption. Les scandales financiers récents ont montré l'importance de se doter d'un dispositif d'alerte permettant de prévenir les cas de fraude d'ordre comptable et financier. Ce dispositif est de plus en plus reconnu comme un outil important de prévention et de détection des cas de corruption et des actes malveillants au sein des organisations. Les lanceurs d'alerte, en révélant les cas de fraude à la direction et/ou aux autorités, risquent leur carrière et leur emploi. Plusieurs pays se sont dotés de lois protégeant les lanceurs d'alerte agissant de bonne foi. L'objet de ce travail est de proposer une boîte à outil pour les entreprises souhaitant instaurer un dispositif d'alerte. Cet outil est destiné aux entreprises privées, entreprises publiques, et aux organisations non gouvernementales. L'idée sous-jacente est d'aider ces organisations à détecter les cas de fraude à un stade précoce, avant qu'ils ne causent des dommages ou d'être révélés aux médias. Ceci nécessite bien évidemment l'adoption d'une politique d'alerte et une procédure claire et précise au sein des organisations.

Les employés qui sont les mieux placés pour détecter les cas de fraude sont concernés au premier chef par la politique d'alerte. Selon cette politique, les employés qui, dans l'exercice de leur fonction au sein de l'organisation, se rendent compte d'actes répréhensibles sont invités à les déclarer à la direction de l'organisation ou à une structure dédiée. Pour ce faire, le présent document permet de les éclairer sur la procédure à suivre pour entamer leur démarche.

Définition du dispositif d'alerte

Le dispositif d'alerte peut être défini « *comme le fait, pour un membre d'une organisation (ancien ou actuel), de révéler l'existence de pratiques illégales, immorales ou illégitimes dont l'employeur a la maîtrise, à une personne ou à un organe susceptible de remédier à la situation* » (Near et Miceli, 1985, p. 4)¹. Les anglo-saxons désignent ce geste par l'expression whistleblowing, ce qui signifie littéralement donner un coup de sifflet. Au sens propre, le terme désigne le policier qui signale une infraction ou un crime par un coup de sifflet destiné à la fois à appeler ses collègues et à alerter la population d'un danger. Le terme whistleblowing peut être traduit par « dispositif d'alerte » ou « alerte professionnelle ».

Guy Dehn, l'inspirateur de la loi du Royaume-Uni de 1998, donne la définition suivante du dispositif d'alerte :

« Alerter les pouvoirs publics au sujet d'informations qui permettent raisonnablement du supposer l'existence de sérieux méfaits, lorsque de telles informations ne sont pas déjà connues, ou facilement vérifiables, et lorsque l'individu qui dévoile ces informations a le

¹ Near J.P. et M.P. Miceli, 1985, "Organisational dissidence : the case of whistleblowing", Journal of Business Ethics, 4: 1, p.1-16.

devoir (par exemple en tant que salarié) de les garder confidentielles, à condition que l'individu en question ait préalablement utilisé les voies internes praticables pour porter l'affaire à l'attention de l'organisme qui l'emploie ».

Le rapport de Transparency-international (France) « *Déclencher l'alerte : un nouveau dispositif de prévention et de lutte contre la corruption* » propose la définition suivante :

« Le déclencheur d'alerte est l'individu qui a connaissance d'informations constituant des indices sérieux qu'un acte contraire aux lois et règlements, ou qu'un acte contraire aux règlements professionnelles propres à un secteur d'activité, a été commis ou est sur le point d'être commis, et qui veut alerter les personnes compétentes au sein de l'entreprise ou de l'organisme dont il dépend ou, lorsque cette alerte n'est pas envisageable ou qu'elle est de nature à l'exposer à un risque sérieux de représailles, les autorités administratives ou judiciaires »

On pourrait distinguer deux sortes de dispositif d'alerte :

1. Le dispositif d'alerte interne : c'est le fait qu'un salarié donne une alerte interne à l'entreprise en transmettant une information à la hiérarchie ou à une structure dédiée.
2. Le dispositif d'alerte externe : c'est le fait de dénoncer les infractions commises aux autorités publiques compétentes.

Le dispositif d'alerte a été rendu obligatoire aux Etats-Unis par le Sarbanes-Oxley Act, pris en 2002 suite à plusieurs scandales financiers comme celui d'Enron ou de WorldCom. Il impose aux entreprises cotées en bourse (sociétés américaines et étrangères) aux Etats-Unis (NYSE, Nasdaq), et à toutes leurs filiales même étrangères, de mettre en place un dispositif d'alerte. La mise en place d'un dispositif d'alerte permet de détecter au moment opportun les irrégularités commises au sein de l'entreprise ce qui permet de prendre les mesures nécessaires. Elle vise également à restaurer la confiance des investisseurs, en renforçant la fiabilité de l'information financière et en améliorant la responsabilité des dirigeants.

Dans ce document nous traitons exclusivement le dispositif d'alerte interne.

Les avantages du dispositif d'alerte

La mise en place d'un dispositif d'alerte est le meilleur moyen de révéler les irrégularités. Détenteurs d'informations privilégiées, les salariés sont les mieux placés pour dénoncer les irrégularités dans une entreprise. Selon une étude réalisée par le « Report to the Nations », les irrégularités représentent pour les entreprises une perte estimée de l'ordre de 5% du chiffre d'affaires annuel des entreprises étudiées. L'étude révèle également que dans 40% des cas sont découverts par des dénonciations internes. Ceci dénote l'importance du mécanisme d'alerte éthique comme un moyen efficace pour les entreprises à lutter contre les délits économiques.

Le principal avantage de la mise en place d'un dispositif d'alerte est de détecter à un stade précoce les risques potentiels. En instaurant un tel dispositif, l'entreprise peut identifier les risques potentiels et adopter les mesures correctives, avant que l'information ne parvienne à l'extérieur. En revanche, si l'entreprise ne dispose pas d'un dispositif d'alerte en interne, elle court le risque de voir l'information sur les éventuelles infractions commises

parvenir aux médias avec les conséquences néfastes que pourrait subir l'image et la réputation de l'entreprise.

Les raisons qui motivent les entreprises cotées ou les organisations à mettre en place une politique d'alerte professionnelle peuvent être résumées ainsi:

- (a) Avoir une procédure claire pour toutes les parties prenantes
- (b) Faire en sorte que l'alerte soit traitée en interne
- (c) Permettre à l'entreprise/organisation de remédier aux cas de fraude avant qu'un dommage soit causé
- (d) Permettre à l'entreprise/organisation de traiter les cas d'alerte avant qu'elle soit parvenue aux médias
- (e) Agir promptement ce qui permet de réduire le risque de l'intervention des autorités ou de la justice
- (f) Renforcer la réputation de l'entreprise/organisation
- (g) Aider à entretenir une bonne culture d'entreprise

Le dispositif d'alerte : une exigence nouvelle de transparence

Dans une économie mondialisée, où la concurrence est de plus en plus rude, les entreprises sont appelées à réduire leurs coûts. Si ce facteur de compétitivité reste un objectif prioritaire pour les entreprises, il existe d'autres facteurs qui gagnent en importance tels que : la qualité des services liés au produit, capacité d'innovation, l'image de marque. Parmi eux, la réputation de l'entreprise et la qualité de sa communication avec les investisseurs sont devenus des enjeux majeurs pour instaurer un capital confiance. En effet, les entreprises contemporaines se financent, de plus en plus, directement auprès du marché financier notamment auprès d'investisseurs institutionnels. Pour satisfaire les besoins de ces nouveaux investisseurs en terme de rentabilité, les entreprises cotées tentent de les séduire en gérant leur image et leur notoriété de façon à faciliter leur accès au capital dans les meilleures conditions, en influant positivement sur leur cours de bourse.

Certaines entreprises n'hésitent pas à publier une information financière d'une façon biaisée de telle sorte qu'elle ne permet pas aux investisseurs et analystes financiers d'avoir une connaissance exacte de la situation réelle des firmes et plus particulièrement le résultat effectif de l'exercice. Ce comportement s'observe notamment dans la préparation par les dirigeants du compte de résultat et du bilan annuel. La presse économique et financière et également les organismes de contrôle font régulièrement état de ce problème lié à la transparence de l'information transmise par les sociétés. En utilisant l'espace discrétionnaire qu'offre tout système comptable, le dirigeant peut manipuler les chiffres comptables afin de publier des résultats qui soient conformes aux attentes des analystes financiers et des investisseurs. Cela a pu donner lieu à certaines dérives comptables comme celui d'Enron ou de WorldCom. D'où le souci de renforcer la transparence et la gouvernance des entreprises.

Par ailleurs, avec le développement d'Internet et des nouvelles technologies de l'information et de la communication, l'information circule désormais plus rapidement dans l'espace et dans le temps. Ce qui expose plus qu'auparavant les stratégies et les pratiques des entreprises en terme d'environnement et au respect des droits sociaux fondamentaux.

Des organisations internationales comme l'OCDE ou l'ONU ont défini un ensemble d'objectifs normatifs en direction des entreprises multinationales. Bien que juridiquement non contraignantes, ces normes influent progressivement sur le quotidien des entreprises. En Tunisie, plusieurs modifications législatives récentes ont renforcé l'obligation de transparence des entreprises cotées concernant leurs modalités de gouvernance interne (Loi n° 2005-96 du 18 octobre 2005, relative au renforcement de la sécurité des relations financières).

Le dispositif d'alerte en tant que mécanisme de protection contre la corruption

Le dispositif d'alerte est l'un des moyens de la lutte internationale contre la corruption (OCDE ou ONU). Les entreprises ont compris l'intérêt d'instaurer un dispositif d'alerte afin d'éradiquer la corruption et la délinquance financière. Ceci passe nécessairement par un changement de culture. En effet, la situation en Tunisie est sans doute plus délicate que dans d'autres pays, dans la mesure où la culture arabo-musulmane ne valorise pas l'acte civique de dénonciation : trop souvent mal perçu. Le dénonciateur risque des représailles et d'être victime d'ostracisme. Le cas particulier de la corruption et de ses différentes formes – corruption active ou passive, copinage, pots-de-vin – se caractérise par la difficulté de les mettre à jour. Cela s'explique par le fait que les deux protagonistes : celui coupable de corruption active et celui coupable de corruption passive ont intérêt à garder leur actes secrets. Dans la plupart des cas les lésés sont des tiers, mais ils ne s'en aperçoivent que rarement. Les initiés sont parmi les rares personnes capables de signaler des cas de corruption et d'identifier le risque inhérent à l'acte. En aidant à détecter les cas de corruption, le lanceur d'alerte joue un rôle critique en transformant le cercle vicieux en un cercle vertueux.

La détection de la corruption est une condition nécessaire pour initier des investigations et des poursuites. Cependant, c'est seulement dans le cas où les cas de corruption sont effectivement poursuivis qu'on peut envisager un changement de culture.

La majorité des scandales de corruption démontre le dommage causé par l'échec de reporter l'acte frauduleux au moment où il a eu lieu. L'indifférence, la peur de représailles, la culture du silence souvent empêchent des témoins potentiels et lanceurs d'alerte à parler. Le rôle joué par les lanceurs d'alerte qui franchissent le pas et qui ne sont plus disposés à jouer les spectateurs à dénoncer un acte répréhensible est capital. Selon l'Association of Certified Fraud Examiners, plus de 40% des délits économiques en sont découverts qu'à la suite d'un signalement interne. La convention des Nations Unies contre la corruption recommande notamment que les personnes qui signalent aux autorités compétentes de bonne foi et sur la base de soupçons raisonnables, des actes de corruption doivent être protégées.

Les expériences internationales

Le Royaume Uni a été le premier pays à adopter une loi permettant d'exercer le droit d'alerte et de protéger les lanceurs d'alerte. Ainsi, le Public Interest Disclosure Act adopté

en 1998 protège tout individu qui de bonne foi, dénonce à son employeur, à des organes ou services internes spécialement désignés ou, en carence de ceux-ci, aux autorités de police ou à la presse, de « sérieux méfaits » (serious malpractice). Les sérieux méfaits couvrent à la fois :

- Les crimes et les délits
- Les infractions aux lois et aux règlements
- Les fautes contractuelles
- Des atteintes à la santé et à la sécurité des personnes
- Des atteintes à l'environnement

La loi permet de protéger les lanceurs d'alerte au cas où ils sont sanctionnés pour avoir utilisé de leur droit d'alerte en leur offrant la possibilité de saisir les tribunaux pour obtenir réparation. La loi déclare abusif le licenciement d'un lanceur d'alerte suite à un signalement d'une alerte et lui permet d'obtenir sa réintégration provisoire en attendant le jugement. Enfin, d'après la loi, sont considérées comme nulles toutes les clauses ayant pour effet d'empêcher l'exercice du droit d'alerte.

Aux États-Unis, la loi Sarbanes-Oxley de 2002 impose aux sociétés cotées d'établir des procédures permettant aux employés de signaler des fraudes ou malversations comptables ou financières. Dans un souci d'efficacité, la loi comprend un mécanisme de protection des lanceurs d'alerte, elle rend passibles de sanctions pénales le fait d'exercer des représailles sur un employé qui a dénoncé de bonne foi des agissements frauduleux.

En Corée du Sud, la loi coréenne a créé une commission indépendante (Korea Independent Commission against Corruption). Elle a notamment pour mission d'encourager l'alerte professionnelle, de recevoir les dénonciations, de protéger les lanceurs d'alerte et de les récompenser.

En 2000, l'Afrique du Sud et la Nouvelle-Zélande ont adopté des lois similaires à celle de la loi britannique. En France, le principe d'interdiction des représailles à l'encontre des salariés est désormais repris en droit français au sein d'un article L. 1161-1 du Code du travail introduit par la loi du 13 novembre 2007 relative à la lutte contre la corruption, lequel dispose qu'« aucun salarié ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire, directe ou indirecte, notamment en matière de rémunération, de formation, de reclassement, d'affectation, de qualification, de classification, de promotion professionnelle, de mutation ou de renouvellement de contrat pour avoir relaté ou témoigné, de bonne foi, soit à son employeur, soit aux autorités judiciaires ou administratives, de faits de corruption dont il aurait eu connaissance dans l'exercice de ses fonctions ».

Toutefois, l'article L.1161-1 du Code du travail se contente de mentionner « de fait de corruption ». Ainsi, la loi française est beaucoup plus restrictive quant à la protection des lanceurs d'alerte, elle ne concerne que le « fait de corruption ».

Les organisations internationales ne sont pas demeurées indifférentes à ce mouvement. L'Organisation pour la coopération et le développement économique (OCDE) a adopté des Principes directeurs en 2004 à l'intention des sociétés multinationales disposent que « les parties prenantes, y compris les salariés au niveau individuel et les organes qui les représentent, doivent pouvoir faire état librement auprès du conseil d'administration de leurs inquiétudes concernant d'éventuelles pratiques illicites ou contraires à l'éthique ». Également, l'Union Européenne protège ses propres fonctionnaires depuis 1999 et, depuis

2004, elle fait obligation à ses agents de communiquer à l'Office européen de lutte antifraude toute information parvenue à leur connaissance laissant présumer l'existence d'une fraude.

Spécificités du dispositif d'alerte

Il est naturellement évident que la procédure d'alerte professionnelle ne peut pas être la même quelle que soit la taille de la société. Ne disposant pas des mêmes moyens financiers et techniques, les entreprises de petite taille et celles de grande taille n'obéissent pas à la même exigence en termes de procédure d'alerte professionnelle. Par conséquent, nous distinguons entre les entreprises de petite taille et celles de grande taille.

	Le dispositif d'alerte	
	Taille de l'entreprise	
	Petite taille	Grande taille
Les personnes concernées par le dispositif d'alerte	<ul style="list-style-type: none"> • Les employés à temps partiel et à temps plein • Les directeurs • Clients et fournisseurs • Connaissances du délinquant • Les membres du conseil d'administration 	<ul style="list-style-type: none"> • Les employés à temps partiel et à temps plein • Les directeurs et les cadres supérieurs • Clients et fournisseurs • Connaissances du délinquant • Les membres du conseil d'administration.
Les moyens techniques pour la transmission de l'information	<ul style="list-style-type: none"> • Dénonciation postale • Système de messagerie 	<ul style="list-style-type: none"> • Plateformes Internet • Lignes d'assistance téléphoniques • Dénonciation postale • Système de messagerie • Instances de médiation externes ou internes
A qui s'adresser	<ul style="list-style-type: none"> • Un ancien employé digne de confiance • La direction • Le fondateur de la société 	<ul style="list-style-type: none"> • Un ancien employé digne de confiance • La direction • Une entité extérieure • Comité d'audit • Advisors • Commission d'enquête
Formation et évaluation	<p>Rappeler à l'ensemble du personnel de l'entreprise l'existence du dispositif d'alerte, lors :</p> <ul style="list-style-type: none"> • de l'entretien d'embauche 	<p>Rappeler à l'ensemble du personnel de l'entreprise l'existence du dispositif d'alerte, lors :</p> <ul style="list-style-type: none"> • de l'entretien d'embauche • des évaluations annuelles • des formations et ateliers portant sur le sujet d'alerte professionnelle

Les difficultés de mise en œuvre

L'instauration d'un dispositif d'alerte au sein de l'entreprise se heurte le plus souvent à une défiance de la part des employés. En effet, les employés perçoivent mal le fait de dénoncer des collègues. En outre, ils appréhendent l'acte de dénoncer à cause des représailles. Il existe deux types d'entreprises : celles, majoritaires, qui considèrent le dispositif d'alerte comme une contrainte empêchant de se concentrer sur son métier ou son business ; et celles qui au contraire y voient une opportunité pour faire de la pédagogie en rappelant les règles d'éthique de l'entreprise.

1. Les résistances au changement

L'expérience en Europe a montré les difficultés de mettre en place un dispositif importé outre-atlantique. Ceci apparaît notamment lorsque certaines entreprises se sont contentées d'importer un dispositif conçu par leur maison mère située à l'étranger (souvent aux Etats-Unis), sans procéder à un effort de pédagogie et d'adaptation au contexte local. C'est ainsi que les employés ont perçu, à tort, le fait d'installer des lignes téléphoniques confidentielles comme un encouragement à la délation anonyme. Ce phénomène de résistance risque d'être plus accentué en Tunisie où la résistance au changement est plus importante. Pour parer à ce genre de problème, les entreprises doivent davantage faire preuve d'innovation et de pédagogie afin d'instaurer un dispositif d'alerte efficace et de gagner l'appui des employés pour le mettre en œuvre.

Le premier objectif de la mise en place d'un dispositif d'alerte n'est pas de sanctionner, mais de créer une nouvelle culture d'entreprise. L'adhésion des employés dans ce projet est un élément clé pour le succès du dispositif mis en place. Dès lors, il est essentiel de négocier la mise en place du dispositif avec les organisations syndicales représentatives des salariés.

2. Les conflits

Les règles dont les lanceurs d'alerte estiment qu'elles ont été transgressées, peuvent être professionnelles (par exemple des procédures standards ont été ignorées), légales (la législation n'a pas été respectée) ou éthiques. Généralement, ces salariés tentent d'abord de suivre la procédure interne mais sont le plus souvent déçus par l'issue de l'investigation. C'est pour quoi ils peuvent être amenés révéler les actes répréhensibles aux médias.

La cause profonde de leur dissidence au sein de l'organisation tient au fait que les attentes et les règles entrent en conflit. La violation des normes professionnelles est la cause la plus commune du tirage d'alerte – conséquence d'une tension presque universelle entre d'un côté, le jugement et l'autonomie professionnels et, de l'autre, la nécessité pour les grandes organisations d'assurer le profit et la maîtrise de leur activité (Bernstein et Jasper (1998)²). Si un conflit de normes et d'attentes explique l'entrée en dissidence de l'employé, sa progression vers le tirage d'alarme est généralement conditionnée par les caractéristiques individuelles et par les structures organisationnelles sur le lieu de travail. Comme le précise

² Bernstein M. et J.M. Jasper (1998), « Les tireurs d'alarme dans les conflits sur les risques technologiques, Entre intérêts particuliers et crédibilité », Politix, Vol. 11, n° 44, Quatrième trimestre, p : 109-134.

Bernstein et Jasper (1998)³ « les salariés sont plus enclins à livrer au public de l'information dommageable pour l'organisation (a) s'ils sont fortement investis dans les objectifs formels de l'organisation ou dans la volonté de faire réussir un projet, (b) s'ils s'identifient à l'organisation et (c) s'ils ont un grand sens de la responsabilité professionnelle ».

La mise en œuvre et la révision

Le dispositif d'alerte est mis en œuvre après la consultation des organisations syndicales représentatives des salariés et après avoir informé chaque employé individuellement que la procédure a été appliquée dans l'entreprise.

L'entreprise doit faire un effort de communication en ce qui a trait au dispositif d'alerte à tous les membres du personnel afin de pouvoir comprendre leur rôle et l'importance pour l'entreprise. Les résultats des enquêtes doivent également être communiqués si c'est possible annuellement. Ils peuvent également figurer dans le rapport annuel de la société.

L'entreprise est amenée à effectuer des révisions périodiques de la procédure d'alerte afin de l'adapter à la situation actuelle de la société.

Aspects pratiques du dispositif d'alerte

Toute personne travaillant dans ou avec l'entreprise et qui se rend compte d'acte répréhensible est tenue de la révéler à la hiérarchie ou à une structure dédiée. Généralement, les employés sont les mieux placés pour jouer ce rôle. En effet, tout salarié ou initié soucieux de son entreprise et motivé par la bonne marche du travail au sein de l'organisation est appelé à être encouragé à se manifester pour dénoncer les délits économiques. Une telle politique est pertinente pour toutes les organisations et les personnes. Nous proposons les conseils suivants qui permettent d'aider les entreprises souhaitant mettre en place un dispositif d'alerte éthique.

1. Objet du déclenchement d'alerte éthique

L'entreprise doit réaliser l'importance de l'enjeu de la mise en place de la procédure de déclenchement d'alerte éthique. Une attention particulière doit être portée aux objectifs suivants :

- L'entreprise doit veiller à la bonne marche de ses affaires en se conformant notamment aux normes les plus supérieures d'éthique des affaires, de transparence, d'intégrité et de responsabilité.
- La société doit traiter avec fermeté toute conduite illégale ou contraire à l'éthique par l'un de ses collaborateurs.
- L'entreprise doit veiller à créer un climat favorable pour les salariés afin qu'ils puissent communiquer librement les pratiques illégales, immorales ou douteuses à la hiérarchie ou à une structure dédiée, sans craintes de représailles.

³ Bernstein M. et J.M. Jasper (1998), « Les tireurs d'alarme dans les conflits sur les risques technologiques, Entre intérêts particuliers et crédibilité », Politix, Vol. 11, n° 44, Quatrième trimestre, p : 109-134.

2. Que faut-il signaler ?

En principe, il faut dénoncer toutes infractions contraires à l'éthique professionnelle ou à la loi. L'entreprise doit déterminer laquelle des infractions constituent de bonnes raisons pour déclencher la procédure d'alerte. En élargissant le champ d'application des infractions commises qui sont soumises à la procédure d'alerte permettrait d'élargir la protection de ses intérêts. Pour ce faire, il faut identifier avec précision les infractions susceptibles d'être commises au sein de l'entreprise et qui couvrent la procédure d'alerte éthique.

A titre d'illustration, on peut citer les infractions suivantes que le déclenchement d'alerte peut couvrir :

- (a) Infraction pénale
- (b) Le non respect d'une obligation légale
- (c) L'erreur judiciaire
- (d) Irrégularité financière
- (e) La corruption
- (f) La discrimination
- (g) L'abus de pouvoir
- (h) Un acte qui cause un dommage pour l'environnement
- (i) Un acte qui met en danger la santé et l'intégrité physique des employés
- (j) L'harcèlement
- (k) La dissimulation délibérée de tout ce qui précède

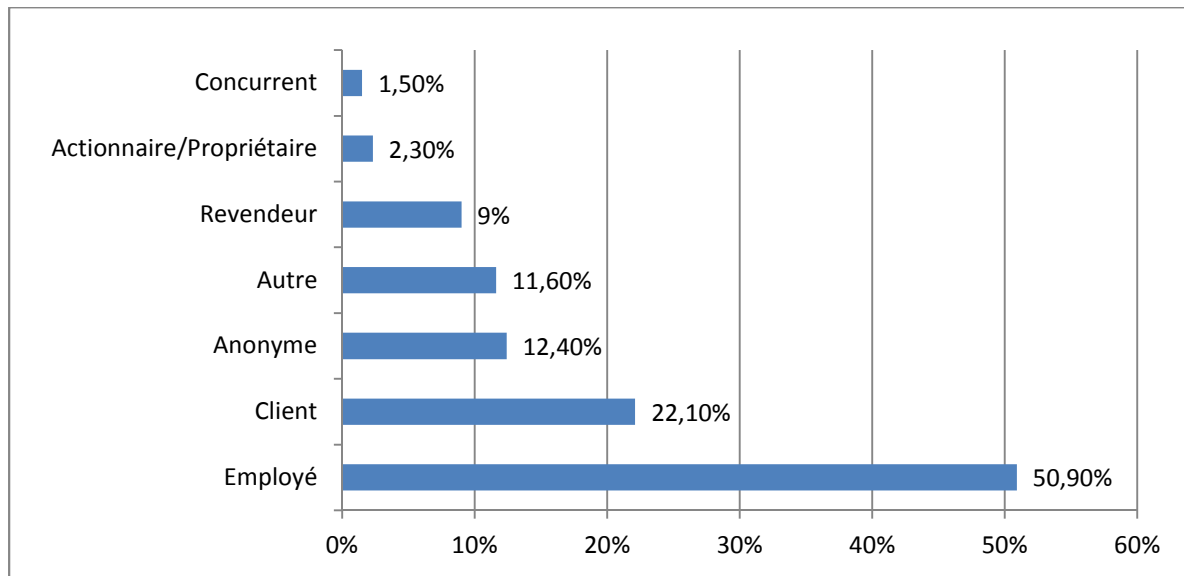
Toutefois, le déclenchement d'alerte ne doit pas couvrir toutes les situations du travail. Il faut en effet exclure du champ d'application de la procédure les erreurs de gestion qui découlent d'une gestion incompétente ou inefficace.

3. Les personnes concernées par le dispositif d'alerte

Pour que la politique d'alerte professionnelle soit efficace, il faut identifier les personnes couvertes par cette politique. En principe, tous les employés, cadres supérieurs, directeurs, etc. sont concernés par la politique d'alerte professionnelle. En effet, pour assurer une protection optimale des intérêts de l'entreprise, il faut associer l'ensemble du personnel de l'organisation au déclenchement d'alerte. Ainsi, sont concernés par la politique d'alerte professionnelle (i) les employés à temps partiel et à temps plein, (ii) les sous-traitants de l'entreprise, (iii) les directeurs et les cadres supérieurs, (iv) clients et fournisseurs, (v) les concurrents, (vi) les connaissances du délinquant, et (vii) les membres du conseil d'administration.

Comme le montre le graphique ci-dessous, les employés sont de loin la principale source de signalement. L'employé est la partie prenante concernée au premier chef par l'usage de l'alerte.

Les personnes concernées par le dispositif d'alerte



Source : Report to the Nations, 2012, ACFE

L'entreprise peut juger utile de limiter le champ d'application de la procédure à des personnes ayant accès dans le cadre de leurs fonctions aux ressources et aux données relatives à la gestion. Cependant, même si ce principe paraît convenir à certaines entreprises, il n'est pas préférable pour l'entreprise de discriminer les employés qui sont soumis à la procédure, et ceux qui ne le sont pas, ce qui risque de créer une confusion et le ressentiment dans l'entreprise.

4. Le libre arbitre du déclencheur d'alerte

Dans le cadre du contrat de travail, en principe, l'employé est soumis à un lien de subordination. Or, le dispositif d'alerte place le lanceur d'alerte en dehors du rapport de prescription hiérarchique. En effet, la possibilité qui lui est conférée de dénoncer des éventuelles pratiques frauduleuses de son supérieur hiérarchique ou de ses pairs signifie théoriquement qu'il peut s'exprimer librement. Pour que l'employé puisse témoigner et exercer pleinement son contrôle sur les dirigeants ou ses pairs, il faut qu'il soit libéré de la contrainte hiérarchique. Ainsi, l'employé peut exercer son libre arbitre c'est-à-dire à apprécier l'éventuelle dimension frauduleuse d'une situation et à décider d'alerter ou non, en conscience. En s'emparant d'espaces de liberté, l'employé peut cheminer vers l'autonomisation de son comportement (Charreire Petit et Surply, 2012)⁴. L'employé se trouve face à un dilemme : celui d'user de sa liberté pour signaler un acte frauduleux ou de ne pas user, et donc de se taire au risque de voir les dysfonctionnements se pérenniser.

⁴ Charreire Petit S. et J. Surply, 2012, « Parler ou se taire ou le dilemme du salarié lanceur d'alerte. Analyse critique à l'aune de sa liberté », Revue Economies et Sociétés.

Selon l'enquête européenne réalisée par Ernest et Young (2007), en France, seules 39% des personnes interrogées « pensent que le salarié de leur société se sentiraient libres de signaler un éventuel cas de fraude dans leur entreprise ». Toutefois, cette liberté est dans la pratique moins évidente : le lanceur d'alerte supporte des « coûts émotionnels très élevés » (Dyck et al., 2007, p 31)⁵ et des risques de représailles. Comme le suggère Charreire Petit et Surply (2012), le fait d'alerter peut constituer une forme d'obéissance dans la mesure où l'employé obéit aux injonctions de la charte éthique de l'entreprise. En effet, « la charte a un statut quasi-contractuel aujourd'hui dans les entreprises. Les salariés la signent fréquemment d'ailleurs ». Le fait de parler peut être interprété comme un acte loyal envers l'organisation. Mais dans certains cas, la peur des représailles ou d'être victime d'ostracisme peut l'emporter. Dans ce cas, l'employé va préférer se taire et ne pas dénoncer les infractions commises. Ce faisant, l'employé « couvre » fraude et fraudeurs.

5. La procédure d'alerte

L'alerte professionnelle est une pratique permettant aux employés d'exercer un contrôle interne via une procédure d'alerte afin de lutter contre la fraude et, plus généralement, contre les dysfonctionnements d'ordre comptable et financier. La procédure d'alerte est mise en place afin de protéger les intérêts de l'entreprise. Toutefois, certains employés peuvent être tentés de faire un mauvais usage ou malveillant pour satisfaire des fins personnelles. Ce comportement s'observe notamment lorsque l'employé adopte une attitude de vengeance ou de dépit. Afin d'éviter ce genre d'agissements déviants, l'entreprise doit encourager les comportements vertueux et responsables. Pour ce faire, l'entreprise est incitée à mettre en place des garde-fous afin d'éviter les comportements déviants potentiels ou encore les actes déloyaux destinés à favoriser la concurrence. Il s'agit là d'un point essentiel dont dépendra l'efficacité du dispositif d'alerte. En effet, s'il est utilisé à mauvais escient, le dispositif peut se retourner in fine contre ceux-là même qu'il est censé protéger.

Pour les raisons cités ci-dessus, la procédure doit être clairement définie. La procédure doit être mise en place et l'entreprise doit expliquer la manière dont elle répondra au lanceur d'alerte. Deux conditions doivent être réunies pour que la procédure soit équitable :

- L'anonymat : pour que le dispositif d'alerte marche, il faut offrir les garanties nécessaires permettant au déclencheur d'alerte de faire son acte dans l'anonymat. Selon une étude réalisée en 2007 par le Security Executive Council (Compliance Benchmark Report, 2007) montre que plus de 53% des lanceurs d'alerte ne communiquaient pas au début leurs données personnelles. L'entreprise doit offrir les conditions nécessaires pour rassurer le déclencheur contre toute mesure de représailles ou de discriminations. Convaincu que seul un rapport anonyme peut le protéger, le lanceur d'alerte doit bénéficier du droit de ne pas divulguer son identité.
- La confidentialité : Pour combattre la culture du silence, il est important d'offrir aux employés les conditions nécessaires de pouvoir s'exprimer de façon confidentielle, en mettant à disposition des employés par exemple des lignes téléphoniques garantissant une entière confidentialité. Bien que ces pratiques paraissent à première vue comme des pratiques des Etats totalitaires, il n'en demeure pas moins

⁵ Dyck A., A. Morse et L. Zingales, 2007, « Who blows the whistle on corporate fraud ? », CRSP Working Paper n° 618, ECGI Finance Working Paper.

que ça constitue dans certains cas comme le seul moyen efficace pour combattre la corruption et les délits économiques. La confidentialité vise à protéger les lanceurs d'alerte : aucun autre employé n'est censé apprendre l'existence de l'acte répréhensible ou le déclenchement de la procédure.

L'entreprise est incitée à considérer toutes les alertes émanant de ses employés et qui sont transmises à une instance extérieure ou à un interlocuteur interne. Ces derniers sont invités à transmettre l'alerte au Président de l'entreprise ou au Président du comité d'audit. L'entreprise peut constituer une commission afin d'enquêter sur ces cas d'alertes. Cette commission doit être en mesure de se procurer des informations complémentaires lorsqu'une enquête est menée. Elle doit être également en mesure de s'adresser au lanceur d'alerte et de lui poser des questions concrètes : bien évidemment ce cas de figure ne peut être envisagé que si le lanceur d'alerte révèle son identité. Même si la dénonciation est anonyme, il est toujours possible en utilisant des systèmes techniques qui permettent de s'adresser au lanceur d'alerte et de lui demander des précisions sans que celui-ci dévoile son identité. Ceci permet de réaliser une enquête exhaustive de l'incident.

L'entreprise peut également envisager un traitement de l'information par une instance extérieure.

Les moyens techniques pour la transmission de l'information doivent bien être bien définis :

- Plateformes Internet
- Lignes d'assistance téléphoniques
- Dénonciation postale
- Système de messagerie
- Instances de médiation externes ou internes

Dans certains cas, le lanceur d'alerte ne peut communiquer ces préoccupations qu'en dehors de la société ; cette dernière est invitée à lui offrir cette possibilité. Afin de garantir la confidentialité de la procédure, il faut que toutes les données concernant l'enquête doivent être stockées et protégées. Si le lanceur d'alerte insiste sur le fait de faire sa démarche de manière anonyme et confidentielle, il faut que cette volonté soit respectée. L'instance chargée de recueillir les cas d'alerte doit enquêter sur les questions soulevées, après avoir informé le Président de l'entreprise et le président du comité d'audit. Il est possible à l'instance chargée de recevoir les cas d'alerte d'obtenir de l'aide des commissaires aux comptes ou un autre expert reconnu afin d'enquêter sur les cas de fraude.

Une procédure spéciale doit être envisagée lorsque l'alerte concerne le Président de l'entreprise ou le président du comité d'audit.

Si l'acte répréhensible se révèle être une infraction criminelle, l'entreprise peut faire appel à des conseillers juridiques, ou même à la police, le cas échéant. Dans ce cas, on peut déroger à la règle de confidentialité.

En outre, toutes les plaintes doivent être traitées dans des délais très courts. Toutefois, il ne faut pas fixer des délais pour l'enquête : l'infraction pénale nécessite généralement un temps beaucoup plus long qu'une simple alerte éthique. L'entreprise doit être souple dans le traitement des enquêtes tout en montrant une célérité et efficacité dans le traitement des situations. Il est important que le lanceur d'alerte puisse déposer sa plainte en dehors des heures de bureau. L'idéal est d'offrir la possibilité à l'employé d'utiliser un service 24 heures

sur 24 et 7 jours sur 7 pour signaler tout acte répréhensible. Cependant, la plainte doit être prise en compte le plus rapidement possible et une réponse écrite doit être fournie aux lanceurs d'alerte dans un délai de temps raisonnable. Toute correspondance doit être envoyée à l'adresse individuelle du lanceur d'alerte.

Si un employé n'est pas convaincu de la manière avec laquelle a été traitée sa requête par les instances spécialisées, il sera autorisé à soulever la question avec le Président de l'entreprise ou le président du comité d'audit.

6. Formation et évaluation

Pour que le dispositif d'alerte mis en place soit efficace, il faut qu'il soit accompagné d'une campagne d'information et de sensibilisation auprès des employés. Il est ainsi conseillé de rappeler à l'ensemble du personnel de l'entreprise l'existence du dispositif d'alerte, que ce soit lors de l'entretien d'embauche, des évaluations annuelles, des formations, ou d'ateliers portant sur ce sujet. Comme le précise « le dispositif d'alerte éthique interne : guide pour les entreprises » publié par Transparency International Suisse, le personnel doit être sensibilisé aux questions suivantes :

- L'existence de la possibilité de signaler une irrégularité
- La procédure à suivre et l'instance à qui s'adresser
- La procédure suivie à la suite d'une dénonciation
- Les actes devant être signalés
- L'absence de sanctions en cas de signalement justifié
- La notion de signalement justifié
- La possibilité de garder l'anonymat et la protection conférée à l'anonymat
- L'exigence du PDG et la direction de dénoncer les cas de criminalité économique et leur adhésion sans réserve au dispositif d'alerte
- L'intolérance face aux cas d'abus.

Généralement, les employés sont déjà conscients de la nécessité de condamner les actes répréhensibles. Toutefois, tout en adhérant à la charte éthique de l'entreprise, ils ignorent comment procéder pour signaler ces actes répréhensibles et sont parfois sceptiques quant à l'efficacité des mesures adoptées. Ces difficultés réelles doivent être prises en compte par l'entreprise et ne doivent pas être sous-estimées. Pour parer à ces difficultés rencontrées par les employés, il est nécessaire que l'entreprise fasse un effort important de pédagogie. Pour ce faire, des formations peuvent être proposées. Ces formations doivent cibler tous les employés : simple salarié, cadres, cadres supérieurs, etc. et être adaptées à leurs attentes. Ils s'agit en effet de susciter chez les employés la notion de coresponsabilité.

Enfin, l'entreprise est invitée à faire des évaluations périodiques sur le fonctionnement du système. Des rapports peuvent être réalisés à cet effet.

Fonctionnement

1^{ère} étape : La désignation des responsables du dispositif d'alerte.

L'employé souhaitant signaler des irrégularités ou poser des questions à ce sujet doit pouvoir, sous le couvert de la confidentialité, s'adresser à une instance interne ou externe présentant de solides garanties, sinon d'indépendance, en tout cas d'impartialité. Normalement, l'employé doit s'adresser en premier lieu à son supérieur hiérarchique direct.

Si cette voie s'avère infructueuse, ou lorsque l'employé a des raisons fondées de s'en défier, qu'il y a lieu de s'adresser à d'autres instances. Si l'employé est de bonne foi, il faut que les personnes ou l'instance auxquelles il peut s'adresser lui paraissent dignes de confiance et qu'il ne craigne pas. Il faut également que l'employé soit assuré que sa démarche ne se retourne pas contre lui.

Cette tâche peut être confiée à une instance (ou une personne) rattachée à l'entreprise ou à une entité externe. En tout cas, l'instance ou la personne à qui l'employé peut s'adresser doit être formée dans la façon d'accueillir les lanceurs d'alerte. Ce rôle peut être joué notamment par une personnalité extérieure désignée en raison de ses compétences ou de ses qualités morales reconnues : un ancien employé pourrait s'en charger. Ce rôle peut également être joué par une entité externe : c'est le cas notamment lorsque l'entreprise installe une ligne téléphonique confidentielle dans le traitement des cas d'alerte professionnelle. Les appels sont reçus alors par une entreprise spécialisée. En outre, l'entité externe doit avoir la compétence de mener elle-même une enquête sur l'alerte ou de la communiquer à une instance interne compétente.

Cependant, le fait de faire appel à une entité extérieure, rémunérée par l'entreprise, ne constitue pas nécessairement un gage d'indépendance. Par conséquent, on peut suggérer désigner une ou plusieurs personnes appartenant à l'entreprise, qui s'en chargera de recueillir les messages des employés et de filtrer les cas nécessitant un traitement. On peut également suggérer une entité paritaire composé pour moitié de représentants du personnel et pour moitié de représentants de la direction. Ainsi, l'organisation d'une telle entité peut constituer un gage d'impartialité.

2^{ème} étape : La position des responsables du dispositif d'alerte dans la hiérarchie

Il est souhaitable que les responsables du dispositif d'alerte soient indépendants de la chaîne hiérarchique et aient le rôle d'advisors en étant rattachées, par exemple, à la direction générale soit au conseil d'administration ou encore au comité d'audit. Ces personnes doivent avoir une certaine expertise dans les domaines de la comptabilité, de gestion des ressources humaines et maîtrisant les aspects juridiques.

3^{ème} étape : Les attributions des responsables du dispositif d'alerte

Il convient de préciser quel est le rôle et quels sont les pouvoirs des entités désignées pour jouer le rôle d'interlocuteur auprès des employés. Les entités peuvent avoir un simple rôle d'information, d'assistance et de conseil. Dans tous les cas, il faut souligner et rappeler d'emblée que le seul employé peut décider des suites à donner à l'alerte. Si toutefois elles ont en plus des pouvoirs d'enquête et de proposition il faut expliciter quels sont ces pouvoirs et quelle peut être l'issue de l'enquête.

4^{ème} étape : La réception des cas d'alerte professionnelle par les responsables

Confirmation de la réception du rapport par les responsables. Les responsables doivent mentionner dans une correspondance adressée au lanceur d'alerte les éléments suivants :

- Votre rapport a été reçu ;
- Nous ferons les investigations nécessaires ;
- Dans la limite des contraintes légales, nous vous avisons des suites qui seront données à votre requête.

5^{ème} étape : Evaluation des rapports de dispositif d’alerte par les responsables

Une fois le problème est relevé, une évaluation doit être faite et les actions appropriées doivent être prises. Ceci peut inclure une révision informelle, une enquête en interne ou une investigation formelle. Le nom de la personne qui sera en charge de l’enquête est communiqué au lanceur d’alerte.

Il faut garder à l’esprit que le dispositif d’alerte mis en place peut constituer pas plus qu’une simple proposition adressée à la Direction, et qu’il ne peut généralement déboucher sur rien. En inculquant aux employés les limites du dispositif d’alerte permettrait de ne pas créer de faux espoirs chez les employés.

6^{ème} étape : Rapport final

Le rapport d’investigation sera passé en revue par le comité d’audit.

Les résultats possibles de l’investigation :

(a) L’allégation ne peut être justifiée

(b) L’allégation est justifiée avec :

- i. Action corrective afin de s’assurer que le problème n’aura pas lieu dans le futur
- ii. Action disciplinaire ou appropriée à l’encontre du fraudeur

7^{ème} étape : Le comité d’audit fait des recommandations à la direction

Un rapport final avec des recommandations (si c’est opportun), seront produits au comité d’audit. Le comité d’audit révisera le rapport final et fait les recommandations nécessaires à la direction.

Les responsables de l’enquête adresseront par écrit le résultat des investigations au lanceur d’alerte.

La mise en place

1) Politique

Les entreprises sont invitées à appliquer une politique d’alerte professionnelle. Pour ce faire, elles doivent édicter les lignes directrices de leur politique en matière de dispositif d’alerte, en précisant l’objet du déclenchement d’alerte, les personnes concernées au premier chef par cette politique, les garanties offertes par l’organisation pour ces employés. Nous proposons l’exemple suivant d’une politique de dispositif d’alerte à mener au sein d’une organisation :

Chacun de nous un jour ou l’autre a eu des préoccupations concernant un acte répréhensible dont il était témoin dans le cadre de l’exercice de ses fonctions. Habituellement, ces problèmes peuvent être facilement résolus. Cependant, si l’acte s’avère sérieux dans la mesure où il constitue un possible danger, une conduite non professionnelle, une fraude comptable ou financière qui pourrait affecter les clients, collègues, ou l’organisation elle-même, il est parfois difficile de savoir ce qu’il faut faire.

Vous pourriez avoir peur de relever ce problème et vous préféreriez le garder secret en pensant peut être qu’il s’agit d’une simple suspicion. Le fait de relever le problème, vous pourriez penser qu’il s’agit d’un acte déloyal envers vos collègues, vos directeurs ou envers

l'organisation. Vous avez déjà entamé la démarche mais vous pourriez penser que vous n'êtes pas adressés à la bonne personne ou votre démarche n'était pas la bonne et vous n'êtes pas sûr de ce qu'il faut faire ensuite.

La direction de [nom de l'organisation] s'engage à faire le nécessaire pour le bon fonctionnement de l'organisation et pour ce faire nous vous invitons à nous aider dans cette tâche. Nous avons introduit cette politique afin de vous rassurer qu'il est dans votre intérêt de nous parler à propos des problèmes qui vous préoccupent dans les plus brefs délais et à un stade précoce. Au lieu d'attendre des preuves, nous préférierions que vous veniez vers nous pour relever les problèmes à un stade précoce.

Cette politique est applicable à tous ceux qui travaillent pour nous : les employés à temps plein, les employés à temps partiel, les employés en intérim ou des volontaires.

Si vous êtes témoin d'actes répréhensibles et vous pensiez qu'il nécessaire que la direction soit mise au courant, prière d'utiliser cette procédure. La politique d'alerte professionnelle est applicable pour les individus qui travaillent pour nous et qui ont relevé des problèmes qui présentent un risque pour les autres employés ou pour l'organisation.

2) L'engagement de l'organisation envers ses employés

L'organisation est amenée à déclarer d'une manière explicite la protection de ces employés contre les représailles à la suite d'un acte d'alerte professionnelle et de leur garantir la protection de leur emploi. Elle doit également, leur offrir la possibilité de le faire d'une manière confidentielle et anonyme. Ci-dessous un exemple d'engagement de l'organisation envers ses employés :

i) La sécurité de l'emploi

La direction s'engage à appliquer la politique de dispositif d'alerte. Si vous relevez un problème concernant notre politique, vous ne risquez pas de perdre votre emploi, ou d'être victime de représailles ou d'ostracisme. Admettons que vous agissez en conscience, il importe peu que vous soyez trompés concernant le problème relevé. Nous ne vous demandons pas de donner des preuves concernant les problèmes relevés. Il est bien sûr admis que cette assurance ne soit pas étendue aux personnes qui agissent d'une manière malveillante.

ii) Confidentialité

Avec les assurances qui vous ont offertes, nous souhaitons que vous releviez tout problème ouvertement. Cependant, nous savons qu'il y a des circonstances où vous préféreriez parler en premier lieu à une personne en confiance. Si c'est le cas, prière de le mentionner dès le début. Si vous nous demandez de ne pas révéler votre identité, nous nous engageons de ne pas le faire sans votre consentement sauf si la loi l'exige. S'il est possible pour vous de participer à l'investigation, le fait que vous soyez à l'origine du signalement, serait dans la mesure du possible gardé confidentiel. Toutefois, il est possible que votre rôle de lanceur d'alerte soit dévoilé à des tierces personnes pendant l'investigation.

Vous devriez comprendre qu'il est parfois impossible pour nous de résoudre le problème sans révéler votre identité par exemple lorsque vos preuves sont liées à votre personne. Dans ces circonstances, nous pourrions discuter avec vous pour une éventuelle levée de la

confidentialité.

Nous tenons à vous rappeler que lorsque vous ne dévoilez pas votre identité et vous préférez rester anonyme, il serait difficile pour l'organisation de traiter le problème et plus particulièrement de vous défendre ou de vous donner des informations en retour.

iii) Anonymat

Nous respectons votre souhait de garder votre rapport confidentiel. Cependant, une allegation anonyme serait beaucoup plus difficile à traiter parce que nous ne serons pas en mesure d'obtenir des informations supplémentaires auprès de vous et faire une évaluation propre.

Généralement, nous n'encourageons pas les rapports anonymes et nous vous encourageons à venir vers nous pour signaler des actes répréhensibles.

3) Faux rapport

L'organisation doit avertir ses employés envers les cas de faux rapport. En effet, certains employés peuvent être tentés de faire un mauvais usage ou malveillant pour satisfaire des fins personnelles. Exemple :

Si vous faites un faux rapport sans fondement, pour des fins personnelles, et que l'information dans le rapport n'est pas précise et fiable, vous vous exposez à des actes disciplinaires, avec un possible licenciement.

4) L'acte répréhensible

L'organisation doit préciser une liste exhaustive des actes répréhensibles. Exemple :

S'il est impossible de donner une liste exhaustive des actes répréhensibles, il est cependant possible de signaler les actes suivants :

- (a) Infraction pénale
- (b) Le non respect d'une obligation légale
- (c) L'erreur judiciaire
- (d) Irrégularité financière
- (e) La corruption
- (f) La discrimination
- (g) L'abus de pouvoir
- (h) Un acte qui cause un dommage pour l'environnement
- (i) Un acte qui met en danger la santé et l'intégrité physique des employés
- (j) L'harcèlement
- (k) La dissimulation délibérée de tout ce qui précède

Même si vous n'avez pas des preuves tangibles concernant des actes répréhensibles, le rapport devrait au moins être motivé par les raisons qui vous ont conduit à donner l'alerte. Si vous faites un rapport en conscience, et même s'il n'a pas pu donner suite après investigation, votre signalement fera l'objet d'une évaluation et appréciation.

5) Comment relever un problème

L'organisation doit préciser la procédure à suivre par un employé au cas où il a eu connaissance d'un acte répréhensible. Exemple :

Si vous n'êtes pas certain de relever votre problème à n'importe quel stade, vous pouvez avoir de l'aide de la part du représentant du personnel. Il est important de vous signaler qu'il est possible de relever le problème sans avoir des preuves à l'appui. Cependant, nous vous demandons d'expliquer dans la mesure du possible les informations détenues ou les circonstances qui vont ont amené à relever le problème.

i) La première étape

Si vous avez des préoccupations à propos d'un risque ou d'un acte répréhensible, nous espérons que vous relevez le problème en premier lieu à votre chef hiérarchique. Cela peut être fait verbalement ou par écrit.

ii) Deuxième étape

Si vous ne pouvez pas relever le problème à votre chef hiérarchique, pour une raison ou une autre, prière de relever le problème avec :

[Nom du responsable désigné (exemple : le président du comité d'audit)]

[Détails du contact]

ou

[Instance paritaire]

Ces personnes sont qualifiées pour traiter les cas d'alerte professionnelle. Si vous souhaitez relever le problème d'une manière confidentielle, prière de le mentionner dès le début pour prendre les mesures nécessaires.

iii) Troisième étape

Si vous avez suivi la procédure précédente et vous n'êtes pas satisfait ou que vous sentez que le problème est suffisamment sérieux pour être traité par la procédure précédente, vous pouvez contacter :

[Le Président Directeur Général]

6) Comment le problème sera traité

L'organisation est invitée à préciser comment le problème sera traité, en précisant le nom de la personne qui s'en charge de l'enquête. L'organisation doit veiller également à communiquer avec le lanceur d'alerte pour avoir un feedback. Exemple :

Une fois le problème est relevé, nous en ferons une évaluation et nous prenons les actions appropriées. Ceci peut inclure une révision informelle, une enquête en interne ou une investigation formelle. Nous vous communiquons le nom de la personne qui sera en charge de l'enquête, et comment le contacter. Si vous le demandez, nous vous adresserons une correspondance dans laquelle nous résumons vos préoccupations et comment nous

procédons pour la résoudre et ce dans le but d'avoir un feedback de votre part.

Votre aide serait précieuse, si vous relevez votre préoccupation avec une éventuelle proposition de votre part sur la manière que vous estimez le mieux pour traiter le problème. Si vous avez un intérêt personnel qui vous a amené à nous signaler votre préoccupation veuillez nous le signaler dès le début.

Dès que possible, nous vous communiquons notre feedback concernant l'issue de notre investigation.

Sachant que nous ne pouvons pas garantir de traiter votre problème de la manière que vous souhaitez, nous vous assurons de traiter votre préoccupation de manière équitable et convenable. En appliquant notre politique, vous nous aidez à atteindre notre but.

Annexe : Positionnement du dispositif d'alerte par rapport à la réglementation tunisienne

La législation tunisienne : un état des lieux

Le droit tunisien consacre-t-il la technique de déclenchement d'alerte ? La réponse à cette question n'est guère facile. En effet, l'examen des lois tunisiennes est révélateur de contradiction en la matière : la nouvelle stratégie législative reflète la recherche de garantir une gestion transparente de l'entreprise. Cependant, l'examen de plusieurs dispositions spéciales nous conduit à regretter l'absence de toute consécration expresse de la technique de déclenchement d'alerte.

Un arsenal juridique important en faveur de la transparence

Le législateur tunisien a toujours été en phase avec le contexte économique national et international. La mondialisation de l'économie, l'accroissement de la concurrence et le besoin d'attirer les investissements étrangers ont influé sur la stratégie législative qui se trouve de plus en plus dirigée vers la garantie de la transparence. La loi relative à la sécurité des transactions financières de 2005⁶ renforcée par la loi n°2009-16 du 16 mars 2009⁷ s'inscrit dans le cadre de la lutte contre la corruption, la mauvaise gestion, les crédits impayés et l'évasion fiscale. Largement inspirée par la loi Sarbanes-Oxley (États-Unis), la loi sur la Sécurité des Transactions Financières en Tunisie repose principalement sur un renforcement du contrôle interne de la société par l'exigence de la désignation des organes de contrôle⁸, un renforcement de la crédibilité des informations financières présentées par les entreprises et un accroissement de l'obligation de diffusion des informations relatives à la gestion et à la prise des décisions au sein de l'entreprise. Ainsi, les dispositions de cette loi valorise le droit d'information et de communication des associés /actionnaires⁹ ainsi que

⁶ La loi n°2005-96 du 18 octobre 2005 relative à la sécurité des transactions financières, JORT n°84 du 21 octobre 2005, p.2811

⁷ La loi n°2009-16 du 16 mars 2009 modifiant et complétant le code des sociétés commerciales

⁸ Il s'agit essentiellement des commissaires aux comptes et des comités permanents d'audit. Article 13 ter csc (Ajouté par la loi n° 2005-96 du 18 octobre 2005) prévoit que « Sont soumis à la désignation de deux ou de plusieurs commissaires aux comptes inscrits au tableau de l'ordre des experts comptables de Tunisie :

- les établissements de crédit faisant appel public à l'épargne et les sociétés d'assurances multi-branches,
- les sociétés tenues d'établir des états financiers consolidés conformément à la législation en vigueur si le total de leur bilan au titre des comptes consolidés dépasse un montant fixé par décret,
- les sociétés dont le total de leurs engagements auprès des établissements de crédit et l'encours de leurs émissions obligataires dépasse un montant fixé par décret.

L'article 256 bis (Ajouté par la loi n° 2005-96 du 18 octobre 2005) prévoit que « La création d'un comité permanent d'audit est obligatoire pour :

- les sociétés faisant appel public à l'épargne à l'exception des sociétés classées comme telles du fait de l'émission d'obligations,
- la société mère lorsque le total de son bilan au titre des états financiers consolidés dépasse un montant fixé par décret,
- les sociétés qui remplissent les limites chiffrées fixées par décret relatives au total du bilan et au total de leurs engagements auprès des établissements de crédit et de l'encours de leurs émissions obligataires (...) »

⁹ Article 11 bis (Ajouté par la loi n°2009-16 du 16 mars 2009) « En sus des registres et documents prévus par la législation en vigueur, la société doit tenir :

- un registre mentionnant les noms, prénoms et adresses de chacun des dirigeants et des membres de conseil de surveillance ;

l'obligation de communication de certaines informations aux autorités compétentes. Selon cette loi, le Conseil du Marché Financier (CMF) doit être informé des résolutions adoptées par l'assemblée générale ordinaire ainsi que de l'état d'évolution du capital, du bilan après affectation du résultat et des états financiers lorsqu'ils avaient subi des modifications, dans un délai ne dépassant pas les 30 jours depuis la tenue de l'assemblée générale ordinaire, pour les sociétés faisant appel public à l'épargne¹⁰.

Dans le cadre du renforcement du contrôle interne de la société, le législateur oblige les commissaires aux comptes de communiquer à la banque centrale de Tunisie une copie de chaque rapport adressé aux assemblées générales¹¹. Aussi, le comité d'audit est-il tenu de veiller au respect par la société de la mise en place de systèmes de contrôle interne performant de nature à promouvoir l'efficacité, l'efficacité, la protection des actifs de la société, la fiabilité de l'information financière et le respect des dispositions légales et réglementaires¹².

Cependant, tout cet arsenal de règle juridique, bien qu'il ait remarquablement renforcé le contrôle et la transparence, souffre de l'absence d'une consécration d'ordre général de la technique de déclenchement d'alerte. Les employés de la société sont restés à l'écart. Rien n'a été dit à propos de leur intervention pour signaler toute sorte d'abus dans la gestion des sociétés. Leur rôle a été négligé quant à la détection des infractions financières ou économiques commises par les organes de gestion et ceux de contrôle des sociétés.

Avant la révolution tunisienne le contexte législatif était caractérisé par un dysfonctionnement remarquable du mécanisme de la dénonciation. Ainsi, les lettres de

- un registre des parts ou valeurs mobilières mentionnant notamment les indications relatives aux titres objet dudit registre, l'identité de leurs propriétaires respectifs, les opérations dont ils ont fait l'objet ainsi que les charges et droits grevant les titres en question, et ce, sous réserve des dispositions de la loi n° 2000-35 du 21 mars 2000 relative à la dématérialisation des titres. Les associés ont le droit d'obtenir des extraits des dits registres, dans les conditions prévues à l'article 11 précité, pendant les horaires habituels de travail à la société. Toutefois, concernant les sociétés anonymes faisant appel public à l'épargne, l'actionnaire peut consulter le registre des valeurs mobilières dans la limite de ce qui se rapporte à sa participation. Dans les autres cas, la consultation peut être faite en vertu d'une ordonnance sur requête du président du Tribunal de première instance dans le ressort duquel se trouve le siège de la société, si le demandeur justifie d'un intérêt légitime. La liste des actionnaires dans la société anonyme doit en outre être mise à la disposition de ces derniers, au moins quinze jours avant chaque assemblée générale des actionnaires.

¹⁰Article 3 bis. – (Inséré par la loi n°2005-96 du 18 octobre 2005, art.15) « Les sociétés faisant appel public à l'épargne doivent publier au bulletin officiel du conseil du marché financier et dans un quotidien paraissant à Tunis, leurs états financiers annuels accompagnés du texte intégral de l'opinion du commissaire aux comptes dans les délais visés à l'article 3 de la présente loi.

Toutefois, à des fins de publication dans le quotidien, les sociétés peuvent se limiter à publier les notes sur les états financiers obligatoires et les notes les plus pertinentes sous réserve de l'obtention de l'accord écrit du commissaire aux comptes ». Article 3 quater. – (Inséré par la loi n°2005-96 du 18 octobre 2005, art.15) prévoit que « Les sociétés faisant appel public à l'épargne doivent déposer au conseil du marché financier et à la bourse des valeurs mobilières de Tunis ou leur adresser quinze jours au moins avant la date de la tenue de l'assemblée générale extraordinaire :

- l'ordre du jour et le projet des résolutions proposées par le conseil d'administration ou par le directoire,
- le rapport du ou des commissaires aux comptes éventuellement,
- les documents mis à la disposition des actionnaires comme appui aux résolutions proposées.

Les résolutions sont adressées au conseil du marché financier et à la bourse des valeurs mobilières de Tunis dès leur adoption par l'assemblée générale ».

¹¹Article 13 quater csc tel que ajouté par la loi n°2005-96 du 18 octobre 2005.

¹² Article 256 bis csc tel que ajouté par la loi n°2005-96 du 18 octobre 2005

l'article 29 du code des procédures pénales¹³ ont été dépourvues de sens par les dispositions relatives à l'obligation de la discrétion professionnelle applicables dans le secteur public aussi bien que privé. Ces défaillances ont attirés l'attention des autorités à l'aube de la révolution tunisienne. Le décret-loi 2011-7 du 18 février 2011 portant création de la commission nationale d'investigation sur la corruption et la malversation était un pas important vers l'instauration d'un système de transparence dirigé vers la lutte contre la corruption. Deux tâches principales confiées à cette commission : une dirigée vers le passé¹⁴ et une autre vers le futur¹⁵. Cependant, la commission n'a pas réussi à réaliser ces deux tâches. Le décret-loi 2011-120 du 14 novembre 2011 portant sur la lutte contre la corruption¹⁶ est donc venu pour corriger les insuffisances du décret-loi du 18 février 2011. L'article 11 de ce décret-loi prévoit que l'Etat protège et encourage toute dénonciation des opérations de corruption par l'instauration d'une protection juridique des victimes, des témoins et des dénonciateurs. Ainsi, l'Instance nationale de lutte contre la corruption a été créée. Il s'agit d'un organisme public indépendant doté de la personnalité morale et de l'autonomie administrative et financière. Parmi les objectifs de cette instance figurent la dénonciation de la corruption dans les secteurs public et privé, la coordination entre les différents intervenants et le soutien du rôle de la justice. Pour réaliser ces objectifs, l'article 15 impose aux différents organismes et autorités publics de coopérer avec l'instance et de concrétiser la protection juridique dont jouit le dénonciateur. Les articles 35 et 36 reconnaissent à l'instance un droit d'accès aux documents des organismes publics et privés et obligent les fonctionnaires de collaborer avec elle pour réaliser ses objectifs.

Ce nouveau contexte juridique est fort marqué par le besoin de rompre avec les pratiques de l'ancien pouvoir. Ce pas aussi important qu'il soit, demeure insuffisant. Les textes juridiques doivent être entièrement révisés. Cette révision doit commencer par une consécration expresse de l'obligation de dénonciation accompagnée par une concrétisation de la protection du dénonciateur.

Le code des bonnes pratiques de gouvernance des entreprises tunisiennes

Le code des bonnes pratiques de gouvernance des entreprises tunisiennes présente les recommandations majeures relatives à la gestion et au contrôle des entreprises (gouvernance d'entreprise) et inclut des normes internationales, inspirées notamment des principes de gouvernement d'entreprise de l'OCDE, et nationales reconnues comme nécessaires à la bonne conduite et à la gestion responsable des entreprises. Le Guide vise à rendre le système tunisien de gouvernance d'entreprise plus transparent et plus

¹³ Article 29 prévoit que « Toutes les autorités et tous les fonctionnaires publics sont tenus de dénoncer au procureur de la République les infractions qui sont parvenues à leur connaissance dans l'exercice de leurs fonctions et de lui transmettre tous les renseignements, procès-verbaux et actes y relatifs. En aucun cas, ils ne peuvent être actionnés en dénonciation calomnieuse ni en dommages-intérêts, en raison des avis qu'ils sont tenus de donner par le présent article, à moins d'établir leur mauvaise foi. »

¹⁴ Art. 2 : « Le comité général est chargé de l'examen des orientations fondamentales ayant trait à l'activité de la commission et de l'identification des stratégies d'avenir afin de lutter contre la corruption et la malversation ».

¹⁵ Art.3 : « Le comité technique est chargé de dévoiler les cas de corruption et de malversation commis par ou pour le compte de toute personne physique et ou morale, publique ou privée ou un groupe de personnes grâce à son poste dans l'Etat ou l'administration ou en raison d'un lien de parenté ou d'alliance ou n'importe quelle autre relation qu'elle que soit sa nature avec un responsable ou un groupe de responsables de l'Etat notamment durant la période allant du 7 novembre 1987 au 14 janvier 2011 ».

¹⁶ Décret-loi 2011-120 du 14 novembre 2011 portant lutte contre la corruption, JORT n°88 du 18 novembre 2011, p.2746.

intelligible. Son objectif est de promouvoir la confiance des investisseurs nationaux et internationaux, des clients, des salariés et du public dans la gestion et le contrôle des entreprises tunisiennes. Ce code a renforcé les droits des employés en leur ajoutant une touche morale. Plusieurs principes généraux y ont été consacrés. Selon ce code « Les salariés représentent les piliers de l'entreprise. Ils ne doivent pas être considérés comme de simples prestataires de services mais, bien au contraire, ils représentent les premiers clients que l'entreprise doit fidéliser car c'est sur eux que repose en grande partie sa capacité à atteindre ses objectifs ». Outre le traitement humain et la protection des salariés contre toute forme de menace ou de discrimination, le code exige le développement d'un climat de confiance en invitant les salariés à s'exprimer librement, la communication aux salariés et à leurs représentants des informations exactes sur l'activité, la stratégie et les résultats de l'entreprise, la mise en place d'un climat de travail sain basé sur la confiance, la transparence, l'équité et le respect. La lutte contre la corruption sous toutes ses formes a été expressément prévu comme norme d'ordre général s'inscrivant dans le cadre de l'obligation d'agir avec droiture et honnêteté.

Par ailleurs, le guide incite les entreprises, surtout de grande taille, à adopter un code éthique de bonne conduite. Un code qui intégrerait sous forme de normes les valeurs de base de management telles que la responsabilité, la loyauté, l'égalité, la transparence, l'intégrité, le respect des personnes et de leurs croyances, ainsi que le respect de l'environnement.

Malgré l'apport indéniable de ce guide, rien n'a été dit à propos de la technique de déclenchement d'alerte. Aucune protection expresse n'a été accordée au dénonciateur des infractions au sein de l'entreprise. Il s'agit d'un simple guide de conduite qui est venu pour moraliser la vie des affaires. Il appartient donc aux entreprises de régler la question dans les codes éthiques de bonnes conduites si de tels codes existent.

Le déclencheur d'alerte bénéficie-t-il d'une protection juridique?

Il convient peut être de reposer la question : le déclencheur d'alerte est-il sanctionné en droit tunisien ? Plusieurs textes nous incitent à répondre par l'affirmative.

L'article 7 de la Loi n° 83-112 du 12 décembre 1983, portant statut général des personnels de l'Etat, des collectivités locales et des établissements publics à caractère administratif prévoit que « Indépendamment des règles prévues dans le code pénal en matière de secret professionnel, tout agent public est lié par l'obligation de discrétion professionnelle pour tout ce qui concerne les faits et informations dont il a connaissance dans l'exercice ou à l'occasion de l'exercice de ses fonctions. Tout détournement, toute communication contraire aux règlements de pièces ou documents de service à des tiers sont formellement interdits. L'agent public ne peut être délié de cette obligation de discrétion ou relevé de l'interdiction édictée par l'alinéa précédent que par autorisation écrite du chef de l'administration dont il dépend »¹⁷.

Selon cet article, l'obligation de réserve qui pèse sur le fonctionnaire public aurait pour effet de l'empêcher de dévoiler même les infractions dont il a eu connaissance à l'occasion de l'exercice de ses fonctions. Toute communication des actes illicites au public serait conditionnée par l'obtention d'une autorisation spéciale du superviseur. Le

¹⁷ Le non respect de ce devoir expose le fonctionnaire aux sanctions disciplinaires en plus des sanctions pénales encourues si l'acte constitue une infraction (art 56 de la même loi)

manquement à cette obligation de réserve est pénalement sanctionné. Article 109 du code pénal prévoit qu' « est puni d'un an de prison, le fonctionnaire public ou assimilé qui, indûment, communique à des tiers ou publie, au préjudice de l'État ou des personnes privées, tout document dont il était dépositaire ou dont il avait connaissance à raison de ses fonctions.

La tentative est punissable ». Cette obligation de discrétion persiste même en cas de convocation du fonctionnaire pour donner son témoignage. L'article 61 du code des procédures pénales prévoit que « toute personne citée comme témoin est tenue de comparaître, de prêter serment et de déposer sous réserve des dispositions du code pénal relatives au secret professionnel».

Le constat est donc clair : le fonctionnaire public est tenu par l'obligation de réserve qui constitue un obstacle majeur devant le déclenchement d'alerte externe c'est-à-dire toute dénonciation de l'infraction qui ne passe pas par les voies administratives ordinaires à savoir l'autorisation spéciale écrite du chef de l'administration. Tout ce que peut faire un fonctionnaire c'est d'informer son supérieur hiérarchique.

Le code du travail tunisien n'a pas apporté une solution différente de celle consacrée par la loi du 12 décembre 1983. L'article 14 quater du code de travail prévoit que « La faute grave est considérée comme l'une des causes réelles et sérieuses justifiant le licenciement. Peuvent être considérées comme fautes graves selon les circonstances dans lesquelles ont été commises notamment les cas suivants : (...) La divulgation d'un des secrets professionnels de l'entreprise hormis les cas autorisés par la loi ». L'article 168 du même code prévoit que : « Les membres de la commission consultative d'entreprise et les délégués du personnel, titulaires ou suppléants, sont tenus au secret professionnel, pour tous les renseignements de nature confidentielle qu'ils acquièrent pendant l'exercice de leurs fonctions et pour toutes les questions se rapportant aux procédés de fabrication. En cas d'infraction, ils sont passibles des sanctions prévues aux articles 138 et 254 du code pénal.

Cependant, quelques dispositions du code de travail nous invite à affirmer l'existence d'une certaine consécration de la technique de déclenchement d'alerte ; une consécration en germe certes, mais existante comme même. En effet, la lecture combinée de certains articles du code permet d'affirmer que l'employé est tenu de signaler les abus et les défaillances qu'il remarque durant l'exercice de ses fonctions au sein de l'entreprise. **L'Article 152-3 du code de travail** prévoit que « Le travailleur est tenu de respecter les prescriptions relatives à la santé et à la sécurité au travail et de ne pas commettre aucun acte ou manquement susceptible d'entraver l'application de ces prescriptions. Il est tenu notamment de ce qui suit : (...) -informer immédiatement son chef direct de toute défaillance constatée susceptible d'engendrer un danger à la santé et à la sécurité au travail... ». **L'article 10 du code de travail** prévoit dans le même ordre d'idée que « Le salarié est responsable des conséquences de l'inexécution des instructions qu'il a reçues, lorsqu'elles sont formelles et qu'il n'y a aucun motif grave de s'en écarter. Lorsque ces motifs existent, il doit en avertir l'employeur et attendre ses instructions s'il n'y a péril en la demeure ».

De ce qui précède on peut déduire que le salarié est tenu d'informer son employeur des infractions qu'il a découvert à l'occasion de l'exercice de ses fonctions. Cette obligation se limite à la sphère interne de l'entreprise. La dénonciation des infractions aux autorités compétentes n'a pas été prévue par la loi. Pis encore, cette dénonciation peut constituer un motif de licenciement puisque elle nuit à la réputation de l'entreprise. Si la situation se

présente, le salarié licencié risque de se trouver sans aucune chance de retrouver son poste. En effet, conformément à l'article 23 du code du travail, le licenciement abusif ouvre droit à des dommages-intérêt. Le juge ne peut donc pas imposer la réintégration du salarié dans l'entreprise.

S'agissant de la corruption, aucune règle de portée générale ne crée une obligation de dénonciation pesant sur l'employé qui en a eu connaissance. En effet, l'article 93 code pénal prévoit qu' « Est absous le corrupteur ou l'intermédiaire qui, avant toute poursuite, révèle volontairement le fait de corruption et, en même temps, en rapporte la preuve ». Cet article limite l'exonération de la peine seulement au corrupteur et à l'intermédiaire. Deux lacunes sont à signaler ici : d'abord, rien n'a été prévu à propos du corrompu qui, en cas de dénonciation de l'infraction s'expose à la sanction pénale. Ensuite, le texte reste muet à propos de l'employé qui a eu connaissance de la corruption et qui ne l'a pas dénoncé aux autorités compétentes. Les dispositions relatives à la corruption se sont donc avérées lacunaires et insuffisantes pour protéger la société contre cette infraction tant présente au niveau des organismes publics ainsi que ceux privés.
